토카막 레이어 2 암호경제 (Tokamak layer 2 Cryptoeconomics)

저자 (Authors)

- Kevin Jeong (kevin@tokamak.network)
- Wyatt Park (wyatt@tokamak.network)

목차 (Contents)

배경 요약 (Background summary)

1. Tokamak Network Pte. Ltd. (“회사”) 는 옵티미스틱 롤업 (Optimistic Rollup) 레이어 2(L2) 솔루션을 활용해 이더리움 (L1) 탈중앙화 애플리케이션의 확장성 문제를 해결할 수 있는 프로토콜을 개발해왔다. (“토카막 네트워크”). 토카막 네트워크는 이더리움 블록체인에 내재된 기능적/성능적 한계를 완화해 애플리케이션을 쉽게 배포할 수 있는 환경을 제공할 것이다.
2. 토카막 네트워크의 특징/기능은 다음과 같다:

   개요 (Overview)

   a. 초당 트랜잭션 수 및 가스 비용의 제한으로 인한 이더리움 블록체인의 확장성 문제를 해결하기 위해 설계된 L2 프로토콜이다. 좀 더 구체적으로는 이더리움 체인 외부에서 트랜잭션을 처리한 다음, 다수의 트랜잭션을 온체인에 일괄적으로 기록 및 저장한다.

   블록 검증 (Block verification)

   b. 옵티미스틱 롤업에서 사용자는“시퀀서”(아래 섹션 1 에서 정의됨) 에게 트랜잭션을 제출한다. 시퀀서는 옵티미스틱 롤업에서 트랜잭션 처리를 담당하는 노드이다. 시퀀서는 트랜잭션을 모아 관련 기초 데이터를 압축해 이더리움에 블록 형태로 기록 및 저장한다.

   c. 시퀀서는 일정량의“토큰”(아래 추가 설명 참조) 을“시퀀서 담보금”(아래 섹션 1 에 정의됨) 으로 설정해야 한다. 시퀀서가 유효하지 않은 블록을 제출하려 하거나 오래된 블록을 기초로 체인을 구축하려 한다면 시퀀서 담보금이 삭감될 수 있기 때문에 시퀀서의 부정직한 행동을 하지 못하도록 장려한다. 토카막 네트워크에서 수행하는 서비스에 대해 시퀀서는 새로 발행된 토큰인 시뇨리지를 보상으로 받는다. 해당 보상의 양은 시퀀서가 운영하는 L2 의 성장에 비례한다 (성장은 토카막 네트워크에서 토큰의 총 공급량 증가를 기준으로 계산됨). 시뇨리지 외에도 시퀀서들은 서로 다른 수수료 정책을 시행해 상이한 방식으로 사용자들로부터 보상을 받을 수 있다. (예: 토큰 또는 타 암호화폐)

   d. 옵티미스틱 롤업에서는 시퀀서가 트랜잭션 배치 (batch, 묶음) 를 이더리움 블록체인에 제출할 때 사용자가 이에“챌린지”(아래 섹션 1 에 정의됨) 할 수 있다. “챌린지 기간”(아래 섹션 1 에 정의된 대로“DTD”라고 함) 은 7~14 일이 주어지

며, 이 기간 동안 사용자는“사기 증명 (fraud proof)”을 계산해 챌린지를 수행할 수 있다. (이 때 백서 3.1.2. 에서 설명된 것과 같이“최소 챌린지 비용”이 담보로 설정되어야 한다.) 시퀀서가 챌린지를 받는 경우, 배치가 유효하게 제출되었는지 여부에 따라 시퀀서 또는 챌린저는 각각 시퀀서 담보금 또는 최소 챌린지 비용을 잃게 되며, 승리한 당사자는 패한 당사자의 삭감된 토큰을 획득한다.

e. 시퀀서나 챌린저가 아닌 사용자 (즉, 트랜잭션 처리 서비스를 제공하거나 사기 증명을 계산하는 데에 관여하지 않는 사용자) 는 최소 챌린지 비용을 담보로 설정하고 시퀀서 또는 챌린저를“지지”함으로써 블록 검증 프로세스에 참여할 수 있다. 이 때 해당 사용자들은 시퀀서 혹은 챌린저가 블록 검증 프로세스에서 얻었을 보상 (예: 시뇨리지 및 / 또는 슬래시 된 토큰) 과 페널티 (예: 잘못된 블록 제출 혹은 유효하지 않은 챌린지로 인한 삭감) 를 공유할 수도 있다. 좀 더 명확히 하자면, 시퀀서 또는 챌린저를“지지”하는 행위는 사용자가 취해야 하는 적극적인 조치이다. 사용자는 토카막 네트워크에서 수동적인 토큰 보유자로 남아 챌린지에“지지자”로 참여하지 않을 수 있다. 챌린지와 관련되어 묶인 혹은 동결된 토큰은 토카막 네트워크에 대한 적극적인 참여를 장려하기 위한 것이며, 토큰이 동결되어 있는 동안 회사는 이를 사용하거나 수익화하지 않는다.

f. 위 내용에도 불구하고, 사용자가 토큰을 스테이킹했지만 위에서 설명한 블록 검증 활동에 참여하지 않는 경우 (즉, 챌린지에서 시퀀서 혹은 챌린저도 아니면서 시퀀서와 챌린저 중 아무도 지지하지 않는 경우), 스테이킹된 토큰의 일부가 삭감된다. 이는 토카막 네트워크의 블록 검증 활동에 대한 적극적인 참여를 장려하기 위함이다.

빠른 출금 및 유동성 공급자 (Fast withdrawals and liquidity providers)

g. 옵티미스틱 롤업 프로토콜에서 사용자가 L1 에서 L2 로 자산을 보내기 위해서는 우선 L1 자산을 L1 토큰 브릿지로 전송해야 한다. L1 자산은 L1 토큰 브릿지에 묶이게 되고 이를 바탕으로 시퀀서가 L2 토큰 브릿지로 하여금 동일한 양의 자산을 L2 에 발행하게 한다.

h. 사용자가 이더리움 (L1) 에 묶인 자산을 인출하기 위한 트랜잭션을 발생시키면 위에서 말한 과정이 반대로 진행된다. 사용자는 L2 토큰 브릿지에 L2 자산을 보내고 L2 출금 요청을 해야 한다. 이는 시퀀서에 의해 처리될 것이고, 위에서 언급한 DTD 기간이 적용된다. DTD 기간 동안 성공적인 챌린지가 없는 경우, 출금 요청은 시퀀서에 의해 L1 토큰 브릿지로 전달된다. 출금 요청된 자산이 L1 에서 풀릴 것이고, 이에 대응되는 L2 토큰 브리지의 자산은 소각된다.

i. 상기에 언급한 DTD 기간으로 인해 토카막 네트워크는 사용자가 빠른 출금 서비스 제공자가 될 수 있게끔 허용한다. 빠른 출금 서비스 제공자는 보류 중인 출금 요청에 대한 수취인의 자격을 얻어 빠른 출금 요청자에게 소정의 수수료를 대가로 L1 유동성을 제공한다. 이를 통해 빠른 출금 요청자는 DTD 를 기다리지고 않고 신속하게 출금을 완료할 수 있다. 회사는 빠른 출금 서비스 제공자 역할을 수행하지 않는다.

j. 사용자들은 스스로 빠른 출금 서비스 제공자 역할을 하는 것 외에 L1 에 토큰을 스테이킹하여 위에서 언급한 빠른 출금 서비스 제공자에게 유동성을 제공할 수 있다. 이 때 빠른 출금 서비스 제공자들은 해당 스테이커들을 위해 자체적인 보상 구조를 만들 수도 있다.

3. “토큰”은 토카막 네트워크의 네이티브 토큰 (native token) 이다. 토큰은 다음과 같은 용도로 사용될 수 있다:

    a. 토카막 네트워크의 시퀀서에게 수수료로 지불될 수 있다;

    b. 블록 검증 프로세스와 관련해서 시퀀서 담보금 및/또는 최소 챌린지 비용으로 사용될 수 있다.
    (챌린지에서 시퀀서, 챌린저 또는 시퀀서/챌린저 중 한 주체를 지지하는 사용자로서)

    c. 사용자가 빠른 출금 서비스를 제공하기 위해 활용하거나 다른 빠른 출금 서비스 제공자에게 스테이킹될 수 있다.

4. 토큰 생성 기간 동안 토큰은 회사로부터 직접 구매할 수 있었지만 현재는 그렇지 않다. 현재 토큰은 (i) 블록 검증 프로세스 참여에 대한 보상을 수령하거나 (시퀀서, 챌린저 또는 이들 중 한 주체를 지지하는 사용자로서); (ii) (만약 가능할 경우) 제 3 자 암호화폐 거래소에서 토큰을 구매함으로써 얻을 수 있다.

