

Nekoyume: 탈중앙화된 대규모 다중 사용자 온라인 롤플레잉 게임

Abstract: 네코유메는 블록체인 기반의 탈중앙화된 MMORPG입니다. 다수의 사용자가 가상 세계 속의 괴물을 사냥하여 경험을 획득하고, 모험에서 중요한 아이템을 수집하여 더 강해질 수 있습니다. 게임의 행동 정보는 블록체인에 기록되어 노드간 통신을 통해 중앙 서버가 없이도 다수의 사용자가 참여할 수 있는 게임을 구성하였습니다. 게임에 꼭 필요한 랜덤 요소를 블록 체인 위에서 구현할 수 있도록 해시 랜덤이라는 별도의 랜덤 컨센서스를 디자인하였습니다. 해시 랜덤은 작업 증명에 의해 만들어진 블록 해시와 개별 행동의 해시값을 조합하여 예측이 어렵고, 특정 이해관계자의 의도를 최소화하며, 개별 행동에 결정적인 랜덤 컨센서스입니다.

Nekoyume: 탈중앙화된 대규모 다중 사용자 온라인 롤플레잉 게임	1
1. 배경	2
2. 유사 랜덤 생성 (PRNG)	2
2.1. 블록 값을 활용한 랜덤 생성	3
2.2. 외부 서비스를 활용한 랜덤 생성	3
3. 해시 랜덤	4
3.1. 행동 정보 해시와 블록 해시의 조합	4
3.2. 블록에 포함할 수 있는 행동 정보 시간 제한	4
4. 탈중앙화된 MMORPG	5
5. 경제 구조	6
5.1. 모험가	6
5.1.1. 행동	6
5.2. 고양이	8
5.2.1. 블록 생성 컨센서스	8
5.2.2. 보상 체계	8
6. 한계	9
6.1. 해시 랜덤의 한계	9
6.2. 작업 증명의 강제	9
7. 결론	9

1. 배경

사토시 나카모토가 제안한 비트코인은 기존의 전자 서명, 해싱, 작업 증명등의 기술을 이용해 블록체인이라는 개념을 제시하였습니다. 블록체인은 9년간 메인넷이 안정적으로 동작하며 탈중앙화되고 누구나 참여 가능한, 신뢰할 수 있는 가상 화폐를 만들 수 있음을 보여주었습니다.¹ 블록체인은 비트코인을 만들기 위해 제안되었지만 이 기술이 제시하는 누구나 참여 가능한 신뢰 시스템이라는 비전은 여러 소프트웨어 프로젝트에게 큰 영감을 주었습니다.

이제 블록체인은 화폐 이상으로 다양한 곳에 활용되고 있습니다. 비탈릭 부테린은 비트코인 스크립트를 더욱 발전시켜 튜링 완전한 스마트 콘트랙트를 바탕으로한 탈중앙화된 애플리케이션 플랫폼인 이더리움을 제안하였습니다.² 이더리움의 등장 이후, 블록체인 위에서 마켓플레이스, 소셜 네트워크 서비스, 거래소 등 다양한 애플리케이션이 만들어지기 시작했습니다.

블록체인에서 다양한 애플리케이션을 만들 수 있게 되자 게임을 만들기 위한 시도도 나왔습니다. 특히 랜덤으로 생성된 고양이를 주고받을 수 있는 크립토 키티³는 이더리움 네트워크가 일시적으로 마비되는 현상까지 보이며 열광적인 반응을 이끌어냈습니다. 하지만 블록체인 위에서 랜덤의 사용은 매우 제한적이기 때문에, 현재 구현할 수 있는 게임도 제약이 있었습니다. 보다 범용적인 랜덤 방식이 제안된다면 더 많은 종류의 게임 애플리케이션을 개발할 수 있을 것입니다.

