

RAILGUN

/// WHITEPAPER
MMXXI

RAILGUN PROJECT
NOVEMBER 6, 2021

목차

| | |
|-----|------|
| 05 | 비전 |
| 06 | 소개 |
| 08 | 기술 |
| 013 | 거버넌스 |
| 015 | 경제 |

RAILGUN PROJECT
NOVEMBER 6, 2021

RAILGUN

RAILGUN은 Eth//reum을 기반으로 구축된 견고한 영지식 기관으로 사용자 및 온체인 애플리케이션을 위한 개인정보 보호 및 익명성을 가능하게 합니다.

RAILGUN: 사용자가 이더리움 해시파워의 완전한 보안을 절충하지 않고 이더리움에서 DeFi 스마트 계약과 상호 작용하면서 개인 정보를 처음으로 유지할 수 있습니다.



비전

프라이버시는 모든 인간이 본능적으로 가치 있게 여기는 것입니다. 이것은 잘 알려진 인권이며, 다른 사람에게 프라이버시를 거부하는 사람들조차도 스스로는 기대하는 것이 프라이버시입니다. 프라이버시와 익명성은 예외가 아닌 기본이 되어야 합니다. 개인 또는 재정 세부 정보가 공개되기 전 귀하의 동의는 분명히 필요합니다.

열정적이고 숙련된 개인 정보 보호 애호가로 구성된 우리의 소규모 커뮤니티는 Ethereum에 직접 구축된 개인 정보 및 익명 시스템인 RAILGUN을 개발 중이며, 이 시스템에서 DEX, 대출 플랫폼 및 인기 있는 스마트 계약 응용 프로그램과 직접 상호 작용할 수 있습니다. RAILGUN은 사용자의 활동을 및 신원을 비밀로 유지하고 개인 정보를 보호하여 익명성을 제공합니다. RAILGUN은 Ethereum과 그 호황을 누리는 생태계의 안전과 활력을 떠나지 않은 상태에서 이 작업을 수행할 수 있습니다. 그뿐만 아니라 RAILGUN은 다른 블록체인 생태계에 혁신적인 이점을 연속적으로 가져올 것을 약속합니다.

투명성이 필요할 시, RAILGUN은 개인 정보 보호 Zero Knowledge 방식을 사용하여 귀하의 활동 및 균형에 대한 검증 가능한 보고서(예: 감사인 또는 규정 준수 책임자용)를 생성할 수 있습니다. 즉, 귀하의 자금은 공개되지 않지만 선택한 동료 또는 수령인에게 출처에 대한 증거를 제공할 수 있다는 것입니다. RAILGUN의 목표는 온체인에서 수행된 작업에 대한 제3자 검증 가능성을 없애는 것이 아니라 사용자에게 누가 무엇을, 언제, 왜 볼 것인지 선택할 수 있는 권한을 부여하는 것입니다.



소개

퍼블릭 블록체인은 바로 말 그대로 개방형 블록체인입니다. 오늘날 가장 인기 있는 블록체인에서는 귀하의 온체인 활동을 전 세계가 볼 수 있으며 아마 10년 후에는 더 그렇게 될 것으로 예상됩니다. 상용적인 온체인 분석 시스템이 귀하와 귀하의 모든 거래를 사소하게 추적할 수 있는 수준으로 개선함에 따라 이는 우리같은 블록체인 사용자에게 명백한 문제를 보여주고 있습니다. 또한, 이것은 오늘날 소수의 국가에 존재하는 전문 전자 감시 조직의 잠재적인 노력과 능력을 고려하기 전입니다. 이러한 상황은 개인, NGO 및 기업의 대규모 채택에 대한 근본적인 도전을 제시합니다. 모닝커피 값을 지불할 시 커피숍, 바리스타 및 다른 고객에게 귀하의 은행 계좌에 얼마가 있는지, 얼마를 받았는지, 또 어디에 돈을 썼는지 알려주는 세상을 상상해 보십시오. 지금처럼 대부분의 암호 화폐를 사용하는 경우 이것이 바로 당신이 겪을 수 있는 상황입니다.