5. 토큰은 법정화폐 또는 기타 암호화폐로 회사에 상환되거나 판매할 수 없다.

6. 토큰 보유자는 토큰을 소유함으로써 회사 자산에 대한 직간접적인 소유권을 갖지 않는다.

7. 토큰은 보유자에게 특정한 투표권을 부여하지만 이는 온체인에서 실행되는 선거 및 제안으로 제한된다. (“온체인 투표권”) 이와 같은 온체인 투표권은 회사의 직원/주주에게 부여되는 권리, 회사의 경영 결정에 관한 투표권 (예: 회사의 자본금, 이사, 정관 또는 배당 변화와 관련된 결정), 토카막 네트워크 또는 회사의 이익이나 수익에 대한 권리와 같지 않다. 온체인 투표권은 다음과 관련된 사안에 대한 투표로 제한된다: (i) 네트워크 업그레이드 및 개선; (ii) 토카막 네트워크의 특정 프로젝트 또는 이니셔티브에 자금 또는 자원을 할당하기 위한 커뮤니티 제안; (iii) 토카막 네트워크 프로토콜의 변경; (iv) 토카막 네트워크에서 다른 토큰 지원; (v) 토카막 네트워크의 거버넌스 구조 변경

0. TL;DR

레이어 2(layer 2) 는 레이어 1(layer 1) 의 느린 트랜잭션 (transaction) 처리 속도를 보완하고자 등장한 기술이다. 블록체인의 계산 자원을 소모하는 활동이 트랜잭션인데 이를 처리하는 것은 레이어 2 에서 하되 레이어 1 은 그 유효성을 담보함으로써 속도를 높인다. 레이어 2 를 구현하는 기술에는 옵티미스틱 롤업 (Optimistic rollup), ZK 롤업 (Zero-Knowledge rollup), Validium 등이 있다. 현재는 아비트럼 (Arbitrum) 과 옵티미즘 (Optimism) 과 같이 옵티미스틱 롤업을 활용한 프로토콜들이 레이어 2 시장의 약 80% 를 차지하고 있다. 옵티미스틱 롤업은 레이어 2 에서 처리된 여러 트랜잭션을 한 묶음으로 만들어 레이어 1 에 제출하는데, 사용자들이 특별히 이의를 제기하지 않는 한 제출된 트랜잭션 데이터가 유효하다고 간주한다.

토카막 네트워크 (Tokamak Network) 는 옵티미즘에 기반해 사용자들에게 필요한 레이어 2 블록체인이 안정적으로 형성될 수 있는 환경을 조성하고자 한다. 이 때 옵티미스틱 롤업에 기초한 여타 프로토콜들과 비교했을 때 경쟁력을 갖추기 위해 네이티브 토큰 (native token) 인 톤 (TON) 의 유용성 (utilities) 을 극대화하기 위해 노력하고 있다. 예를 들어, 이전 연구에서는 신규 발행되는 톤, 즉 톤 시뇨리지 (seigniorage) 가 어떻게 레이어 2 의 성장을 돕는 동시에 네이티브 토큰이 레이어 2 수수료 토큰으로 활용될 수 있는 토대를 마련할 수 있는지 살펴봤다.

이 글에서는 기존 스테이킹 서비스를 업그레이드함으로써 레이어 2 환경에서의 톤의 유용성을 좀 더 확장하는 것에 대해 논의하려고 한다. 우선 이전 연구에서 살펴봤던 것과 같이 톤 시뇨리지를 통해 시퀀서 (sequencer) 의 성과를 보상함으로써 레이어 2 의 양적/질적 성장을 촉진할 수 있다. 이를 바탕으로 레이어 2 수수료 토큰 딜레마를 완화해 네이티브 토큰이 레이어 2 수수료 토큰으로 쓰일 수 있는 기초를 다진다. 결과적으로 토카막 네트워크의 레이어 2 블록체인들이 자생 경제를 확립해 지속가능한 성장을 할 수 있도록 돕는다.
또한, 톤은 챌린지에서의 보상 및 페널티와 빠른 출금 (fast withdrawal) 의 매개체로 작용해 스테이커들이 레이어 2 안정성에 기여하도록 자극한다. 챌린지에서의 보상 및 페널티를 통해 좀 더 균형잡힌 스테이킹 인센티브를 구축하면 스테이커들이 책임감있게 검증 작업을 수행할 수 있도록 자극할 수 있다. 여기에 스테이커들이 제공하는 빠른 출금 서비스까지 더해져 검증자의 딜레마를 완화해 더 안전한 레이어 2 환경을 조성할 수 있다.

1. 용어 정의 (Terminology)

- 스테이킹 (Staking): 토큰을 상응하는 컨트랙트로 이전해 네트워크의 보안에 기여하고 시뇨리지를 획득하는 행위이다. 이 문건에서는 레이어 1 상에서의 스테이킹만 다룬다.
- 언스테이킹 (Unstaking): 스테이킹된 토큰을 회수하는 행위이다.
- 시뇨리지 (Seigniorage): 특정 화폐의 액면 가치와 발행 비용의 차이를 뜻한다. 예를 들어, 톤의 발행 비용은 사실상 제로이기 때문에 톤 시뇨리지는 신규 발행된 톤의 개수와 같다.
- 인플레이션 (inflation): 신규 화폐 발행량 / 총 화폐 발행량
- 예치 (Deposit): 사용자가 레이어 1 에서의 토큰 잔액을 레이어 2 로 옮기는 행위이다.
- 시퀀서 (Sequencer): 레이어 2 트랜잭션 (transaction) 을 처리해 블록을 생성하고 관련 데이터를 레이어 1 에 제출하는 주체를 뜻한다.

- 시퀀서 담보금 (Sequencer collateral): 시퀀서가 레이어 2 를 개설할 때 담보 형태로 묶어두는 자산을 의미한다.
- 챌린지 (Challenge): 임의의 주체가 챌린지 기간 동안 레이어 1 으로 넘어가는 레이어 2 트랜잭션 데이터를 검증하는 행위이다.
- 챌린지 기간 (DTD, Dispute Time Delay): 임의의 주체가 레이어 1 으로 넘어가는 레이어 2 트랜잭션 데이터를 검증할 수 있는 기간을 뜻한다.
- 출금 (Withdraw): 사용자가 레이어 2 에서의 토큰 잔액을 레이어 1 으로 옮기는 행위이다.
- 일반 출금 (Standard Withdrawal): 챌린지 기간 경과 후 완료되는 출금을 의미한다.
- 빠른 출금 (Fast Withdrawal): 챌린지 기간 경과 전 완료되는 출금을 의미한다.
- 사기 증명 (Fraud proof): 트랜잭션에 의한 상태 이전이 유효하지 않음을 증명하는 것을 의미한다,
- 유효성 증명 (Validity proof): 트랜잭션에 의한 상태 이전이 유효함을 증명하는 것을 의미한다.

  특별히 언급하지 않는 한, 이 노트에서'토큰', '화폐', '자산'등은 모두 톤을 의미한다. 예를 들어, 스테이킹은 톤 스테이킹이고 예치금은 톤 예치금인 것이다. 이는 논의를 최대한 단순하게 하기 위함이다.

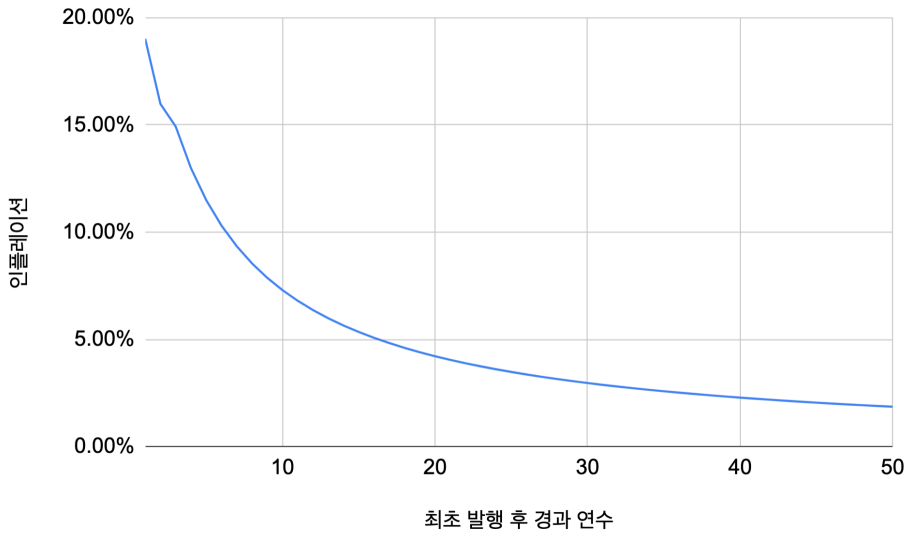
2. 시뇨리지 (Seigniorage)

토카막 네트워크에서 톤 시뇨리지는 레이어 2 성장의 촉매제로 작용한다. 레이어 2 가 확장을 거듭하면서 네이티브 토큰이 수수료 토큰으로 사용될 수 있는 토대가 마련된다. 한 마디로 톤은 레이어 2 블록체인이 자생 경제를 확립해 지속가능한 성장을 할 수 있도록 돕는다.

