Nekoyume: A truly decentralized massively multiplayer online role-playing game

Abstract: Nekoyume is a decentralized blockchain technology-based massively multiplayer online role-playing game (MMORPG). In Nekoyume, a large number of users can hunt virtual monsters to gain experience, collect essential in-game items from adventures, and become stronger. The action information of the game is recorded in a blockchain ledger, thereby enabling several users to participate without the requirement for a centralized server. In this work, we design a separate random consensus, called Hash random, to implement the game on the blockchain. Hash random is a random consensus obtained by combining the block hash, which is created by the proof of work, and the hash value of the individual action. Hash random minimizes the intentions of specific stakeholders, and is deterministic by each behavior.

1. Background

Bitcoin, proposed by Satoshi Nakamoto, introduced the concept of blockchain, which applied techniques such as digital signature, hashing, and proof of work, to create a public ledger. Blockchain has demonstrated that the decentralized main net is stable for nine years and that anyone can participate in the creation of a trustworthy virtual currency. [1]The vision of this trusted technology has also inspired several software projects. At present, blockchain technology is being implemented in applications that go beyond cryptocurrency. Vitalik Buterin further developed the bitcoin script to propose Ethereum, which is a decentralized application platform based on Turing complete Smart Contract. [2]

In the efforts to create a wide variety of applications for blockchain, several researches attempted to develop games. For example, CryptoKitties, is an online game where users can send and receive randomly generated cats. The enthusiastic response received almost paralyzed the Ethereum network temporarily.[3] However, since the use of random consensus on the blockchain is limited, there are several limitations to the games that can be implemented at present. If a more general-purpose random number generation approach is developed, users will be able to create and develop several different types of gaming applications using blockchain technology.

2. Pseudo-random number generation (PRNG)

One of the major limitations of Blockchain is 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, it is not possible to use a typical random value in an application on the blockchain, because all the users will be able to view different values based on the same data. However, several famous games, including Tetris, have

[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

random elements; therefore, implementing games on a blockchain without any restrictions is a significant limitation. To that end, there have been studies on pseudo-random number generation (PRNG) on blockchains to make blockchains more universal.

2.1. Random generation using block values

As regards the implementation, the use of block values for random generation is relatively simple. However, the miner can edit all the block variables, and therefore, it is not suitable for blockchains where the miner and the user are the same entity. [4]

2.2. Random generation using external services

Random generation using external services enables the complete concealment of random generation. However, because it is not a decentralized approach, it may lead to trust issues. [5]

Thus, the random generation method proposed in this work 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 created fairly by minimizing the likelihood of intentional involvement of specific user interests. To address this problem, Nekoyume proposes a random generation method called Hash random.

3. Hash Random

Hash random is designed to prevent stakeholders from attempting to generate an intentional number, in a way that would be detrimental to the interests of other users. To this end, we present two fundamental concepts.

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

3.1. Combination of behavior information from hash value and block hash

The hash value derived from a user's behavior information contains the signature of the user; therefore, it prevents the miner from intentionally transforming the hash value. The block hash is a value created by the miner. Therefore, the user cannot deliberately intervene in the generation of the block hash. 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 in the case that a combination of behavior information from hash and block hash value is used as a random seed, a miner can intentionally attempt to generate a favorable hash based on the behavior information of a user. To safeguard against this loophole, the timestamp corresponding to the creation of behavior information that can be included in the block is limited to 10 times the maximum block creation time. A miner may spend more time than other miners to find a hash that has a good combination of specific behavioral information at the expense of the following:

- The miners will be at a disadvantage when competing for hash compensation.
- The process of intentionally looking for profitable blocks is longer because of the requirement for periodically obtaining new behavior information.