Ethereum은 거래 및 기타 분산 금융 애플리케이션의 선두 체인이지만 Ethereum과 비공개 및 익명으로 상호 작용하는 것은 어려운 것으로 입증되었습니다. 최근까지는 이를 위한 도구를 사용할 수 없었습니다. 현재 이미 존재하는 솔루션에는 Ethereum에 있는 DEX, 애플리케이션 및 유동성에 직접 액세스할 수 없는 특수 블록체인이 필요합니다. 많은 사용자는 자신의 거래 내역을 전 세계와 영구적으로 공유하는 것과 비교하여 '덜 나쁜' 것으로 간주되는 모든 종류의 개인 데이터를 중앙 집중식 솔루션에 마지못해 의존하고 있는 상황입니다.

RAILGUN이란?

RAILGUN은 영지식 증명을 확인하는 스마트 계약 모음으로, 사용자가 자산, 금액 또는 신원을 공개하지 않고도 거래를 하며, 보내고, 받을 수 있습니다. 거의 같은 방식으로 사용자는 DEX 거래, 수확량 농업 및 기타 dApp (탈중앙화 앱)에 사용되는 것과 같은 스마트 계약과 상호 작용할 수 있습니다. 이 온체인 시스템의 상단에는 기존 애플리케이션을 위한 Adapt Module이라는 어댑터 제품군이 있습니다.

누구나 배포할 수 있는 Ethereum에서 이러한 시스템에는 두 가지 근본적인 이점이 있습니다.

1. 첫째, 익명성 풀의 크기와 노이즈를 증가시킵니다. 모든 전송, 교환, 대출, 차용 및 일반적으로 모든 종류의 분산 응용 프로그램과의 거래는 RAILGUN과의 상호 작용의 처리량과 변동을 크게 증가시켜 RAILGUN에서 인출을 RAILGUN으로 입금하는 것을 점점 더 어렵게 만듭니다. 이는 RAILGUN에 입금한 사용자가 온체인에서 사용 가능한 다른 시스템보다 더 빠르게 개인 정보 보호와 익명성을 달성할 수 있음을 의미합니다.

2. 둘째, 사용자는 RAILGUN 시스템 내에서 다른 토큰으로 변환하지 않고 자산을 원래 형태로 장기간 유지할 수 있습니다. 자산을 개인적으로 거래할 수 있을 뿐만 아니라 개인적으로 저장할 수 있을 때 진정한 프라이버시와 익명성이 달성됩니다. RAILGUN의 사용자는 RAILGUN 외부의 자산으로 할 수 있는 모든 작업을 여전히 수행할 수 있으므로 이러한 자산을 이전하는 인센티브가 줄어듭니다. 이것은 익명성 풀의 크기와 노이즈를 증가시켜 훨씬 더 나은 수준의 개인 정보 보호 및 익명성을 제공하는 데 도움이 됩니다.

개인 정보 보호, 익명성, 전송, 거래 및 기타 모든 활동이 한 곳에서 발생하는 생태계를 만들어 모든 사용자가 점점 더 큰 익명성 풀의 혜택을 누릴 수 있습니다. 시스템의 모든 사용자는 다른 사람의 활동을 피기백하여 자신의 개인 정보와 익명성을 높일 수 있습니다.

RAILGUN은 어떠한 방식으로 작동되니까?

RAILGUN은 다음과 같은 주요 기능으로 구성됩니다.

ADD는 자산을 RAILGUN으로 전송하고 모든 자산과 해당 소유자를 나타내는 새로운 영지식 노트를 생성합니다. 이 작업 자체는 비공개가 아닙니다 (시스템 외부에서 시작되지만 개인 정보 보호를 위한 첫 번째 단계이기 때문입니다). 그런 다음 이 노트가 라이브 풀에 추가됩니다.

SPLIT은 하나 이상의 영지식 노트를 두 개의 영지식 노트로 나눕니다. 입력된 노트는 라이브 풀에서 데드 풀로 이동되고 출력된 노트는 라이브 풀에 추가됩니다. 이 모든 것은 사용자가 자신이 입력 노트를 소유하고 있으며 이 노트 자체를 공개하지 않고 입력 노트가 이전에 사용된 적이 없음을 증명하는 영지식 내에서 수행됩니다. SPLITTING은 새로 생성된 노트 중 하나에 다른 소유자를 설정하여 자금을 이체하는 방법으로도 사용할 수 있습니다. 이것은 SPLIT의 정확한 의도를 숨기는 데 도움이 됩니다.