2.1. 시뇨리지 발생 (Seigniorage generation)

이더리움 블록당 3.92 톤이 신규 발행된다. 여기서 주목할 점은 2022 년 9 월 15 일 완료된 머지 (Merge) 를 기점으로 이더리움 블록 생성 시간이 달라졌기 때문에 연간 톤 신규 발행량, 즉 연간 시뇨리지에도 변화가 있었다는 것이다. 머지 이전에는 평균 13 초마다 이더리움 블록이 생성됐기 때문에 연간 약 9,509,317 톤에 해당하는 시뇨리지가 발생했다. 하지만 머지 이후로는 블록 생성 시간이 12 초로 고정됐기 때문에 연간 시뇨리지가 10,301,760 톤으로 늘어났다.

최초 발행량이 50,000,000 톤이기 때문에 최초 인플레이션은 약 19.0%(9,509,317 / 50,000,000) 이다. 인플레이션은 최초 발행 후 10 년 후에는 약 7.3%, 50 년 후에는 약 1.9% 까지 하락한다.



2.2. 시뇨리지 분배 (Seigniorage distribution)

시뇨리지를 분배한다는 것은 신규 발행된 톤을 나눠주는 것이다. 다시 말해, 톤 공급량 증가에 따른 이익 및 불이익을 조정하는 것이다.

논의를 단순화하기 위해 다음과 같은 사항들을 가정한다:

1. 시뇨리지는 일정 주기마다 지급된다.
2. 레이어 2 는 단 하나만 존재한다.

2.2.1. 톤 스테이킹 V1(TON staking V1)

현재 토카막 네트워크가 운영 중인 스테이킹 서비스가 바로 스테이킹 V1 이다.

스테이킹 V1 에서 시뇨리지는 각 주체에게 다음과 같이 분배된다:

스테이커: $(\frac{S}{T} + W_S * \frac{T-S}{T}) * Seig$
톤 다오: $W_D * \frac{T-S}{T} * Seig$
sTOS 보유자: $W_P * \frac{T-S}{T} * Seig$

- T: 톤 총 공급량
- S: 스테이킹 총량
- $Seig$: 일정 기간 동안 발생한 시뇨리지
- W_S, W_D, W_P: 스테이커 / 톤 다오 (TON DAO) / sTOS 보유자들에게 분배되는 시뇨리지 가중치 $(W_S + W_D + W_P \leq 1)$

논의를 단순화하기 위해 W_S = 1, W_D = W_P = 0 으로 가정하면 시뇨리지는 전부 스테이커에게 귀속된다:

스테이커: $(\frac{S}{T} + 1 * \frac{T-S}{T}) * Seig$ = $Seig$
톤 다오: $0 * \frac{T-S}{T} * Seig$ = 0
sTOS 보유자: $0 * \frac{T-S}{T} * Seig$ = 0

2.2.2. 톤 스테이킹 V2(TON staking V2)

레이어 2 환경이 확립되면 스테이킹 V1 이 스테이킹 V2 로 업그레이드될 것이다. 스테이킹 V2 에서의 시뇨리지 분배에서 달라지는 점은 시퀀서가 레이어 2 성장에 비례해 시뇨리지 수익을 얻을 수 있다는 것이다. 예를 들어, $Seig$ 를 다음과 같이 분배할 수 있다:

시퀀서: $\frac{D+C}{T} * Seig$ = $\frac{T_{L2}}{T} * Seig$
스테이커: $\frac{T-D-C}{T} * Seig$ = $\frac{T-T_{L2}}{T} * Seig$ = $\frac{T_{L1}}{T} * Seig$

- D: 예치금 총량
- C: 시퀀서 담보금
- $T_{L2} \equiv D + C$: 레이어 2 톤 공급량
- $T_{L1} \equiv T - D - C = T - T_{L2}$: 레이어 1 톤 공급량

2.3. 레이어 2 의 지속가능한 성장 (Sustainable growth of L2)

톤 시뇨리지는 레이어 2 의 외연 확장을 촉진하는 동시에 레이어 2 수수료 토큰 딜레마를 완화함으로써 레이어 2 가 지속가능한 성장을 구가하게 해준다.

2.3.1. 레이어 2 의 양적/질적 성장 (Quantative/Qualitative growth of L2)

2.3.1.1. 레이어 2 의 양적 성장 <=> 시퀀서 시뇨리지의 양적 증가 시퀀서에게는 예치금 및 시퀀서 담보금을 키워 시뇨리지를 극대화할 유인이 존재한다. 이는 레이어 2 의 양적 성장으로 이어질 수 있다. 레이어 2 의 TVL(Total Value Locked) 이 증가한다고도 이해할 수 있다.

2.3.1.2. 레이어 2 의 질적 성장 <=> 시퀀서 시뇨리지의 질적 개선 시뇨리지의 절대적 크기 못지 않게 중요한 것이 바로 질 (quality) 이다. 예를 들어, 레이어 2 에 단 한 명의 예치자만 있다면 여기서 파생되는 시뇨리지는 불안정하다. 해당 예치자가 출금하면 시퀀서가 수취하는 시뇨리지가 급감할 것이기 때문이다.

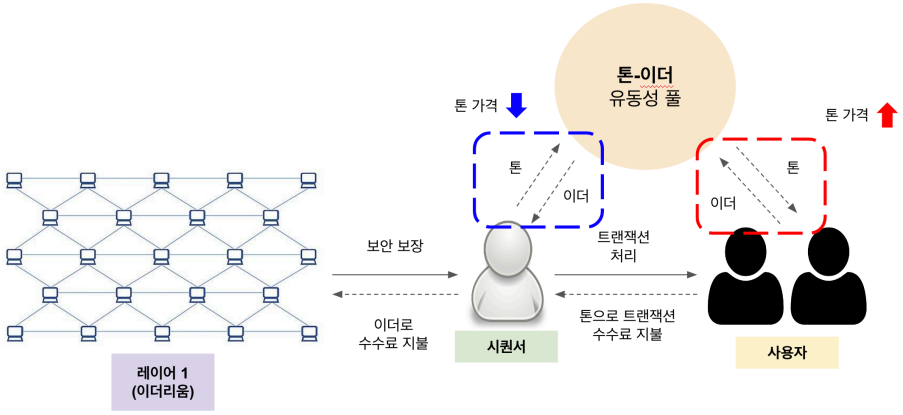
이는 레이어 2 의 질적 성장과도 직결되는 이슈이다. 레이어 2 유동성이 소수의 예치자에게 집중되면 활발한 트랜잭션 발생이 저해되어 레이어 2 UX(User Experience) 가 악화될 것이기 때문이다.

결과적으로 시퀀서는 시뇨리지의 질적 개선을 위해 많은 예치자를 유치하기 위해 노력할 것이고, 이는 레이어 2 의 질적 성장으로 이어질 것이다.

2.3.2. 레이어 2 수수료 토큰 딜레마 완화 (Alleviation of L2 fee token dilemma)

> 해당 섹션은 https://github.com/Onther-Tech/economics/blob/main/Tokamaklayer2.md 를 참고하고 있다.

레이어 2 가 시뇨리지에 힘입어 양적/질적 성장을 이룩하면 레이어 2 의 고질적 문제가 해결될 수 있다. 그'고질적 문제'란 바로'레이어 2 수수료 토큰 딜레마'다.



(출처: How to unravel fee token dilemma in layer 2 by Wyatt Park)

예를 들어, 톤을 레이어 2 수수료 토큰으로 사용할 경우 톤의 수요는 크게 증가할 수 있다. 레이어 2 트랜잭션을 실행할 때마다 톤이 필요할 것이기 때문이다. 하지만 이는 동전의 한 단면에 불과하다. 레이어 2 는 보안을 위해 레이어 1 에 트랜잭션 데이터를 제출하는데 이때 소정의 수수료가 부과된다. 이 수수료 (레이어 1 보안 수수료) 는 이더로만 낼 수 있기 때문에 설사 레이어 2 트랜잭션 수수료로 톤을 받더라도 곧바로 되팔아야 할 수도 있다. 다시 말해, 레이어 2 트랜잭션 수수료를 통한 수요 증가 효과가 레이어 1 보안 수수료로 인한 공급 증가 효과로 인해 상쇄되는 것이다. 이를 레이어 2 수수료 토큰 딜레마라고 한다.