2. 유사 랜덤 생성 (PRNG)

블록체인은 모두가 원장을 공유하는 특성상 체인 위의 데이터와 해당 실행 결과가 결정적이어야 한다는 제약이 있습니다. 즉, 블록체인 위의 애플리케이션에서 일반적인 랜덤 값을 활용하면 같은 데이터를 기반으로 모두가 다른 값을 볼 수 있기에 이를 원천적으로 금지할 수 밖에 없습니다. 하지만 테트리스를 포함한 많은 대중적인

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

게임에는 랜덤 요소가 존재하여, 랜덤 없이 블록체인 위에서 게임을 구현하는 것은 큰 제약이 있었습니다. 그렇기 때문에, 블록체인을 보다 범용적으로 사용할 수 있도록 하기 위해서 블록체인 위에서의 유사 랜덤 생성(PRNG)에 대한 연구가 있어왔습니다.

2.1. 블록 값을 활용한 랜덤 생성

블록 내에 접근 가능한 변수를 시드로 활용하여 랜덤을 생성하는 전략이 처음 제시되었습니다.⁴ 이 방식은 간단하게 랜덤 구현이 가능하지만 채굴자가 모든 블록 변수를 편집할 수 있기 때문에, 채굴자와 사용자가 동일인이 될 수 있는 블록체인에 적합한 방식은 아닙니다.

2.2. 외부 서비스를 활용한 랜덤 생성

외부 서비스를 통해 현재 행동에 대한 랜덤값을 받아와 적용하는 방법이 있습니다.⁵ 이는 랜덤이 만들어지는 방식을 완전히 숨길 수 있지만, 탈중앙화된 방법이 아니기 때문에 외부 서비스에 대한 신뢰 문제가 발생합니다.

이와 같이 현재 제안되어있는 랜덤 생성 방식은 특정 집단의 의도적 개입이 가능하다는 단점이 있습니다. 카지노에서 딜러가 확률을 조작하면 안되듯이, 랜덤은 특정 이해 관계의 의도적 개입 가능성을 최소화하여 공정하게 생성되어야 합니다. 이 문제를 해결하기 위해 네코유메에는 해시 랜덤이라는 랜덤 생성 방식을 제안합니다.

⁴ <https://etherscan.io/address/0xa11e4ed59dc94e69612f3111942626ed513cb172#code>

⁵ <http://www.oraclize.it/>

3. 해시 랜덤

해시 랜덤은 네코유메에서 제시하는 랜덤 컨센서스입니다. 해시 랜덤은 이해 관계자가 의도적인 유리한 수를 내기 위한 시도를 차단하거나, 시도를 하더라도 이해 관계상 손해가 나도록 디자인하였습니다. 이를 위해, 두 가지 주요 개념을 제시합니다.

3.1. 행동 정보 해시와 블록 해시의 조합

사용자의 행동 정보의 내용을 이용해 나온 해시 값은 사용자의 서명이 포함되기 때문에 채굴자가 의도적으로 변형할 수 없습니다. 블록 해시는 채굴자가 만드는 값이기 때문에 사용자가 의도적으로 개입할 수 없습니다. 두 해시 값을 XOR한 값을 랜덤 시드로 활용하여, (1) 사용자가 랜덤값에 대해 개입할 수 없으며, (2) 한 블록에서 모든 사용자의 행동은 개별 랜덤 시드를 바탕으로 진행될 수 있습니다.

3.2. 블록에 포함할 수 있는 행동 정보 시간 제한

행동 정보 해시와 블록 해시의 조합을 랜덤 시드로 활용한다고 해도 채굴자가 의도적으로 자신과 이해관계가 맞는 사용자의 행동 정보를 바탕으로 유리한 해시 생성을 시도할 수 있습니다. 이를 견제하기 위해, 블록에 포함될 수 있는 행동 정보 시간은 최대 블록 생성 시간의 10배 이내로 제한합니다. 채굴자는 특정 행동 정보와 조합이 유리한 해시를 찾기 위해 다른 채굴자보다 더 많은 시간을 투자할 수 있지만, 아래와 같은 손해를 감수해야 합니다.