REMOVE는 노트를 파괴하여 RAILGUN에서 임의의 주소로 자산을 전송합니다. 다시 말하지만, 이것은 사용자가 노트나 자신을 드러내지 않고 파괴된 노트의 소유권을 증명하는 영지식 내에서 수행됩니다. 그러나 받는 사람이 시스템 외부에 있기 때문에 이 작업을 수행할 시 자금이 이체되는 주소와 금액은 표시됩니다. 그러나 실제 사용자 정보가 아니라 RAILGUN 시스템에서 온 것이라고 표시됩니다.

모든 작업 단계에서는 다양한 수준의 개인 정보 보호 및 익명성이 수반되므로 사용자는 필요한 경우 가스 비용을 줄이기 위해 다양한 작업 유형을 선택할 수 있습니다. 또한 가스 비용을 줄이기 위해 사용자는 여러 작업을 하나의 증명으로 일괄 처리할 수 있습니다.

기술

RAILGUN은 다음을 가능하도록 설계 되었습니다.

- 미사용 암호화폐 자산의 완전 개인적인 저장소 구축
- 완전한 개인 정보 보호 및 블록체인의 완전한 보안으로 DeFi 플랫폼 거래 및 참여
- 온체인 활동 추적 없이 다른 사용자와 비공개로 토큰 교환
- 자산 출처에 대한 증거 제시 예: 규정 준수용

이 외에도 RAILGUN DEX가 (DAO가 찬성하는 경우) 곧 출시되어 외부 당사자에게는 보이지 않지만 RAILGUN 내에서는 가능한 동일한 온체인 기술 내에 구축된 P2P 거래를 촉진할 계획입니다.

RAILGUN 핵심 시스템 및 프로토콜

Railgun 프로토콜의 핵심은 (U)TXO, 즉 (Unspent) 트랜잭션 출력 모델에서 작동하는 JoinSplit 트랜잭션입니다. 여기에서 U는 외부 관찰자가 어떤 TXO(트랜잭션 출력)가 사용되었고 어느 것이 사용되지 않았는지 결정할 수 없기 때문에 () 안에 있습니다. 각 UTXO는 사용할 수 있는 사람, 금액, 토큰 ID (예: USDT, WETH, WBTC 등 해당 ERC-20 지갑 주소로 표시)를 설정하는 공개 키의 암호화된 노트이며 노트 약정(즉, 해시)을 무작위화 합니다. 우리는 내부적으로 머클트리 (암호화 해시 기능을 사용하여 대규모 데이터 구조의 내용을 효율적이고 안전하게 검증할 수 있는 트리 데이터 구조)의 효율적인 구현을 사용하여 이 정보를 온체인으로 유지합니다.

우리는 외부 자가 TXO에 연결할 수 없지만 이중 지출의 가능성을 제거하기 위해 트랜잭션에서 결정적으로 생성되는 사용자의 개인 키를 사용하여 생성되는 특정 유형의 해시인 Nullifier를 사용합니다. Nullifier는 지출 키의 해시(질문의 UTXO에 대한 지출자의 개인 키)와 머클 루트의 경로 인덱스를 사용하여 계산되며, 이는 각 노트가 항상 고유한 Nullifier를 생성하도록 합니다. Nullifier는 지출자만 생성할 수 있으므로 RAILGUN은 이를 이중 지출 제거로 사용할 수 있습니다. 지출자는 어떤 Nullifier가 어떤 UTXO에 속하는지 연결할 수 있는 유일한 사람입니다.

RAILGUN 시스템 내에서는 영지식 증명을 많이 사용합니다. 영지식 거래는 일부 공개 입력과 일부 개인 입력이 같이 있는 작은 프로그램으로 간주될 수 있습니다. 따라서 증명자 프로그램은 공개 및 비공개 입력으로 증명을 생성한 다음 ZKP(Zero-Knowledge Proof)와 함께 검증자 프로그램에 공개 입력을 제공할 수 있습니다. 이 정보를 통해 검증 프로그램은 증명자 프로그램이 성공적으로 실행한 것을 확인할 수 있습니다. 공개 입력은 개인 입력이 검증자가 예상한 값이고 위조된 값이 아님을 증명하는 정보의 일부로 존재하며 UTXO 세트의 머클 트리 루트는 증명자가 '나는 10000000000 ETH를 가진 UTXO를 가지고 있습니다' 라고 주장할 수 없도록 효율적으로 보장합니다.