여기서 주목할 점은 레이어 2 사용자 유치를 장려하는 시뇨리지 분배를 통해 딜레마가 완화될 수 있다는 것이다. 시뇨리지 수익에 자극받은 시퀀서가 많은 사용자들을 레이어 2 로 끌어들이면 평균적인 레이어 2 트랜잭션 수수료 수입 외의 수익이 창출될 수 있기 때문이다. 시퀀서의 유연한 수수료 정책이나 유용한 댑 (Dapp) 으로부터 발생하는 현금 흐름이 대표적인 예시라고 할 수 있다. 즉, 시퀀서는 레이어 2 트랜잭션 수수료로 받은 네이티브 토큰 (위 예시에서는 톤) 을 매도하지 않고도 부가 수입을 통해 레이어 1 보안 수수료를 충당할 수 있을 것이다.

3. 검증 경제 (Verification economics)

스테이킹 V2 에서 톤은 레이어 2 의 성장 뿐만 아니라 보안에도 기여한다. 좀 더 구체적으로는 톤이 챌린지에서의 보상/페널티의 매개체로써 작용해 스테이커들로 구성된 상시 감시 체계를 구축한다. 더 나아가 스테이킹 및 스테이킹을 활용한 빠른 출금은 검증자의 딜레마를 누그러뜨려 레어어 2 보안을 더욱더 견고히 한다.

3.1. 챌린지 (Challenge)

3.1.1. 개요 (Overview)

레이어 2 의 보안은 구조적으로 시퀀서에 크게 의존하고 있다. 강력한 경제적 인센티브 구조 및 다수의 검증자를 바탕으로 한 레이어 1 의 보안에 비해 취약하다고 할 수 있다. 따라서 이러한 단점을 보완하고자 레이어 2 트랜잭션 데이터를 레이어 1 에 제출해 저장하는 것이다. 이 때, 레이어 1 에 넘어가기 전 레이어 2 트랜잭션 데이터의 유효성을 담보하기 위한 행위가 바로 챌린지이다. 챌린지 기간 동안 임의의 주체가 레이어 2 에서 레이어 1 으로 넘어가는 트랜잭션 데이터를 검증하는 것이다.

물론'임의의 주체'의 선의에만 기댄 보안은 본질적으로 불안할 수밖에 없다. 따라서 업그레이드된 스테이킹 서비스에서는 스테이커들이 챌린지를 주도하게끔 인센티브 구조가 설계될 것이다.

3.1.2. 절차 (Procedure)

토카막 네트워크에서 챌린지는 다음과 같이 진행될 것으로 기대된다:

1. 시퀀서가 레이어 2 블록을 레이어 1 에 제출한다.

2. 챌린저는"최소 챌린지 비용"을 담보로 설정한 후, 시퀀서와 해당 블록에 대한 유효성을 검증하기 위한 질의응답을 진행한다. - 만약 답이 잘못됐거나 사전에 정해진 기간 내에 응답을 하지 못할 경우 챌린지에서 패한다. - 승패가 가려지기까지 약 7-14 일이 소요된다 (DTD 와 동일하거나 약간 짧음).

3. 챌린저가 아닌 스테이커 역시 챌린지에 참여할 수 있다 (그룹 챌린지). - 최소 챌린지 비용 이상의 담보를 설정할 때 그룹 챌린지에 참여할 수 있다. - 이 때 스테이커는 챌린저, 시퀀서 중 하나의 그룹에 동참할 수 있다.

4. 결과

- 챌린저가 승리할 경우:
  - 챌린저가 시퀀서 자격을 승계한다 (시퀀서 담보금 포함).
  - 챌린저의 편에 선 스테이커들의 자산 변동은 없다. 다만, 상황에 따라서 챌린저가 획득한 시퀀서 담보금을 나눠가질 수도 있다.
  - 시퀀서는 자격을 박탈당한다.
  - 시퀀서의 편에 선 스테이커들은 담보로 설정한 최소 챌린지 비용을 몰수당하는 동시에 스테이킹 지분이 삭감된다.
  - 챌린지에 아예 참여하지 않은 스테이커들의 지분 일부가 삭감된다.
- 시퀀서가 승리할 경우:
  - 시퀀서의 자산 변동은 없다.
  - 시퀀서의 편에 선 스테이커들의 자산 변동은 없다.
  - 챌린저 및 챌린저의 편에 선 스테이커들은 담보로 설정한 최소 챌린지 비용을 몰수당하는 동시에 스테이킹 지분이 삭감된다.
  - 챌린지에 아예 참여하지 않은 스테이커들의 지분 일부가 삭감된다.

5. 특이 사항 - 다음 조건이 충족되면 챌린지가 발생할 경우 시퀀서는 곧바로 패배한다.

- DTD 내에 커밋이 일어나지 않는 경우

3.2. 빠른 출금 (Fast Withdrawal)

3.2.1. 개요 (Overview)

빠른 출금은 챌린지 기간 경과 전 완료되는 출금을 의미한다.

앞서 설명했듯이 임의의 주체가 챌린지를 시작하고 챌린지 기간 동안 레이어 2 트랜잭션의 유효성을 따질 수 있다. 이말인즉슨, 원칙적으로는 챌린지 기간이 끝나기 전까지 레이어 2 트랜잭션의 유효성을 담보할 수 없다는 것이다. 따라서 출금을 요청한 사용자는 챌린지 기간 동안 출금하려고 하는 레이어 2 자산에 대응되는 레이어 1 자산에 접근할 수 없다. 이러한 구조적 특성에서 기인하는 불편을 경감시키고자 나온 것이 바로 빠른 출금이다.

3.2.2. 자금 원천 (Source of liquidity)

챌린지 기간 동안 출금하고자 하는 레이어 2 자산에 대응되는 레이어 1 자산에 접근할 수 없기 때문에 예치금을 제외한, 빠른 출금만을 위한 유동성 확보가 필수적이다.

스테이킹 V1 이 V2 로 개편되면 외부적으로 조성된 유동성 풀뿐만 아니라 스테이킹된 톤도 빠른 출금을 위한 유동성으로 활용될 수 있다. 스테이킹 보상과 빠른 출금 수수료가 스테이커들로 하여금 빠른 출금 서비스를 제공하도록 자극할 것이다. 추가적으로 빠른 출금 시 챌린지 기간 동안의 스테이킹 보상을 보전해줌으로써 스테이커가 부담해야 하는 리스크를 줄이려고 한다.

3.3. 검증자의 딜레마 (Verifiers'dilemma)

> 해당 섹션은 https://medium.com/onther-tech/optimistics-not-secure-enough-than-you-think-46bf93d80292 다루는 Super-Simple Model in Optimistic Rollup 을 차용한다.

3.3.1. 개요 (Overview)

챌린지에서 보상 및 처벌을 도입하는 것과 별개로 그 상대적 크기를 정하는 것도 매우 중요하다. 이 때 발생하는 문제가 바로'검증자의 딜레마'이다. 쉽게 말해, 검증 기대 보수가 비검증 기대 보수보다 크지 않을 경우 검증에 나서는 사람들이 없을 것이라는 의미다.

롤업에 이해 관계가 있는 단일 검증자가 챌린지를 할 수 있다고 가정할 때, Super-Simple Model in Optimistic Rollup 에서 검증/비검증 기대 보수는 다음과 같다:

검증 기대 보수: $X * C + VR - VC$
비검증 기대 보수: $-X * L + (1 - X) * VR$

- C: 시퀀서 보증금 (담보금), 검증자가 검증에 성공할 시 검증자에게 보상으로 주어진다.
- L: 롤업에 예치된 검증자의 자산, 검증자가 검증에 실패할 시 시퀀서에게 보상으로 주어질 수 있다.
- X: 시퀀서가 공격할 확률
- VC: 검증 비용
- VR: 검증 단위당 검증자가 얻는 수익 (안전한 레이어 2 로부터 얻을 수 있는 수익)

식을 정리하면 $X > \frac{VC}{C+L+VR}$ 일 때 검증 기대 보수가 비검증 기대 보수보다 커지는 것을 알 수 있다. 반대로 말하면, $X \leq \frac{VC}{C+L+VR}$ 이면 검증자의 딜레마가 발생한다고도 이해할 수 있다. 여기서 주목할 점은 검증자의 딜레마를 완전히 해소하기는 힘들다는 것이다. 예를 들어, $VC \geq C + L + VR$ 이면 항상 검증자의 딜레마가 발생한다. $0 \leq X \leq 1 \leq \frac{VC}{C+L+VR}$ 이기 때문이다. 반대로 $VC < C + L + VR$ 이면 VC, C, L, VR 이 음수가 될 수 없음을 고려할 때 시퀀서는 $0 < X_A \leq \frac{VC}{C+L+VR}$ 를 만족하는 X_A 를 찾을 수 있다.

