# Scalable한 신뢰

## Fraud Proof와 Data Availability 개요

본 보고서는 blockchain의 scalability를 증가시키기 위한 기술인 rollup에 대한 보고서 중 첫 번째입니다.

1. blockchain의 확장성(scalability)과 안정성(security)

blockchain이 안전하다고 불리는 가장 큰 이유는 모든 참여자가 transaction(e.g. 송금)을 독립적으로 검증(Decentralized)하기 때문입니다. 참여자는 유효한 transaction만 블록에 포함시키고 무효한 transaction은 거부함으로써 합의를 이룹니다. 정직한 참여자가 네트워크의 과반수를 차지할 때, PoW 합의 메커니즘은 모든 노드가 동일한 상태(e.g. 계좌 잔액)를 공유하도록 보장하므로 블록체인의 안전성이 확보됩니다.[1]

TPS를 증가시키기 위해 단순히 블록 내 트랜잭션 수를 늘리면 어떻게 될까요? 그러면 풀 노드에 과도한 메모리와 CPU 자원이 필요하게 되어, 풀 노드의 수가 감소하고 네트워크의 분산성과 안전성이 훼손됩니다.[2] 비트코인은 이를 인식하여 블록 크기를 1MB로 제한함으로써 풀 노드의 접근성을 유지하지만, 그 대가로 초당 약 7개 정도의 트랜잭션만 처리할 수 있습니다. (이는 Visa의 평균 1,500~2,000 TPS와 비교하면 극히 제한적입니다)
풀 노드의 자원 필요량을 유지하면서 TPS를 증가시키는 해결책은 무엇일까요? 바로 트랜잭션의 검증 및 실행을 풀 노드로부터 분리하는 것입니다. 풀 노드가 모든 트랜잭션을 직접 검증하고 실행하지 않으면, 트랜잭션 수를 증가시켜도 각 노드에 요구되는 계산 자원이 선형적으로 증가하지 않습니다. 따라서 풀 노드의 수를 현 수준으로 유지하면서도 처리량을 크게 늘릴 수 있습니다. 이것이 바로 Roll-up 개념의 핵심입니다.

2. roll-up 과정

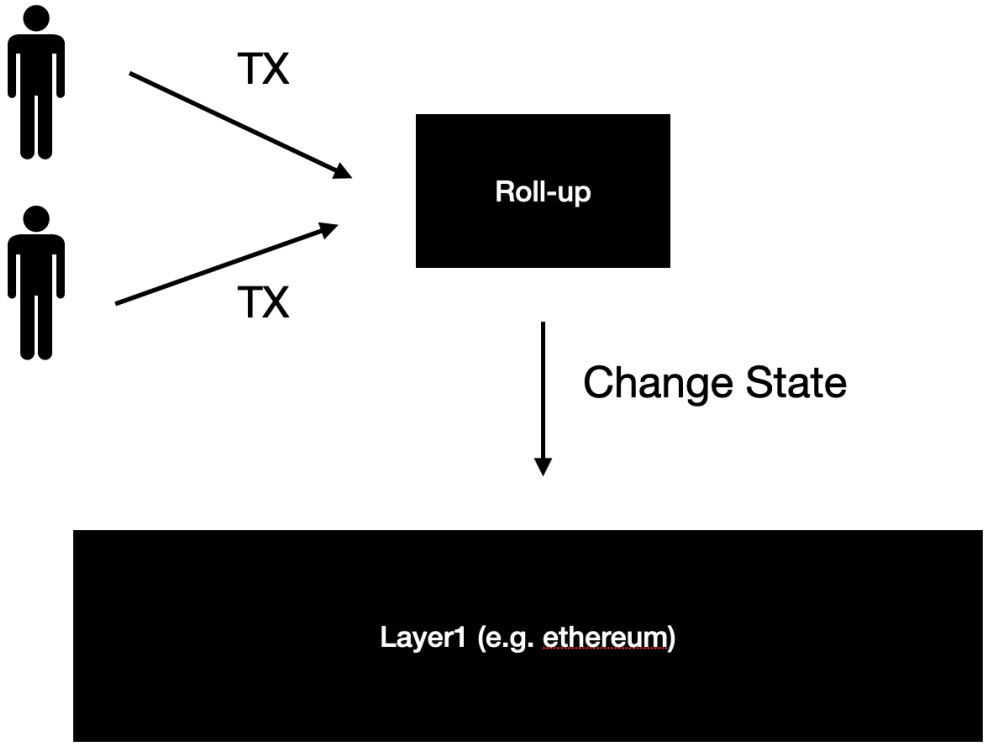
roll-up의 기본적인 architecture

rollup의 기본적인 과정은 다음과 같습니다.