영지식 프로그램에는 다음과 같은 공개 입력이 있습니다.

- Adapt ID (다음 섹션에서 이에 대한 자세한 설명)
- 입금금액
- 출금금액
- 머클루트
- Nullifiers
- UTXO 해시 출력
- 암호화된 UTXO 출력, 수신자만 해독 가능

또한 다음과 같은 옵션의 공개 입력도 있습니다.

- 입출금을 해야 하는 경우 공개되어야 하는 TokenID, 그러나 입출금이 모두 0인 경우 비공개인 TokenID
- 논제로가 아닌 출금을 위해 공개되어야 하는 출금 주소

개인 입력은 다음과 같습니다.

- 입력 금액
- UTXO에 대한 개인 키가 사용되는 지출 키
- 머클 회원 증명
- 수신자 공개 키
- 출력 금액

이러한 입력을 통해 영지식 프로그램은 다음을 확인합니다.

- 입금 금액 + 입력 금액 = 출금 금액 + 출력 금액, 이로하여 아무나 쉽게 토큰을 만들 수 없습니다
- 머클루트 및 머클 멤버십 증명을 사용한 머클 트리에 입력 노트의 존재
- 지출 키는 노트의 개인 키만 사용할 수 있으므로 입력 노트에 대해 유효합니다.
- Nullifier의 올바른 계산

계약은 다음 사항을 확인합니다.

- 거래에 대한 영지식 증명이 유효합니다.
- 이전 Nutifiers가 확인된 적이 없으므로 이중 지출을 제거합니다.
- 사용자가 UTXO를 구성하는 것을 방지하기 위해 현재 또는 이전 사용된 머클 루트입니다.
- 그런 다음 스마트 계약은 입금액이 지정된 경우 사용자 지갑에서 자체적으로 토큰을 전송하거나 대신 출금 금액이 지정된 경우 공개 입력에서 지정된 사용자 지갑 주소로 토큰을 자체적으로 전송합니다. 그런 다음 출력 UTXO의 해시가 머클 트리에 추가되어 나중에 사용할 수 있습니다.

어댑터 모듈

어댑터 모듈은 개인 거래 및 NFT 등과 같은 기능을 용이하게 할 수 있는 RAILGUN 프로토콜에 대한 별도의 스마트 계약 확장입니다. 이러한 어댑터 모듈은 RAILGUN의 핵심 코드를 부풀리지 않고 추가 기능을 구현할 수 있습니다. Adapt ID 인터페이스 자체는 단순하지만 매우 강력합니다.

Adapt ID 인터페이스는 계약 주소와 매개변수의 두 필드로 구성됩니다.

계약 주소가 지정된 경우 RAILGUN 핵심 계약은 Adapt ID 모듈 인터페이스를 통해 지정된 계약 주소에서 트랜잭션이 제출된 경우에만 트랜잭션을 처리합니다. 모든 관련 증명은 지정된 계약에서만 제출할 수 있기 때문에 RAILGUN 핵심 프로토콜의 유효성 검사 규칙과 어댑터 모듈의 유효성 검사 규칙을 모두 통과한 경우에만 유효합니다.

Adapt ID 매개변수는 어댑터 모듈이 원하는 모든 사용자 정의 로직을 구현할 수 있도록 하는 핵심 RAILGUN 코드에 의해 검증되지 않습니다 (예: AAVE와 같은 외부 DeFi 계약과의 상호 작용 세트일 수 있음).

어댑터 모듈을 별도의 계약으로 유지하면 RAILGUN 사용자의 자금이 잘못 코딩되거나 악의적인 어댑터 모듈의 위험에 노출되지 않습니다.

