블록체인에서의 신뢰 가능한 난수 생성 기법 및 적용 사례

강예준*, 김현지*, 김원웅*, 서화정*†
* 한성대학교 대학원 IT융합공학부

요 약

- 블록체인에서는 높은 난수성 및 신뢰성을 가진 난수가 필요 → 블록체인의 특성상 난수가 조작될 위험성이 존재
- 블록체인에서의 난수는 비편향성과 예측 불가능성 뿐만 아니라, 조작 불가능성을 만족해함
- TEE를 통해 보안 영역에서 난수를 생성하는 기법
- VRF를 통해 검증 가능한 난수를 생성하는 기법
- BLS 임계값 서명을 통해 난수에 사용되는 SEED를 참여자들이 함께 생성하는 기법

서 론

- 블록체인에서 난수는 지갑 및 거래에 사용되는 키를 생성하거나 스마트계약에 사용됨 → 높은 난수성 및 신뢰성을 가진 난수가 필요
- 하지만 블록체인은 제 3자인 중앙 기관이 존재하지 않기 때문에, 신뢰 가능한 난수를 생성하기 어려움
- 또한 모든 내역이 공개되므로 악의적인 노드가 공개된 내역을 보고 난수를 자신에게 유리하게 조작 가능
- 대표적인 블록체인 네트워크 중 하나인 이더리움에서 조차 난수생성기를 제공 X

동 향

1) TEE

- TEE(Trusted Execution Environment)는 메인 프로세서 내의 분리된 보안 영역으로서 신뢰 실행 환경을 제공[2].
- TEE를 통해 실행된 코드의 신뢰성, 런타임 상태의 무결성, 메모리에 저장된 코드의 무결성 등을 보장
- 이러한 특성으로 인해 Middleware'16에서는 TEE를 통해 생성한 난수를 활용하는 PoL 합의 알고리즘을 제안[3].
- 해당 합의알고리즘에서는 TEE기반의 RDRAND라는 명령을 통해 인텔 하드웨어 난수 생성기로부터 난수를 생성
  → 하지만 해당 합의알고리즘은 Intel을 신뢰한다는 전제하에 동작하는 합의 알고리즘
  → 블록체인의 특성인 탈중앙화를 만족시키지 못한다는 단점 존재

2) VRF(Verifiable Random Function)

- 암호학적으로 검증 가능한 난수 값을 출력하는 함수 → VRF는 크게 키 생성, 평가 그리고 검증 함수로 구성됨
- 주로 위임 기반 합의 알고리즘에서 대표자를 선출할 때 사용 → 대표적으로 Algorand[5]에서 해당 기법을 채택
- 하지만 VRF의 경우 온-체인 상에서 검증을 수행하기 때문에, 추가적인 시간 및 비용이 요구된다는 단점 존재

3) BLS 임계값 서명

- BLS 임계값 서명에서는 명의 그룹 참여자들이 개인키를 나누어서 소유[6].
- 각 참여자들은 개인키의 일부분만 소유하고 있으며, 참여자들은 그룹 서명이 필요할 경우 각자 자신의 개인키를 통해 서명
  → 이때 N명 중 K명 이상이 서명했을 경우에만 유효한 서명으로 인정
- 이를 통해 SEED 값을 정할 때, 특정 값에 대해 K명 이상이 서명했을 경우에만 해당 값을 SEED 값으로 사용
  → 따라서 다수의 참여자가 협력하여 난수를 생성할 수 있으며, K명의 참여자만이 서명을 수행하면 난수를 생성할 수 있기 때문에 악의적인 참여자가 의도적으로 서명을 하지 않더라도 이에 대해 대응이 가능
- 하지만 반대로 명의 악의적인 참여자가 집단적으로 부정직한 행동을 할 경우 문제가 발생할 수 있다는 단점도 존재
- BLS 임계값 서명을 통해 난수를 생성하는 대표적인 합의 알고리즘으로는 Roll-DPoS, Beacon Chain, DFINITY 등이 있음[7][8][9].

결 론

- 블록체인에서 난수를 생성하는 기법 및 적용 사례에 대해 조사 → 대표적으로 TEE, VRF 그리고 BLS 임계값 서명을 통해 난수를 생성
- 각 기법마다 장단점이 존재하므로 블록체인 네트워크에 따라 적절한 기법을 사용하여 난수를 생성해야할 것으로 생각됨
- 또한 이러한 단점들을 보완할 수 있는 새로운 난수 생성 기법에 대해서도 연구되어야할 것으로 생각됨

참고 문헌

[1] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." Decentralized business review (2008).
[2] Sabt, Mohamed, Mohammed Achemlal, and Abdelmadjid Bouabdallah. "Trusted execution environment: what it is, and what it is not." 2015 IEEE Trustcom/BigDataSE/Ispa. Vol. 1. IEEE, 2015.
[3] Milutinovic, Mitar, et al. "Proof of luck: An efficient blockchain consensus protocol." proceedings of the 1st Workshop on System Software for Trusted Execution. 2016.
[4] Micali, Silvio, Michael Rabin, and Salil Vadhan. "Verifiable random functions." 40th annual symposium on foundations of computer science (cat. No. 99CB37039). IEEE, 1999.
[5] Gilad, Yossi, et al. "Algorand: Scaling byzantine agreements for cryptocurrencies." Proceedings of the 26th symposium on operating systems principles. 2017.
[6] Zhang, Fangguo, Reihaneh Safavi-Naini, and Willy Susilo. "An efficient signature scheme from bilinear pairings and its applications." Public Key Cryptography-PKC 2004: 7th International Workshop on Theory and Practice in Public Key Cryptography, Singapore, March 1-4, 2004. Proceedings 7. Springer Berlin Heidelberg, 2004.
[7] Fan, Xinxin, and Qi Chai. "Roll-DPoS: a randomized delegated proof of stake scheme for scalable blockchain-based internet of things systems." Proceedings of the 15th EAI international conference on mobile and ubiquitous systems: computing, networking and services. 2018.
[8] Cassez, Franck, Joanne Fuller, and Aditya Asgaonkar. "Formal verification of the ethereum 2.0 beacon chain." International Conference on Tools and Algorithms for the Construction and Analysis of Systems. Cham: Springer International Publishing, 2022.
[9] Hanke, Timo, Mahnush Movahedi, and Dominic Williams. "Dfinity technology overview series, consensus system." arXiv preprint arXiv:1805.04548 (2018).