1) user가 자신의 transaction을 ethereum이 아닌, roll-up에 보냅니다.

2) roll-up은 들어오는 transaction에 대한 순서를 결정합니다(sequencing)

3) roll-up은 transaction에 대한 유효성을 검증하고, state를 변경합니다. (aggregate)




4) roll-up은 ethereum에 변경된 state를 기록합니다. 여기서 state란 각 계정들의 잔액을 의미합니다. 실제로 저장될 때는 merkle tree로 암호화되어 저장됩니다.

Roll-up이 ethereum에 state를 기록하는 이유는 user들이 같은 state에 대해 합의를 하고, transaction이 기록될 때, 올바른 시점에서 시작했음을 보장하기 위함입니다.즉, 여기서는 ethereum이 transaction을 실행하는 역할이 아닌, 모두가 합의할 수 있는 state를 저장하는 분산 ledger로서 역할을 합니다. 구체적인 architecture와 구현은 [3]의 3.1, 3.2 와 [4]를 참고하시면 됩니다. 또한, 여기서는 sequencing하는 주체가 단일 객체로 표현되지만, 분산 합의로 구현될 수도 있습니다.[5]

## 3. Fraud Proof

만약 roll-up이 잘못된 transaction을 유효하다고 속여 state를 기록하면 어떻게 될까요?(e.g. A는 100 bitcoin만큼 가지고 있지만, A가 B에게 101 bitcoin 전송하는 transaction을 ethereum에 기록) 이러한 것을 방지하기 위해 다른 참여자는 fraud proof를 ethereum에 제출해, 잘못되었다는 것을 증명합니다. 만약 이것을 증명하면, rollup에서

ethereum에 state를 기록한 사람(rollup 연산자)에게 deposit을 빼앗고, 증명한 사람에게 그것을 줍니다. Fraud proof의 구체적인 증명 과정은 다음과 같습니다.

1) 증거 제출: 잘못된 transaction, 잘못된 transaction을 실행하기 전의 state, 후의 state를 contract에 제출합니다.

2) 검증 실행: Contract는 state가 잘못된 transaction에 의해서 제대로 변경되는지 검증합니다.

이 때, contract는 ethereum에 있으므로 100% 신뢰적이라고 볼 수 있습니다.

그런데 여기서 중요한 질문이 생깁니다. 다른 참여자가 사기 증명을 제출하려면, 먼저 rollup 연산자가 제출한 잘못된 transaction과 state 변화를 알아야 합니다. 만약 rollup 연산자가 의도적으로 이 정보를 숨기거나 공개하지 않으면 어떻게 될까요?
예를 들어, rollup 연산자가 100개의 transaction을 처리했는데, 그 중 일부만 이더리움에 제출하고 나머지는 숨긴다면? 다른 참여자들은 숨겨진 transaction의 존재 자체를 알 수 없기 때문에 사기 증명을 제출할 수 없습니다. 이것이 바로 Data Availability 문제입니다.

4. Data Availability(DA)
Data Availability(DA)이란 rollup 연산자가 처리한 모든 transaction 데이터가 네트워크의 모든 참여자가 접근할 수 있도록 공개되어야 한다는 원칙입니다. 이것이 보장되어야만 다른 참여자들이 fraud proof을 제출할 수 있고, rollup의 보안이 유지됩니다.
가장 쉬운 방법은 참여자에게 모든 transaction을 전송하는 것입니다. 하지만 대부분의 참여자는 모든 transaction을 저장할 정도로 컴퓨터 자원이 많지 않습니다. 따라서 참여자는 rollup 연산자에게 random으로 transaction을 요구합니다. 그리고 random하게 받은 transaction을 바탕으로 데이터가 조작되지 않았는지 확인합니다. 이것을 Data Availability Sampling(DAS) 이라고 합니다. 다음 report에서는 DAS에 대해 구체적으로 다루겠습니다.

Reference

[1]: Bitcoin: A Peer-to-Peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf

[2]: M. Al-Bassam, A. Sonnino, and V. Buterin, “Fraud proofs: Maximising light client security and scaling blockchains with dishonest majorities,” CoRR, vol. abs/1809.09044, 2018.

[3]: John Adler, Mikerah Quintyne-Collins “Building Scalable Decentralized Payment Systems”, https://arxiv.org/abs/1904.06441

[4]: https://github.com/juincc0/optimistic-rollup-example-erc20

[5]: Mark Odayan, The Practical Guide to Ethereum Rollups, https://web.archive.org/web/20241108142548/https://research.2077.xyz/the-practical-guide-to-ethereum-rollups