- Alice와 Bob이 토큰을 교환하기 위해 어댑터 모듈을 사용하는 방법을 살펴보겠습니다.
- Alice는 100 USDC를 100 USDT에 판매하기를 원하므로 혼자 사용할 수 있는 100 USDT에 대한 노트를 생성합니다 (노트 A라고 칭명).
- Bob은 100 USDT를 100 USDC에 판매하기를 원하므로 혼자 사용할 수 있는 100 USDC에 대한 노트를 생성합니다 (노트 B라고 칭명).
- Alice는 Bob에게 노트 A를 보내고 Bob은 노트 B를 Alice에게 보냅니다.
- Alice는 약정 A의 해시를 Adapt ID로 사용하여 노트 B에 지출하는 증명을 생성합니다 (이를 증명 A라고 칭명).
- Bob은 약정 B의 해시를 Adapt ID로 사용하여 노트 A에 지출하는 증명을 생성합니다 (이를 증명 B라고 칭명).
- Bob은 자신의 증거를 Alice에게 보냅니다. Alice는 자신의 증거를 Bob에게 보냅니다. Alice 또는 Bob은 두 증명 모두를 공통 릴레이어로 보냅니다. 이 예에서는 Alice가 두 증명을 직접 보낼 것입니다.
- Alice는 두 가지 증명을 모두 Swap 모듈에 제출합니다 (릴레이어를 통해). Swap 모듈은 증명 A의 Adapt ID가 증명 B의 노트 해시 중 하나와 동일하고 증명 B의 Adapt ID가 증명 A의 메모 해시 중 하나와 동일한지 확인합니다. 둘다 동일하다면, 두 증명 모두 원자적 트랜잭션으로 RAILGUN 시스템에 제출됩니다. 두 증명 중 하나라도 동일하지 않다면 전체 트랜잭션이 되돌려 집니다.

Swap 트랜잭션 및 RAILGUN DEX

Swap 트랜잭션은 Adapt ID 인터페이스를 사용합니다. 각 RAILGUN 트랜잭션은 채우려는 출력의 해시를 지정합니다. Swap Adapt ID 모듈의 유효성 검사 규칙은 지정된 출력 해시로 출력하는 다른 트랜잭션이 함께 제출되는 경우에만 트랜잭션이 유효한지 확인합니다. 따라서 모든 Swap은 원자적 및 무신뢰 방식으로 수행되며 출력이 서로 일치하는 트랜잭션 쌍만 유효하며 실행됩니다.

릴레이어 네트워크

RAILGUN에서는 누구나 릴레이어가 될 수 있습니다. 사용자는 자신이 원하는 거래 및 가스 가격을 지정해 제출합니다. 그런 다음 릴레이어는 지불받을 수수료에 대해 응답합니다 (릴레이어의 ETH 가스 비용). 그 후, 사용자는 요청된 수수료와 일치하는 릴레이어의 주소에 대한 출력 중 하나를 사용하여 RAILGUN 트랜잭션을 생성합니다. 릴레이어는 출력 중 하나가 올바른 수수료로 지정되었는지 확인한 다음 지정된 가스 비용으로 네트워크와 사용자 모두에게 트랜잭션을 보냅니다. 이것은 RAILGUN 내부 사용자의 트랜잭션이 ETH 주소와 연결되는 것을 방지합니다.

기술적인 로드맵 가능성

출시 후 DAO 사용자는 다음 항목에 투표할 수 있습니다.

- 참조 프론트엔드로 RAILGUN Core 배포
- Binance Smart Chain 및 Polygon에 RAILGUN 배포(2021년 7월/8월 예정)
- 릴레이어 네트워크 배포
- 일괄 거래 검증 기능 내부화 및 Swap 거래를 더 저렴하게 교환
- RAILGUN DEX (RAILYSWAP)
- 거래되는 것과 다른 토큰으로 수수료 지불
- 개인 NFT 지원
- 철저한 비공개 NFT 경매
- NFT 지분을 통한 비공개 투표
- SOL / Solana RAILGUN(SOLRAIL) 배포(2021년 11월 예정)
- Polkadot RAILGUN(DOTRAIL) 배포(2022년 1월 예정)

거버넌스

RAILGUN은 한 개인이나 팀의 통제를 받지 않으며 앞으로도 그럴 계획입니다. 모든 지침은 항상 거버넌스 토큰 소유자가 프로젝트의 운영 및 방향을 정의하는 투표 DAO (Decentralized Autonomous Organization) 인 RAILGUN DAO에서 제공됩니다. RAILGUN 스마트 계약 코드는 DAO 거버넌스 투표 후에만 배포되거나 업데이트됩니다. 출시 시, RAILGUN DAO는 배포된 RAILGUN 개인 정보 보호 계약 없이 바로 실행되며 배포되는 코드 버전은 RAIL 토큰 스테이커가 투표한 버전이 됩니다.