단일 검증자가 아닌 복수의 검증자가 존재하더라도 상황은 크게 달라지지 않는다. 복수의 검증자가 챌린지를 할 수 있다고 상정할 때 특정 검증자의 검증/비검증 기대 보수는 다음과 같다 (여기서 C 는 챌린지에 참여한 검증자들이 동일하게 나눠 갖는다고 가정한다):

검증 기대 보수: $\frac{X*C}{N} + VR - VC$
비검증 기대 보수: $-X * Y * L + (1 - X * Y) * VR$

- N: (검증자 본인을 포함한) 검증을 수행하는 검증자 수
- Y: 검증자 본인을 제외한 다른 검증자들 중 단 한 명도 검증을 수행하지 않을 확률

검증자 본인을 제외한 다른 검증자들이 검증을 하지 않는 경우 $(N = 1, Y = 1)$ 검증/비검증 기대 보수는 다음과 같다:

검증 기대 보수: $X * C + VR - VC$
비검증 기대 보수: $-X * L + (1 - X) * VR$

단일 검증자를 가정했을 때와 같이 $X > \frac{VC}{C+L+VR}$ 일 때 검증을 수행할 경제적 유인이 생긴다.

모든 검증자들이 검증을 수행하는 경우 $(N = \text{검증자 수} = N_v, Y = 0)$ 검증/비검증 기대 보수는 다음과 같다:

검증 기대 보수: $\frac{X*C}{N_v}$ + VR - VC
비검증 기대 보수: VR

즉, $X > \frac{N_v*VC}{C}$ 일 때 검증을 수행할 경제적 유인이 생긴다.

만약 일부 검증자들만 검증을 한다면 기준값은 $\frac{VC}{C+L+VR}$ 와 $\frac{N_v*VC}{C}$ 사이에 있을 것임을 어렵지 않게 추론할 수 있다.

결론은 다음과 같이 요약할 수 있다:

1. $X > \frac{N_v*VC}{C}$: 모든 검증자가 검증을 수행함
2. $\frac{VC}{C+L+VR} < X \leq \frac{N_v*VC}{C}$: 일부 검증자가 검증을 수행할 수 있음
3. $X \leq \frac{VC}{C+L+VR}$: 아무도 검증을 수행하지 않음

즉, 단일 검증자가 존재하는 상황과 마찬가지로 $\frac{VC}{C+L+VR} \geq 1$ 이면 X 의 값과 상관 없이 검증자의 딜레마가 발생한다. 뿐만 아니라 $\frac{VC}{C+L+VR} < 1$ 라도 시퀀서가 X 를 $\frac{VC}{C+L+VR}$ 보다 작게 조절할 수 있기 때문에 검증자의 딜레마를 완전히 없애는 것은 현실적으로 매우 어렵다.

결국 L2 보안을 제고하기 위한 최선의 방책은 아무도 검증을 하지 않게끔 하는 X 의 최대값 (해당 모델에서는 $\frac{VC}{C+L+VR}$) 을 작게 만드는 것이다. 토카막 네트워크는'스테이킹 및 스테이킹을 활용한 빠른 출금'을 통해 이 난제를 해결하고자 한다.

3.3.2. 검증자의 딜레마 완화 (Mitigation of verifiers'dilemma)

3.3.2.1. 기본 검증 모델 단일 검증자가 챌린지를 할 수 있다고 가정한 Super-Simple Model in Optimistic Rollup 에서의 검증/비검증 기대 보수를 다시 살펴보자:

검증 기대 보수: $X * C + VR - VC$
비검증 기대 보수: $-X * L + (1 - X) * VR$

- C: 시퀀서 보증금 (담보금), 검증자가 검증에 성공할 시 검증자에게 보상으로 주어진다.
- L: 롤업에 예치된 검증자의 자산, 검증자가 검증에 실패할 시 시퀀서에게 보상으로 주어질 수 있다.
- X: 시퀀서가 공격할 확률
- VC: 검증 비용
- VR: 검증 단위당 검증자가 얻는 수익 (안전한 레이어 2 로부터 얻을 수 있는 수익)

식을 정리하면 X > $\frac{VC}{C+L+VR}$ 일 때 검증을 할 경제적 유인이 생김을 알 수 있다. 반대로 말하면 시퀀서가 X 를 $\frac{VC}{C+L+VR}$ 이하로 낮춰야 검증자의 딜레마가 발생한다. 물론 이는 복수의 검증자를 가정하다라도 변하지 않는다.

3.3.2.2. 스테이킹 검증 모델

- 단일 검증자

이제 단순 이해 관계자가 아닌 스테이커들에게 검증의 책임을 지우는 구조를 생각해보자. 즉, 스테이커가 검증자가 되어 챌린지를 하는 것이다. 이 때 검증/비검증 기대 보수는 다음과 같다:

검증 기대 보수: $X * C + VR - VC$
비검증 기대 보수: $-X * A * S + (1 - X) * VR$

- S: 스테이킹된 톤
- A: 스테이킹 지분 삭감 비율

기본 모델과 유일한 차이점은 비검증 기대 보수에서 L 이 $A * S$ 로 바뀐 것이다. 스테이킹 보상은 검증과는 직접적인 연관이 없을 뿐더러 검증/비검증 기대 보수에 똑같이 적용되기 때문에 반영하지 않았다.

식을 정리하면 $X \leq \frac{VC}{C+A*S+VR}$ 일 때 검증자의 딜레마가 발생함을 알 수 있다. 기본 모델과 비교했을 때, $A * S$ > L 이면 스테이킹을 활용한 검증이 딜레마를 완화하는 데에 효과적임을 알 수 있다. 여기서 주목할 점은 해당 부등식을 만족시키자는 것이 단순히 이론적인 주장이 아닌, 실현 가능한 주장이라는 데에 있다. A 가 L 보다 프로토콜이 통제하기 쉬운 변수이기 때문이다.

- 복수 검증자

복수의 스테이커가 검증자로 존재할 때 특정 검증자의 검증/비검증 기대 보수는 다음과 같다 (여기서 C 은 챌린저인 스테이커와 챌린저는 아니지만 그룹 챌린지에 참여한 스테이커들이 동일하게 나눠 갖는다고 가정한다):

검증 기대 보수: $\frac{X*C}{N} + VR - VC$
비검증 기대 보수: $-X * A * S + (1 - X * Y) * VR$

- N: (검증자 본인을 포함한) 검증을 수행하는 검증자 수
- Y: 검증자 본인을 제외한 다른 검증자들 중 단 한 명도 검증을 수행하지 않을 확률

여기서 주목할 점은 다른 검증자들의 검증은 스테이킹된 톤의 삭감과는 무관하다는 것이다. 설사 다른 스테이커가 챌린지를 하더라도 거기에 동참하지 않으면 스테이킹된 톤은 줄어들 것이기 때문이다.

검증자 본인을 제외한 다른 검증자들이 검증을 하지 않는 경우 $(N = 1, Y = 1)$ 검증/비검증 기대 보수는 다음과 같다:

검증 기대 보수: $X * C + VR - VC$
비검증 기대 보수: $-X * A * S + (1 - X) * VR$

단일 검증자를 가정했을 때와 같이 $X > \frac{VC}{C+A*S+VR}$ 일 때 검증을 수행할 경제적 유인이 생긴다.

반면 모든 검증자들이 검증을 수행하는 경우 $(N = \text{검증자 수} = N_v, Y = 0)$ 검증/비검증 기대 보수는 다음과 같다:

검증 기대 보수: $\frac{X*C}{N_v} + VR - VC$
비검증 기대 보수: $-X * A * S + VR$

즉, $X > \frac{VC}{C/N_v+A*S}$ 일 때 검증을 수행할 경제적 유인이 생긴다.

만약 일부 검증자들만 검증한다면 기준값은 $\frac{VC}{C+A*S+VR}$ 와 $\frac{VC}{C/N_v+A*S}$ 사이에 있을 것임을 어렵지 않게 추론할 수 있다.