- 채굴자 해시 보상의 경쟁에서 불리한 위치가 됩니다.
- 행동 정보를 주기적으로 새로 받아야 하기 때문에 유리한 블록을 의도적으로 찾는 과정은 더 길어지게 됩니다.

4. 탈중앙화된 MMORPG

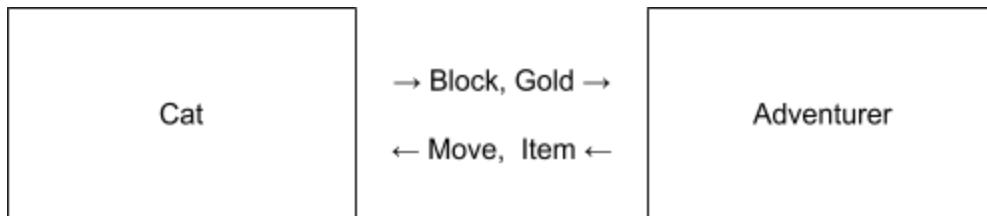
네코유메는 해시 랜덤의 개념을 처음으로 적용한 블록체인 기반의 다중 접속자 역할 수행 게임(MMORPG)입니다. 참여자는 모험가가 되어 게임 속 세계에서 모험을 하고 거래를 하거나, 고양이가 되어 게임 진행에 핵심인 블록 탐색을 진행할 수 있습니다.

네코유메는 블록체인 기반의 MMORPG이기 때문에 특정 주체의 중앙화된 서버가 존재하지 않습니다. 이는 아래와 같은 장점을 지닙니다.

1. 특정 주체에 의해 운영되는 중앙화된 서비스는 해당 게임의 수익성에 따라 서비스가 지속적으로 운영되지 못할 가능성을 가지게 됩니다. 블록체인 기반의 게임은 참여자가 1명이라도 남아있다면 게임을 계속 진행할 수 있습니다.
2. 운영 주체의 사업적인 의도로 게임의 재미 요소가 운영 주체의 수익성에 맞춰 크게 변경되는 일이 없습니다. 게임성의 변경은 참여자 중심 커뮤니티의 신중한 협의에 의해 결정되므로, 참여자 다수가 원하는 게임의 재미요소를 올바르게 키워갈 수 있습니다.
3. 중앙화된 서비스는 서비스 운영 주체에게 경제적 이익이 집중되지만, 블록체인 기반의 게임은 합의된 토큰 경제 모델에 맞춰 게임의 보상이 분배됩니다.

5. 경제 구조

다음은 네코유메의 고양이 참여자와 모험가 참여자가 서로 공유하는 요소에 대한 간단한 도표입니다.



5.1. 모험가

모험가는 자신의 직업을 설정하고, 모험을 하며 아이템과 경험을 모아 성장하며 더 강해질 수 있습니다.

5.1.1. 행동

아래와 같은 행동을 수행할 수 있습니다.

- ❄ 접근전: 현재 구역에서 출몰하는 괴물과 전투를 벌입니다.
- 💡 수면: 수면을 취해 체력을 회복합니다.
- 💡 레벨업: 레벨을 올려 능력치를 향상시킵니다.
- 💬 대화: 하고 싶은 말을 남깁니다.

행동을 선언하면 네트워크에 행동 정보가 전달되고, 다음 블록이 생성될 때 실제로 행동이 수행됩니다. 블록 생성 주기는 15초이며, 한 블록에 한 사용자의 두 행동이 포함될 수 없기 때문에, 최소 행동 주기는 15초가 됩니다.

블록 생성이 완료되면 해당 블록에 포함된 행동이 평가됩니다. 평가 시 해시 랜덤에 의해 결정된 랜덤값이 행동 결과에 반영되는데, 해시 랜덤에 의해 랜덤값이 만들어지는 과정은 아래와 같습니다.

```
>>> 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]
```

모험가는 모험을 통해 다양한 아이템을 획득할 수 있습니다. 하지만 골드는 거래를 통해서만 획득이 가능하기 때문에, 모험을 통해 성장하고 더 강한 괴물과의 전투를 통해 좋은 아이템을 획득해야 시장에서 많은 골드를 받을 수 있습니다.