RAIL 토큰 & 투표

RAIL은 RAILGUN DAO의 거버넌스 토큰입니다. 하나의 토큰(투표 계약에 스테이킹됨)은 하나의 투표와 같습니다. 스테이킹 아직 하지 않았거나 언스테이킹한 사용자는 투표할 수 없습니다. RAIL 토큰이 스테이킹되면 언스테이킹 기간은 30일이므로 투표 후 토큰을 보유하는 데 최소 30일의 유효 시간이 있습니다. 이는 유권자가 프로토콜 업그레이드 또는 수수료에 대한 투표에 대해 선택할 때 최소 한 달 전에 미리 살펴봐야 한다는 것을 의미합니다. "투표 공격" 행위는 있을 수 없으며 유권자들은 앞으로 몇일 만이 아닌 희망찬 미래를 내다볼 것입니다.

RAIL 배포

RAILGUN DAO 거버넌스 토큰인 RAIL의 분배는 다음과 같이 요약될 수 있습니다.

- Airdrop에 25% 할당
- 재단에 25% 할당
- 50%는 RAILGUN DAO에 할당

출시 시, 총 순환 토큰 공급량은 5천만 개의 RAIL 토큰입니다. RAIL 토큰의 최대 평생 총 공급량은 1억 개의 토큰이 될 것이며 1억 개 이상을 생성하는 것 자체가 불가능합니다.

에어드롭 토큰(25%): ETH 네트워크에서 TOR 프로젝트, Right to Privacy 재단, Free Software 재단 등과 같은 비영리 자선 단체 및 재단에 기부한 Ethereum 주소에는 RAIL 토큰이 에어드롭됩니다. 커뮤니티 형성의 가장 중요한 부분은 구성원을 포함하는 것이며 Railgun의 목표에 대한 장기적인 관심을 이미 입증한 구성원은 DAO를 시작하기에 제일 적합한 구성원입니다. 이러한 수신자 중 다수는 이에 대해 직접 알릴 방법이 없기 때문에 자신이 에어드랍을 받는다는 사실을 인지하지 못할 수 있습니다.

재단 토큰(25%): 프라이버시 권리 재단은 RAILGUN 프로젝트 개발을 위한 보조금을 발행했으며 프로젝트의 장기적인 이점을 지원하기 위해 RAIL 토큰의 25%를 관리하기로 자원했습니다. 재단은 등록된 자선 단체이며 이익을 목적으로 하지 않습니다. 이 토큰은 향후 배포를 포함하여 개발자에게 인센티브를 제공하고 RAILGUN 플랫폼을 홍보하는 것에만 사용됩니다. 재단은 첫 DAO 연도 동안 토큰 판매자가 되지 않을 것입니다.

DAO 토큰(50%): DAO에 제공된 5천만 개의 토큰은 잠겨 있고 민팅되지 않습니다. RAIL 토큰 소유자의 DAO 투표로만 민팅할 수 있습니다. 예를 들어, DAO가 RAIL 토큰의 유동성 풀 주자에게 보너스 수익률을 제공하고 싶을 경우, DAO는 이 할당에서 필요한 수의 RAIL 토큰을 민팅하고 잠금을 해제하도록 투표합니다. DAO는 RAILGUN 재무부에서 RAIL 토큰 보유자에게 거래 수수료를 분배하는 방법에 대해 투표할 수 있습니다.

요약

모든 사용자는 RAILGUN의 의미 있는 일원이어야 하며, 디지털 시대의 프라이버시를 중시하는 커뮤니티로서 프로젝트의 성장과 방향에 영향을 줍니다. RAIL 토큰은 이러한 종류의 팀워크를 위해 DAO 거버넌스 시스템에서 사용됩니다. 사용자는 변경 제안을 제출하고 변경 사항에 대해 비공개로 안전하게 투표할 수 있습니다. 처음 몇 주 동안 기본 데스크톱 및 모바일 RAILGUN 앱에서 RAILGUN 재무에 수집된 거래 수수료를 스테이킹된 RAIL 토큰 보유자에게 분배하는 것에 대한 초기 지지자들의 제안을 보았습니다.