결론은 다음과 같이 요약할 수 있다:

1. $X > \frac{VC}{C/N_v+A*S}$: 모든 검증자가 검증을 수행함
2. $\frac{VC}{C+A*S+VR} < X \leq \frac{VC}{C/N_v+A*S}$: 일부 검증자가 검증을 수행할 수 있음
3. $X \leq \frac{VC}{C+A*S+VR}$: 아무도 검증을 수행하지 않음

역시 A 를 충분히 키움으로써 아무도 검증을 수행하지 않게 하는 X 의 최댓값을 낮출 수 있다.

3.3.2.3. 스테이킹 & 빠른 출금 검증 모델

- 단일 검증자

만약 스테이커들이 검증자로서 챌린지를 할뿐만 아니라 빠른 출금까지 제공할 경우 검증 기대 보수 및 비검증 기대 보수는 다음과 같이 업데이트된다:

검증 기대 보수: $X * C + VR - VC$
비검증 기대 보수: $-X * (A * S + FW) + (1 - X) * VR$

- FW: 스테이커가 빠른 출금에 제공한 톤

스테이킹 검증 모델과 다른 점은 빠른 출금 (FW) 이 비검증 기대 보수에 추가됐다는 것이다. 스테이킹 보상과 마찬가지로 빠른 출금 수수료 역시 검증과 직접적으로 연관되어 있지 않고 검증/비검증 기대 보수에 동일하게 적용되기 때문에 고려하지 않았다.

식을 정리하면 $X \leq \frac{VC}{C+A*S+VR+FW}$ 일 때 검증자의 딜레마가 발생함을 알 수 있다. 빠른 출금에 제공한 톤이 비검증 기대 보수를 낮춰 일반 스테이커보다 검증을 할 가능성이 높아졌다고 볼 수 있다. $(\frac{VC}{C+A*S+VR} > \frac{VC}{C+A*S+VR+FW})$

- 복수 검증자

복수의 스테이커가 검증자로 존재하는 상황으로 일반화하면 빠른 출금을 제공한 특정 검증자의 검증/비검증 기대 보수는 다음과 같다 (여기서 C 은 챌린저인 스테이커와 챌린저는 아니지만 그룹 챌린지에 참여한 스테이커들이 동일하게 나눠 갖는다고 가정한다):

검증 기대 보수: $\frac{X*C}{N} + VR - VC$
비검증 기대 보수: $-X * (A * S + FW) + (1 - X * Y) * VR$

- N: (검증자 본인을 포함한) 검증을 수행하는 검증자 수
- Y: 검증자 본인을 제외한 다른 검증자들 중 단 한 명도 검증을 수행하지 않을 확률

스테이킹 검증 모델과 비슷하게 다른 검증자들이 빠른 출금을 제공한 검증자의 비검증 기대 보수에 미치는 영향은 미미하다. 스테이커가 챌린지에 참여하지 않을 경우 스테이킹된 톤은 다른 검증자들의 검증 여부와 상관없이 삭감될 수 있다. 또한, 빠른 출금은 다른 검증자들이 해당 트랜잭션을 검증하기도 전에 완료되기 때문에 철저히 검증자 본인의 검증에 의존할 수밖에 없다.

이전 모델들에서 활용한 논리를 그대로 적용하면 다음과 같은 결론을 얻을 수 있다:

1. $X > \frac{VC}{C/N_v+A*S+FW}$: 모든 검증자가 검증을 수행함
2. $\frac{VC}{C+A*S+VR+FW} < X \leq \frac{VC}{C/N_v+A*S+FW}$: 일부 검증자가 검증을 수행할 수 있음
3. $X \leq \frac{VC}{C+A*S+VR+FW}$: 아무도 검증을 수행하지 않음

여전히 스테이킹 검증 모델과 비교했을 때 아무도 검증을 수행하지 않게 하는 X 의 최댓값이 더 낮음을 알 수 있다. $(\frac{VC}{C+A*S+VR} > \frac{VC}{C+A*S+VR+FW})$

3.3.2.4. 모델 간 비교

	기본 검증 모델	스테이킹 검증 모델	스테이킹 & 빠른 출금 검증 모델
검증자의 딜레마를 촉발하는 X 의 최댓값	$\frac{VC}{C+L+VR}$	$\frac{VC}{C+A*S+VR}$	$\frac{VC}{C+A*S+VR+FW}$

기본 검증 모델과 비교했을 때 스테이킹 검증 모델은 A 를 유연하게 조정함으로써 검증 인센티브를 보다 용이하게 통제할 수 있다. 스테이킹 & 빠른 출금 검증 모델은 FW 를 통해 비검증 기대 보수를 낮춤으로써 검증자의 딜레마를 완화하는 효과를 극대화할 수 있다.

4. 톤의 유용성 (Utilities of TON)

4.1. 레이어 2 의 지속가능한 성장 (Sustainable growth of L2)

톤 시뇨리지는 시퀀서가 레이어 2 의 양적/질적 성장에 기여할 수 있도록 인센티브를 제공한다. 시퀀서가 안정적인 시뇨리지 수익을 극대화하기 위해 많은 예치자로부터 많은 예치금을 유치하려 할 것이고, 이는 자연스럽게 레이어 2 확장으로 이어지는 것이다.
레이어 2 사용자 기반이 충분히 구축되면 시퀀서가 재량적 트랜잭션 수수료 정책, 부가가치가 높은 다양한 애플리케이션 등을 통해 평균적인 레이어 2 트랜잭션 수수료 외의 수입원을 확보할 수 있다. 레이어 2 가 이와 같은 추가적인 현금 흐름을 통해 레이어 1 보안 수수료를 지불하면 레이어 2 수수료 토큰 딜레마에 빠지지 않고 네이티브 토큰을 수수료 토큰으로 활용할 수 있게 된다.

결과적으로 토카막 네트워크에서의 레이어 2 블록체인은 외부 의존도를 줄인, 자생 경제를 확립할 수 있다.

4.2. 레이어 2 의 보안성 제고 (Enhanced L2 security)

우선 챌린지에서 톤을 매개체로 하는 인센티브 체계는 스테이커들이 레이어 2 운영 상황을 상시 감시할 수 있는 시스템을 마련한다. 스테이커들의 검증/비검증 기대 보수를 프로토콜이 유연하게 조정할 수 있기 때문에 일반적인 챌린지보다 검증 인센티브를 설계하기 용이하다.

추가적으로 스테이커들이 제공하는 빠른 출금 서비스는 검증자의 딜레마를 완화할 수 있다. 이는 빠른 출금의 경우 다른 검증자의 검증을 통한 효익을 누리기 어렵다는 사실에서 기인한다. 즉, 비검증에 대한 처벌이 훨씬 크기 때문에 빠른 출금을 제공한 스테이커는 검증을 통해 레이어 2 보안에 기여할 유인이 매우 크다고 할 수 있다.

5. 유효성 증명 (Validity Proof)

지금까지의 논의는 레이어 2 트랜잭션의 유효성을 증명할 별다른 기술적 수단이 존재하지 않는다고 가정했다. 예를 들어, 토카막 네트워크는 옵티미스틱 롤업의 사기 증명 (fraud proof) 에 기초해 스테이커들로 하여금 챌린지를 통해 잘못된 트랜잭션을 바로잡게 하려고 한다. 하지만 향후 영지식 증명 (zero-knowledge proof) 과 같은 유효성 증명이 등장할 경우, 레이어 2 트랜잭션 검증 과정이 한층 더 간소화될 것이다.

이는 톤의 유용성에도 영향을 미치는데 우선 빠른 출금이 사실상 사라진다는 것에 주목할 필요가 있다. 레이어 2 트랜잭션의 유효성을 따지는 데에 소요되는 시간이 대폭 줄어들거나 사라질 것이기 때문이다. 따라서 빠른 출금을 통해 검증 유인을 강화할 필요가 없어진다.
다만, 사기 증명 혹은 유효성 증명을 활용하는 것과 상관없이 스테이킹을 활용한 챌린지는

그대로 유지될 수 있다. 다시 말해, 톤이 챌린지를 통한 보상 및 페널티의 매개체로써 레이어 2 보안에 기여할 수 있다. 추가적으로 레이어 2 확장을 자극하는 시뇨리지 분배 시스템 역시 계속 남아있을 것으로 기대된다. 톤 시뇨리지가 레이어 2 의 양적/질적 성장을 촉진하는 동시에 레이어 2 수수로 토큰 딜레마를 완화함으로써 레이어 2 생태계의 지속가능한 성장을 위한 발판을 제공할 것이다.