모험가의 생활 주기는 [던전 월드](#) 규칙을 채택하였습니다. 던전 월드는 세이지 라토라와 아담 코벌이 아포칼립스 월드 엔진을 기반으로 만든 판타지 TRPG 규칙입니다. 던전월드는 플레이어간의 상호작용이 매우 중요한 TRPG의 특징을 계승하기 때문에 여러 사용자가 참여하는 블록체인의 특성에 적합하며, 사용자의 모든 행동을 6면체 주사위 2회 굴림을 통해 판정을 하도록 디자인되었기 때문에 해시 랜덤을 사용하기에 적합한 규칙이라고 판단하였습니다.

5.2. 고양이

고양이는 비트코인에서의 채굴자의 역할과 동일합니다. 모험가의 행동 정보가 들어오면, 다른 고양이에게 행동 정보를 공유하고, 행동 정보를 패키징하는 블록을 탐색합니다.

5.2.1. 블록 생성 컨센서스

네코유메는 해시 랜덤을 사용하기 위해서 작업 증명을 주요 컨센서스로 채택하였기 때문에, 프로토콜에서 제시하는 난이도를 바탕으로 해시 캐시를 진행해야 합니다. 블록 생성 주기는 15초를 목표로 하고 있기 때문에, 최근 블록 생성 시간의 평균이 15초보다 낮으면 요구 난이도는 올라가며, 반대로 15초보다 높으면 요구 난이도는 낮아집니다.

5.2.2. 보상 체계

블록 탐색이 완료되면 채굴자 보상으로 골드를 지급받을 수 있습니다. 골드 보상은 초기에는 블록당 16골드가 지급되며, 4년에 한번씩 반감기를 맞아 16년 후부터는 블록당 1골드로 고정되게 됩니다.

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. 한계

해시 랜덤은 블록체인 위에서 이해 관계자의 개입을 최소화하는 랜덤 컨센서스이지만 아래와 같은 한계를 가지고 있습니다.

6.1. 해시 랜덤의 한계

해시 랜덤은 사용자에게 랜덤에 개입할 여지를 없애고, 채굴자에게는 이해 관계상 상대적으로 랜덤 결과를 의도하지 않는 작업 증명이 가장 큰 이익이 될 수 있도록 랜덤 개입에 제약을 추가하였습니다. 하지만 만일 게임에서 랜덤을 통해 제시하는 이익이 이 구조상 손해를 무시할 정도로 큰 보상이라면 채굴자는 제약을 감안하며 의도적인 해시 생성을 시도할 수 있습니다. 따라서 해시 랜덤을 쓴다고 할지라도 랜덤에 과도한 보상이 이루어지지는 않도록 시스템을 설계할 필요가 있습니다.

6.2. 작업 증명의 강제

해시 랜덤은 작업 증명과 함께 쓰인다는 가정하에서 설계되었습니다. 지분 증명이나 기타 다른 컨센서스 방식을 사용하는 생태계라면 채굴자가 손쉽게 랜덤에 개입할 수 있기 때문에 해시 랜덤의 도입은 적절하지 않습니다.

7. 결론

네코유메는 탈중앙화된 MMORPG를 만들기 위해 기존 비트코인, 이더리움의 컨센서스 체계를 가져오면서 해시 랜덤이라는 새로운 방식의 랜덤 컨센서스를 제안하고 이를 구현하였습니다. 이 문서에서는 기존 블록체인에서 시도된 랜덤 생성 방식과 해시 랜덤의 차이를 정리하고, 이를 통해 네코유메가 어떤 형태로 개발되고 있는지를 함께 살펴보았습니다. 해시 랜덤은 작업 증명과 꼭 함께 쓰여야 의도된 대로 동작하며, 해시 랜덤을 쓴다고 할지라도 랜덤값에 의한 생태계 내의 지나치게 큰 보상은 발생하지 않도록 해야 할 것입니다.