경제

다음은 출시 후 첫 주에 RAILGUN DAO 회원들의 투표로 전달될 경제적인 제안입니다. DAO 투표권을 갖게 될 RAIL 스테이커는 대안을 제안하거나 이 특정 제안에 대해 찬성 또는 반대 투표를 할 수 있습니다. 거버넌스 모델 및 프로세스에 대한 자세한 내용은 거버넌스 섹션을 참조해 주시길 바랍니다.

RAILGUN 과 RAIL Token 의 경제학

RAILGUN 네트워크의 경제 정책은 RAILGUN 시스템과 그 익명성 풀에 직접적으로 기여하고 상호 작용하는 사람들에 의해 통제됩니다. RAIL 토큰은 시스템, 업그레이드 및 매개변수를 관리하는데 사용되며 또한 거버넌스와 성장에 대한 참여를 장려하는 데에도 사용될 것입니다.

RAIL은 모든 유동성 풀에 지속적으로 방출됩니다. RAIL 유동성 풀이 가장 먼저 존재하게 되며, 그 유동성 공급자는 예치된 RAIL의 양에 비례하는 거버넌스 권한을 얻게 됩니다. 유동성 풀의 비공개 및 익명 특성으로 인해 RAIL 보유자는 알려지지 않고 비밀리에 통치할 수 있습니다. 이는 유권자를 보호하고 보다 강력하고 독립적인 RAILGUN DAO에 기여하는 RAILGUN 시스템 고유의 자산입니다. 정확한 배출 일정은 RAIL 보유자가 통제할 수 있지만 10년 배출 일정으로 시작됩니다.

수수료 및 RAILGUN 재무

수수료는 모든 상호 작용에 코딩됩니다: 수수료는 RAILGUN DAO 재무 주소로 전송됩니다. DAO의 과반수 투표만이 DAO 재무부 자금의 지출을 통제할 수 있으며 다른 사람은 이를 절대 이동할 수 없습니다. ADD 기능 수수료 및 REMOVE 기능 수수료를 제외하고 모든 RAILGUN 수수료는 처음에 0으로 설정되며 시작 시 각각 25bp로 설정됩니다. 이는 RAILGUN 프라이버시 스마트 계약이 예치 또는 인출에 대해 토큰의 0.25%를 청구한다음 것을 의미합니다. RAILGUN 프라이버시 계약을 통해 대량의 개인 정보 보호 거래가 발생할 것으로 예상됨에 따라 처음부터 재무부에 징수되는 수수료는 RAILGUN 프라이버시 계약 활동으로 인해 매우 커질 것으로 예상됩니다.

RAIL에 대한 유동성 프로비저닝

RAIL은 개발 및 테스트 참여를 장려하기 위해 초기 버전 및 프로토타입의 초기 사용자 및 유동성 공급자에게 DAO에서 릴리스됩니다. 일반적으로 RAIL 토큰은 네트워크 활동에 비례하여 향후 10년 동안 유동성 공급자 및 활성 사용자에게 릴리스됩니다. 이는 먼저 네트워크의 적극적인 사용을 장려하는 역할을 하며 둘째로, 이는 RAILGUN의 거버넌스가 실제로 RAILGUN을 사용하고 성공과 밀접하게 연계된 사용자에게 전달되도록 합니다.

멀티 체인

RAILGUN 프로젝트가 Binance Smart Chain & Polygon에 먼저 RAILGUN을 배포하고 나중에 Solana & Polkadot에 배포함에 따라 새로운 해당 토큰(POLYRAIL, SOLRAIL, DOTRAIL 등)은 이미 RAIL을 스테이킹하는 사람들과 RAIL용 LP 토큰을 보유하고 있는 사람들에게만 에어드롭됩니다. Binance Smart Chain RAILGUN(BRAIL) 및 Polygon RAILGUN(POLYRAIL)과 같은 대형 체인 배포는 RAIL 스테이커뿐만 아니라 DEX(LP 토큰을 보유하는 사람)에서 RAIL 유동성을 제공하는 사람들에게 에어드롭되어야 합니다.

다른 당사자는 이러한 새로운 토큰 에어드롭을 받지 않으며 예비 공급이 전혀 없을 것입니다. 이 새로운 비 ETH 체인 토큰은 RAIL과 무관하게 완전히 새로운 시가 총액과 가격을 갖게 됩니다.



Pr1vacy & An0nymity

NOVEMBER 6, 2021