6. 예시 (Examples)

6.1. 시뇨리지 분배 (Seigniorage distribution)

해당 예시에서는 다음과 같은 기호를 사용할 것이다: - T: 톤 총 공급량 - S: 스테이킹 총량 - $Seig$: 일정 기간 동안 발생한 시뇨리지 - D: 예치금 총량 - C: 시퀀서 담보금

이제 막 레이어 2 를 개설한 시퀀서를 생각해보자. 예를 들어, $Seig$ = 10 톤, T = 100 톤, D = 0 톤, C = 20 톤일 경우, $Seig$ 는 대부분 스테이커에게 귀속된다:

시퀀서: $\frac{D+C}{T} * Seig$ = $\frac{0+20}{100} * 10$ = 2 톤
스테이커: $\frac{T-D-C}{T} * Seig$ = $\frac{100-0-20}{100} * 10$ = 8 톤

만약 시퀀서가 수취하는 $Seig$ 을 늘리기 위해 더 많은 예치자를 모집해 D 가 30 톤까지 늘어나면 $Seig$ 는 시퀀서와 스테이커에게 다음과 같이 재분배된다:

시퀀서: $\frac{D+C}{T} * Seig$ = $\frac{30+20}{100} * 10$ = 5 톤
스테이커: $\frac{T-D-C}{T} * Seig$ = $\frac{100-30-20}{100} * 10$ = 5 톤

레이어 2 TVL 이 20 톤에서 50 톤으로 증가하면서 시퀀서에게 돌아가는 $Seig$ 역시 2 톤에서 5 톤으로 늘어났다.

만약 50 톤의 예치금이 L1 보안 수수료를 충당할 만큼 레이어 2 트랜잭션 수수료 외의 추가 수입을 창출한다면 시퀀서는 D 를 50 톤까지 키우려고 노력할 것이다:

시퀀서: $\frac{D+C}{T} * Seig$ = $\frac{50+20}{100} * 10$ = 7 톤
스테이커: $\frac{T-D-C}{T} * Seig$ = $\frac{100-50-20}{100} * 10$ = 3 톤

시퀀서가 수취하는 $Seig$ 가 5 톤에서 7 톤으로 더욱 증가했다. 또한, 50 톤의 D 를 기반으로 레이어 2 트랜잭션 수수료 외의 현금 흐름이 발생해 더 이상 수수료로 받은 네이티브 토큰을 팔 이유가 없어졌다. 레이어 2 수수료 토큰 딜레마를 피해갈 수 있는 것이다.

6.2. 검증 경제 (Verification economics)

6.2.1. 챌린지 (Challenge)

해당 예시에서는 다음과 같은 기호를 사용할 것이다: - C: 시퀀서 담보금 - S_A, S_B, S_C: 스테이커 A, B, C 가 각각 스테이킹한 톤 - $MinChal$: 최소 챌린지 비용 - A: 슬래싱(삭감) 비율

스테이커 A, B, C 총 3 명이 보안을 책임지는 레이어 2 를 생각해보자. C = 1000 톤, S_A = 200 톤, S_B = 300 톤, S_C = 500 톤, $MinChal$ = 100 톤, A = 30% 다.

이 때 시퀀서가 유효하지 않는 트랜잭션을 통해 공격을 감행했다. 스테이커들은 챌린지를 하지 않을 수도, 할 수도 있다. 만약 아무도 챌린지를 하지 않으면 각 주체의 자산 변동은 다음과 같다:

시퀀서: 0 톤
스테이커 A: $-S_A * A$ = $-200 * 0.3$ = -60 톤
스테이커 B: $-S_B * A$ = $-300 * 0.3$ = -90 톤
스테이커 C: $-S_C * A$ = $-500 * 0.3$ = -150 톤

이번에는 스테이커 A 가 챌린지 기간 동안 이의를 제기하고 스테이커 B 가 스테이커 A 의 편에 서서 챌린지에 참여한다고 가정하자. 반면에 스테이커 C 는 챌린지 과정에 아예 참여하지 않는다. 이 때 각 주체의 자산 변동은 다음과 같다:

시퀀서: $-C$ = -1000 톤
스테이커 A: $+C$ = +1000 톤
스테이커 B: +0 톤
스테이커 C: $-S_C * A$ = $-500 * 0.3$ = -150 톤

이 때 스테이커 C 가 챌린지에 참여하긴 하지만 시퀀서의 편에 설 경우 그 손실은 더 커진다:

시퀀서: $-C$ = -1000 톤
스테이커 A: $+C$ = +1000 톤
스테이커 B: +0 톤
스테이커 C: $-MinChal - S_C * A$ = $-100 - (500 * 0.3)$ = -250 톤

계산 결과에서 알 수 있듯이, 적절한 보상 및 처벌이 프로토콜 관점에서 바람직한 행동을 유발할 수 있다. 우선 시퀀서의 악의적 행위를 잡아낼 수 있다면 스테이커 A 와 같이 보상을 획득할 수 있다. 반대로 아무도 이의를 제기하지 않는다면 모든 스테이커의 자산 일부가 삭감된다. 추가적으로 누군가 챌린지를 하더라도 이에 참여하지 않으면 스테이커 C 와 같이 스테이킹된 톤 일부를 잃을 수 있다. 마지막으로 챌린지에 참여하더라도 편을 잘못 고르면 손실이 더욱 늘어날 수 있다.

6.2.2. 검증자의 딜레마 (Verifiers'dilemma)

논의를 단순하게 하기 위해 아래 예시들에서는 단일 검증자를 가정한다. 앞에서 살펴봤듯이 복수 검증자를 상정하더라도 결론은 동일하기 때문에 무리라고 보기 어렵다.

6.2.2.1. 기본 검증 모델 Super-Simple Model in Optimistic Rollup 에서의 검증/비검증 기대 보수는 다음과 같다:

검증 기대 보수: $X * C + VR - VC$
비검증 기대 보수: $-X * L + (1 - X) * VR$

- C: 시퀀서 보증금 (담보금), 검증자가 검증에 성공할 시 검증자에게 보상으로 주어진다.
- L: 롤업에 예치된 검증자의 자산, 검증자가 검증에 실패할 시 시퀀서에게 보상으로 주어질 수 있다.

- X: 시퀀서가 공격할 확률
- VC: 검증 비용
- VR: 검증 단위당 검증자가 얻는 수익 (안전한 레이어 2 로부터 얻을 수 있는 수익)

$C = 10$, $L = 10$, $VC = 20$, $VR = 10$ 이라 가정하면 검증/비검증 기대 보수를 같게 만드는 X 의 값은 $\frac{2}{3}$ 다:

검증 기대 보수: $\frac{2}{3} * 10 + 10 - 20 = -\frac{10}{3}$
비검증 기대 보수: $-\frac{2}{3} * 10 + (1 - \frac{2}{3}) * 10 = -\frac{10}{3}$

이 때 C 이나 L 을 늘려 검증 기대 보수를 키우려고 하면 검증자의 딜레마를 발생시키는 X 의 최댓값은 감소한다. 예를 들어, C 을 두 배로 증가시키면 검증/비검증 기대 보수를 같게 만드는 X 의 값은 $\frac{1}{2}$ 로 줄어든다.

검증 기대 보수: $\frac{1}{2} * 20 + 10 - 20 = 0$
비검증 기대 보수: $-\frac{1}{2} * 10 + (1 - \frac{1}{2}) * 10 = 0$

마찬가지로 L 을 두 배로 키우면 검증/비검증 기대 보수를 같게 만드는 X 의 값은 $\frac{1}{2}$ 로 하락한다:

검증 기대 보수: $\frac{1}{2} * 10 + 10 - 20 = -5$
비검증 기대 보수: $-\frac{1}{2} * 20 + (1 - \frac{1}{2}) * 10 = -5$

결과적으로 C 이나 L 을 증가시키면 검증자의 딜레마를 유발하는 X 의 최댓값이 감소함으로써 레이어 2 가 더 안전해진다. 다만, 프로토콜 입장에서 C 이나 L 은 통제하기 어려운 변수라는 한계가 있다.

6.2.2.2. 스테이킹 검증 모델 스테이킹 검증 모델에서 검증/비검증 기대 보수는 다음과 같이 수정된다:

검증 기대 보수: $X * C + VR - VC$
비검증 기대 보수: $-X * A * S + (1 - X) * VR$

- S: 스테이킹된 톤
- A: 스테이킹 지분 삭감 비율

기본 모델에서와 같이 $C = 10$, $VC = 20$, $VR = 10$ 이라 가정하고, $A = 0.1$, $S = 100$ 을 추가하면 검증/비검증 기대 보수를 같게 만드는 X 의 값은 $\frac{2}{3}$ 다 ($L = 10 = 0.1 * 100 = A * S$):

검증 기대 보수: $\frac{2}{3} * 10 + 10 - 20 = -\frac{10}{3}$
비검증 기대 보수: $-\frac{2}{3} * 0.1 * 100 + (1 - \frac{2}{3}) * 10 = -\frac{10}{3}$

A 를 두 배로 올리면 검증/비검증 기대 보수를 같게 만드는 X 의 값은 $\frac{1}{2}$ 이다:

검증 기대 보수: $\frac{1}{2} * 10 + 10 - 20 = -5$
비검증 기대 보수: $-\frac{1}{2} * 0.2 * 100 + (1 - \frac{1}{2}) * 10 = -5$

기본 검증 모델에서 $L = 10$, $L = 20$ 일 때의 결과와 동일한 것을 알 수 있다. 하지만 통제하기 쉬운 A 를 통해 좀 더 수월하게 같은 결과를 얻을 수 있다.