4. Decentralized MMORPG

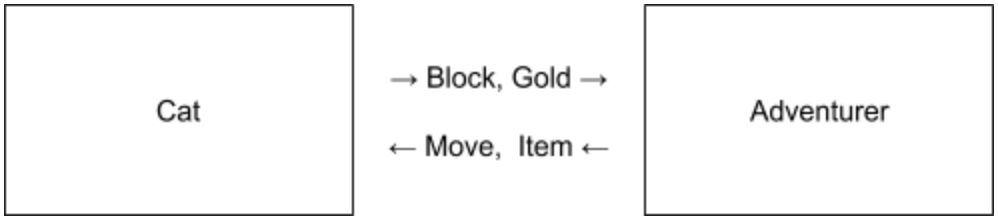
Nekoyume is a massively multiplayer online role-playing game (MMORPG) based on blockchain, which is regarded as the first game to incorporate the concept of Hash random. Users take on the role of adventure seekers, who venture and trade in the world of games, or become cats who can navigate blocks that 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, which has the following advantages.

1. In a centralized service operated by a specific entity, the service may be discontinued if the profitability of the game is not sustained. On the other hand, a blockchain-based game can continue as long as there is one participant left.
2. The fun factor of the game is not subject to the business intention (profitability) of the operating entity. The change in game design is determined by the consensus of the participant-oriented community; several participants can develop the fun elements of the game through consensus.
3. While centralized services give the service operator an economic advantage, blockchain-based games are distributed according to the agreed token economic model.

5. Economic Structure

The following figure illustrates the various elements shared by Nekoyume's cats and adventurers.



5.1. Adventurer

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

5.1.1. Moves

The player can perform the following actions in Nekoyume.

- ⚔ Hack & Slash: Combats monsters from the current area.
- 💉 Sleep: Player sleeps to regain physical strength.
- 🆙 Level Up: Raises the player level, thus improving player skill and ability.
- 🗣 Conversation: Allows the player to communicate with other players.

When the player moves, the behavior information is passed to the network, and the move is actually performed after the creation of the next block. The block creation cycle is takes approximately 15 seconds; moreover, one block cannot contain more than two actions per user, therefore the minimum action cycle is also approximately 15 seconds.

After the creation of a new block, 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. The process of creating the random value by using 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]
```

Players can acquire various in-game items through the adventure. However, since gold is only available through transactions, the players are required undertake adventures and obtain items through battles against stronger monsters, enabling the players to receive a lot of gold in the market.

The life cycle of the adventurer has been adopted from the Dungeon World rule. Dungeon World is a fantasy tabletop role-playing game (TRPG) 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 application of blockchain involving multiple users. Moreover, since all of the user's actions are designed to be judged by rolling a hexahedral dice twice, it is suitable to use random element.

5.2. Cat

The function of a Cat in Nekoyume is identical to that of a miner in Bitcoin. After receiving the adventurer's move information, 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 adopted the hashcash as a key consensus because it uses the Hash random with proof-of-work requirement. Since the block generation cycle is limited to 15 seconds, if the average of the recent block generation time is lower than 15 seconds, the demanding difficulty increases. Conversely, the average of the recent block generation time is higher than 15 seconds, the hard difficulty becomes lower.

5.2.2. Compensation system

After the completion of block search, the miner can receive gold as compensation. Initially, 16 gold per block are awarded; the reward reduces by half every four years, and will be affixed 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; however, it suffers from the following limitations.

6.1. Limitation of Hash Random

Hash random eliminates room for user intervention and has added constraints over random intervention. This enables the miner to benefit significantly from proof-of-work, which does not intentionally involve random results. However, if the miner stands to gain a sufficiently large reward that offsets the structural damage, the miner may attempt to create a deliberate hash despite the constraints. Therefore, even if Hash random is used, it is necessary to design the system such that excessive compensation is not provided 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 suited to ecosystems using that use proof-of-stake or other consensus methods because certain stakeholders can easily intervene at random.

7. Conclusion

Nekoyume proposed and implemented a new random consensus, called Hash random, by combining the existing Bitcoin and Ethereum consensus systems to develop a decentralized MMORPG. In this article, we have summarized the difference between the random generation method and Hash random in the existing blockchain. In addition, we also discussed the scope for Nekoyume’s further development. Hash random should be used with the proof-of-work consensus, and it will work as intended. Therefore, even if Hash random is used, the system must avoid providing heavy compensation to random values.