



프롬(PROM)

주요내용설명서(국문백서)
Korean White Paper

2026년 8월 24일

Disclaimer

본 번역본은 2026년 8월 24일 기준의 프롬(Prom) Docs 관련 내용 위주로 번역됐습니다.

빗썸은 발행주체 또는 운영주체가 제공하는 가상자산의 총발행량, 유통량 계획, 사업 계획 등이 포함된 정보를 이용자들의 편의를 위해 참고용으로 제공하고 있습니다.

본 번역본은 그 내용이 정확하지 않을 수 있으며 원문의 내용이 일부 누락될 수 있으므로, 정확한 정보 습득을 위해서는 원문을 참고하시거나 원문 작성 측에 문의하시기를 바랍니다. 또한 본 번역본은 오픈 커뮤니티의 검토에 따라 내용이 변경될 수 있습니다.

프로젝트 소개

프롬(Prom)은 영지식 증명¹을 활용하는 폴리곤 CDK² 기반의 고성능 확장형 네트워크입니다. 영지식 증명을 통해 오프체인에서 실행된 트랜잭션³의 진위 여부를 검증하고 트랜잭션을 빠르게 확정하는 것이 가능하며, 이러한 과정을 zk롤업⁴이라 칭합니다. zk롤업 시스템은 투명하게 스마트 컨트랙트⁵를 실행하고 검증을 위한 영지식 증명을 생성한 뒤 공개하는 방식을 작동되며 EVM⁶ 연산코드⁷와 완벽한 호환성을 유지합니다.

zkEVM를 활용한 이더리움 확장

분산형 원장 기술⁸의 본질적인 트릴레마⁹ 문제로 인해 이더리움은 탈중앙화나 보안을 타협하지 않고 확장성을 강화하는 것이 제한적입니다. 바로 이러한 제약을 극복하기 위해 프롬이 탄생하게 되었습니다.

프롬은 EVM의 모든 연산코드를 복제하는 방식으로 EVM을 모방한 구조이기 때문에 이더리움의 기존 스마트 컨트랙트를 쉽게 통합할 수 있습니다. 프롬의 zk롤업은 확장성과 트랜잭션 처리 속도를 대폭 개선함으로써 이더리움 메인넷의 성능을 강화합니다.

프롬은 오프체인 연산의 정확성을 확인하는 데 검증 가능한 영지식 증명을 활용합니다. 영지식 증명은 처리 과정에 복잡한 다항식 계산이 포함되기는 하지만 오프체인 트랜잭션을 효율적이면서도 직관적인 방식으로 검증 및 확정할 수 있는 수단입니다.

¹ Zero-knowledge (zk) proof

² Polygon CDK (Chain Development Kit)

³ Transaction

⁴ Zero-knowledge rollup

⁵ Smart contract

⁶ Ethereum virtual machine

⁷ Opcode

⁸ Distributed ledger technology (DLT)

⁹ Trilemma

프롬이 영지식 증명을 접목한 혁신적인 설계 모델을 채택한 것은 사용자와 개발자 모두의 불편함을 감소시키기 위한 전략적 결정이었습니다. 모델 도입을 위해 EVM의 모든 연산코드를 재구현하여 이더리움 스마트 컨트랙트를 투명한 방식으로 통합할 수 있도록 했습니다.

프롬의 주요 이점

- EVM 동등성
- 이더리움 보안 활용
- 영지식 증명을 통한 확장성 강화

개발자는 프롬에 기존 스마트 컨트랙트를 원활하게 배포할 수 있으며, 사용자는 이더리움에서 자산을 옮겨 오프체인 작업에 쉽게 활용할 수 있습니다. 그러한 작업들은 묶음 처리되어 영지식 증명을 통해 검증됩니다. 이를 통해 모든 트랜잭션의 유효성을 보장하고 시스템 운영자가 사용자의 자산을 부정하게 사용하는 것을 방지할 수 있으며, 궁극적으로는 이더리움 보안 프레임워크의 신뢰도가 유지되게 됩니다.