6.2.2.3. 스테이킹 & 빠른 출금 검증 모델 만약 스테이커들이 빠른 출금까지 제공할 경우 검증 기대 보수 및 비검증 기대 보수는 다음과 같이 업데이트된다:

검증 기대 보수: $X * C + VR - VC$
비검증 기대 보수: $-X * (A * S + FW) + (1 - X) * VR$

- FW: 스테이커가 빠른 출금에 제공한 톤

스테이킹 검증 모델에서와 같이 $C = 10$, $VC = 20$, $VR = 10$, $A = 0.1$, $S = 100$ 이라 가정하고 $FW = 100$ 을 추가하면, 검증/비검증 기대 보수를 같게 만드는 X 의 값은 $\frac{2}{13}$ 다:

검증 기대 보수: $\frac{2}{13} * 10 + 10 - 20 = -\frac{110}{13}$
비검증 기대 보수: $-\frac{2}{13} * (0.1 * 100 + 100) + (1 - \frac{2}{13}) * 10 = -\frac{110}{13}$

빠른 출금이 없는 스테이킹 검증보다 더 안전함을 알 수 있다. $(\frac{2}{3} > \frac{2}{13})$

이 때 A 를 두 배 인상하면 검증/비검증 기대 보수를 같게 만드는 X 의 값은 $\frac{2}{14} = \frac{1}{7}$ 로 떨어진다:

검증 기대 보수: $\frac{1}{7} * 10 + 10 - 20 = -\frac{60}{7}$
비검증 기대 보수: $-\frac{1}{7} * (0.2 * 100 + 100) + (1 - \frac{1}{7}) * 10 = -\frac{60}{7}$

역시 스테이킹 검증보다 더 안전하다. $(\frac{1}{2} > \frac{1}{7})$

6.2.2.4. 모델 간 비교 $C = 10$, $L = 10$, $VC = 20$, $VR = 10$, $A = 0.1$, $S = 100$, $FW = 100$ 을 가정할 때 각 모델에서 검증자의 딜레마를 촉발하는 X 의 최댓값은 다음과 같다:

	기본 검증 모델	스테이킹 검증 모델	스테이킹 & 빠른 출금 검증 모델
검증자의 딜레마를 촉발하는 X 의 최댓값	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{7}$
비고		기본 검증 모델 대비 패러미터 값을 조정하기 쉬움	기본 검증 모델 대비 패러미터 값을 조정하기 쉬움

7. 참고 문헌 (References)

https://github.com/Onther-Tech/economics/blob/main/Tokamaklayer2.md

https://medium.com/onther-tech/optimistics-not-secure-enough-than-you-think-46bf93d80292

8. 부록 (Appendix)

8.1. 면책조항 (Disclaimer)

본 백서 및 이와 관련해 배포된 기타 문서들은 토카막 네트워크의 개발 및 응용에 활용되며, 이들 자료는 정보 제공만을 목적으로 하고, 향후 그 내용이 변경될 수 있다.

백서는 향후 진행될 프로젝트에 관한 것이다

백서는 프로젝트의 지속 지원을 위해, 백서를 작성한 토카막 네트워크 (Tokamak Network Pte. Ltd.) 의 믿음을 바탕으로 한 미래 예측이 포함되어 있다. 백서에 언급된 토카막 네트워크는 현재 개발이 진행중이며, 주요 거버넌스 및 기술적 기능을 비롯해 다양한 내용들이 지속적으로 업데이트되고 있다. 톤 (TON) 토큰은 백서에 명시된 목표 달성과 성과로 이어지지 않을 수도 있는 실험적 플랫폼 (소프트웨어) 과 관련 기술의 개발 및 활용에 기반한다. 토카막 네트워크가 완성될 경우, 백서에 명시된 내용과는 상당히 차이가 있을 수 있고, 모든 계획, 향후 예상 또는 전망의 달성과 관련해 어떠한 보증도 하지 않으며, 본 문서의 어떠한 내용도 미래에 대한 약속으로 간주되어서는 안된다.

적격성

백서의 내용은 향후 특정 구매자들에게 직접 제공되며, 이들 구매자 외에는 누구도 백서의 수령이나 열람 대상이 아니다. 단순히 백서를 수령한 것으로는 적격성이 보장되지 않으며 참여에 제한이 있을 수 있다.

규제 대상 품목

토카막 네트워크 플랫폼, 톤 (TON) 토큰이나 해당 플랫폼상에서 운영되는 모든 토큰은 유가증권이나 어떠한 법정관할 지역에서 규제 대상 품목으로 지정된 것을 의미하지 않는다. 본 문서는 유가증권 또는 기타 규제 대상 제품의 제공이나 권유, 투자 목적의 홍보, 초대 또는 권유를 위한 것이 아니다. 백서는 금융 서비스 제공 목적의 문서나 그 어떤 투자설명서도 아니다. 톤 (TON) 토큰은 플랫폼이나 소프트 웨어 또는 기업의 자본, 수익, 소득 또는 수입에 대한 지분, 출자 지분, 유닛, 로열티 및 권리, 또는 모든 관할구역의 플랫폼이나 기타 공공 또는 사설 회사, 조직 및 기타 독립체와 관련된 지식재산을 표시하는 것이 아니다.

백서는 투자 권고문이 아니다

백서는 톤 (TON) 토큰 구매 권고문이 아니다. 본 문서는 계약이나 구매 결정과 관련된 것으로 간주되어서는 안된다.

리스크

톤 (TON) 토큰의 구매 및 판매 참여에는 상당한 리스크가 존재한다. 톤 토큰을 구매하기에 앞서 모든 리스크에 대한 신중한 평가 및 고려가 이루어져야 한다.

백서의 관점

백서는 토카막 네트워크 (Tokamak Network Pte. Ltd.) 의 관점과 견해를 담고 있으며, 이는 어떠한 법정관할 지역의 정부나 준정부, 당국 또는 규제기관 등의 공공기관의 정책이나 입장을 반영하지 않는다. 백서에 포함된 정보들의 경우 신뢰할 수 있는 출처를 통해 확보된 내용을 바탕으로 한 것이기는 하나, 그 정확성 또는 완전함에 대해서는 보증하지 않는다.

백서의 공식 언어는 영어

백서 및 관련 자료들은 영어로만 발행된다. 번역본은 참조용일 뿐이며, 토카막 네트워크나 기타 개인의 인증을 받은 것이 아니다. 번역본의 정확성 및 완전함에 대해서는 그 어떤 보증도 하지 않는다. 백서의 번역본과 영어 버전의 내용상 불일치가 존재하는 경우에는 영어 버전이 우선하는 것으로 한다.

제삼자 제휴와 보증을 의미하지 않는다

백서에서의 특정 기업 및 플랫폼에 대한 언급은 단순히 예시적인 차원에서 이루어진 것이다. 기업이나 플랫폼의 명칭 및 등록상표의 사용이 해당 당사자의 제휴나 보증을 뜻하는 것은 아니다.

전문가의 조언

톤 (TON) 토큰 구매 또는 토카막 네트워크 프로젝트 참여 여부를 결정하기에 앞서, 필요에 따라 변호사, 회계사, 세무사 또는 기타 전문가들로부터의 상담이 권고된다.

백서와 관련해 관할 구역의 규제 당국이 검토한 것은 아니다

백서의 특정 기업, 네트워크 또는 잠재적 활용 사례들에 대한 언급은 오로지 예시적 차원에서 이루어진 것이다. 토카막 네트워크 (Tokamak Network Pte. Ltd.) 등 명확하게 언급된 파트너나 제공자를 제외하고, 기타 기업 또는 플랫폼 명칭 및 등록상표의 사용이 해당 당사자의 제휴나 보증을 뜻하는 것 또한 아니다.

관련 자료 중 백서가 최우선시된다

만약 백서 이외의 자료가 백서와 충돌하는 부분이 있다면 백서를 우선시하는 것으로 한다.