프롬 네트워크는 호환성과 확장성 중 어느 하나도 타협하지 않고 모두 효과적으로 확보합니다.

비즈니스 모델

zk노드¹⁰

zk노드는 프롬 노드를 실행하기 위해 필요한 소프트웨어입니다. 네트워크 사용자는 zk노드를 사용해 프롬 네트워크의 상태를 확인하고 동기화합니다. 네트워크 상태와 상태 확정에 영향을 주는 주요 참여 주체는 검증된 시퀀서¹¹와 애그리게이터¹²입니다.

프롬이 zk롤업 작업을 위해 활용하는 핵심 구성 요소는 아래와 같습니다.

- 사용자: 메타마스크¹³와 같은 RPC(원격 프로시저 호출)¹⁴ 노드를 통해 네트워크에 접속하여 데이터베이스(풀 DB)에 트랜잭션을 제출합니다.
- 풀 DB: 사용자가 제출한 트랜잭션이 저장되어 있는 곳으로, 풀 DB에 존재하는 트랜잭션은 이후 시퀀서에 의해 배치¹⁵ 처리됩니다.
- 시퀀서: 풀 DB의 트랜잭션을 조회하여 검증한 뒤 유효한 트랜잭션들을 묶어 배치로 처리하는 노드입니다. 모든 배치의 순서를 정렬하여 레이어1에 제출함으로써 작업한 배치가 레이어1 상태에 모두 반영되도록 합니다.
- 싱크로나이저¹⁶: 이더맨¹⁷을 통해 이더리움의 데이터를 조회하여 상태 DB를 업데이트합니다.
- 이더맨: 저수준¹⁸으로 구현된 구성 요소로 레이어1 네트워크 및 스마트 컨트랙트와의 모든 상호 작용을 처리합니다.
- 상태 DB: 상태 데이터(머클 트리¹⁹ 제외)를 영구적으로 저장하는 데이터베이스입니다.

¹⁰ Zero-knowledge node

¹¹ Sequencer

¹² Aggregator

¹³ MetaMask

¹⁴ Remote procedure call

¹⁵ Batch

¹⁶ Synchronizer

¹⁷ Etherscan

¹⁸ Low-level

¹⁹ Merkle tree

- 애그리게이터: 증명을 생성하여 시퀀서가 제출한 상태 변경 사항의 정확성을 검증하는 노드입니다. 애그리게이터가 생성하는 증명은 영지식 증명이며, 증명 생성을 위해 암호화 구성 요소(증명자)를 활용합니다.
- 증명자: 정교한 암호화 도구로서 트랜잭션 배치에 대한 영지식 증명을 생성하고 생성된 증명들을 하나의 영지식 증명으로 합산한 다음 유효성 증명²⁰ 형태로 공개합니다.

거버넌스

블록체인 생태계가 발전할수록 거버넌스 메커니즘 또한 중대한 변화를 겪게 됩니다. 메인넷 출시 이후 프롬 다오를 도입한 것도 같은 맥락입니다. 다오 도입은 프롬이 블록체인 분야에서 더욱 민주적이고 참여 지향적인 거버넌스 모델로 나아가는 과정을 나타냅니다.

프롬 네트워크 거버넌스의 진일보를 상징하는 프롬 다오는 네이티브 토큰²¹인 프롬(PROM)을 보유한 사용자가 네트워크가 나아갈 방향에 직접적으로 영향을 줄 수 있는 역할 기반 거버넌스 구조를 갖고 있습니다. 이 같은 구조를 통해 PROM 보유자는 투표권을 다른 다오 구성원에게 위임하여 네트워크의 의사 결정 과정에 참여하고 생태계 성장에 따른 혜택을 같이 누릴 수 있습니다.

프롬 다오의 기술적 프레임워크

프롬 다오의 거버넌스 모델은 투명하고 탈중앙화된 기반 환경을 갖추고 있어 선별된 참여자 그룹이 아닌 네트워크 커뮤니티 전체에 의해 의사 결정이 이루어집니다. PROM은 프롬 다오 거버넌스의 매우 중요한 요소로서 거버넌스 과정에서 일종의 지분이자 의결권 역할을 합니다.

- **의사 결정 과정**

프롬 다오는 핵심 컨트랙트 업그레이드, 취약점 해결, 성능 강화, 사용자 경험 개선 등 다양한 사안에 대해서 유연하게 의사 결정을 진행합니다. 이러한 과정을 거치며 네트워크는 사용자와 폭넓은 생태계의 요구에 맞춰 변화하고 대응합니다.

- **역할 기반 거버넌스 구조**

프롬 다오는 역할 중심의 명확한 체계를 활용해 거버넌스 절차를 간소화합니다.

²⁰ Validity proof

²¹ Native token

- 대리인: 다른 커뮤니티 구성원으로부터 투표권을 위임받은 PROM 보유자입니다. 프롬 다오 구성원의 이익을 대변하는 중요한 역할을 맡습니다.
- 검증인: 제품 개발 과정의 무결성을 유지하고 제안이 네트워크의 장기 비전에 부합하는지 확인합니다. 초기 투표 단계를 통과한 제안을 추가적으로 검토 및 검증하는 역할을 합니다.
- 구성원: 다오의 토대가 되는 주체로, PROM 보유한 사용자라면 누구나 다오에 참여할 수 있습니다. 제안을 제출하고 사안에 대한 투표를 진행하면서 네트워크 거버넌스에 기여합니다.

- **경제적 인센티브**

프롬 다오는 적극적인 참여를 유도할 수 있도록 강력한 인센티브 모델을 채택합니다. 대리인과 검증인에게 네트워크 수수료의 32%를 공유함으로써 네트워크의 경제적 성과와 네트워크 관리자들에게 분배되는 보상을 직접적으로 연결시킵니다. 이는 네트워크에 적극적이면서도 유의미하게 참여함으로써 네트워크의 거버넌스와 발전에 많은 기여를 하는 사용자들에게 적절한 보상을 제공하기 위함입니다.

- **토큰 위임 및 보상**

투표권을 위임하고자 하는 토큰 보유자는 프롬 거버넌스 포털에서 PROM을 락업²²한 뒤 투표권을 선택한 대리인에게 할당하면 됩니다. 투표권 위임 시스템은 토큰 보유자와 대리인 사이에 상생 관계를 형성하고, 두 주체 모두 네트워크 거버넌스 활동으로부터 이익을 얻을 수 있게 합니다.

토큰믹스

PROM은 프롬 생태계를 작동시키는 네이티브 토큰으로서 트랜잭션 실행, 거버넌스 참여, 커뮤니티 인센티브 등의 용도로 활용됩니다.

- 가스비²³: 트랜잭션과 컨트랙트 상호 작용이 원활하고 빠르게 처리될 수 있도록 돕습니다.
- 거버넌스: 보유자에게 의결권을 부여하여 네트워크의 미래를 함께 만들어 나갈 수 있도록 합니다.
- 접근 권한: 프롬 네트워크의 다양한 서비스를 이용하는 데 사용됩니다.
- 검증: 노드를 설정하여 생태계에 참여하는 데 사용됩니다.

²² Lockup

²³ Gas fee

잠금 해제 진행 상황



잠금 해제된 시가총액(UMC) ⓘ ₩76.47B

잠금 해제된 순환 공급량 (UCS) ⓘ 19.25M PROM

※ PROM 분배 및 유통 계획은 프로젝트에서 코인마켓캡²⁴에 제공한 자료를 토대로 작성되었으며, 향후 프로젝트의 사정에 따라 위 내용이 변경될 수 있습니다.

로드맵

프롬은 별도 로드맵을 공지하고 있지 않으나, 블로그 및 X(구 트위터) 등을 통해 사업 현황에 대한 공지를 상시로 진행하고 있습니다.

- 블로그 <https://prom.io/blog>
- X(구 트위터) https://x.com/prom_io

*상기 링크는 작성일 기준으로 유효한 링크이며 변경될 가능성이 있습니다.

²⁴ CoinMarketCap