

맨틀(Mantle)

해당 번역본은 이용자가 디지털자산 관련 정보를 편리하게 확인할 수 있도록
단순 참고용으로 번역된 것이며, 투자 권유를 목적으로 하지 않습니다.
그 내용이 정확하지 않을 수 있으므로 정확한 정보 습득을 위해서는
원문을 참고하시거나 원문 작성 주체 측에 문의하시기 바랍니다.
두나무는 해당 번역본 내용의 진실성 및 정확성을 보장하지 않고,
제공된 정보에 의한 투자 결과에 대하여 어떠한 책임도 지지 않으며,
투자 손실은 투자자에게 귀속됩니다.

개요

맨틀 네트워크는 이더리움을 위한 EVM 호환 확장 솔루션을 구축하는 데 전념하고 있습니다. 이는 이더리움에서 실행되는 모든 계약과 도구가 최소한의 수정으로 맨틀 네트워크에서도 작동할 수 있음을 의미합니다. 모듈식 아키텍처를 활용하여 맨틀 네트워크는 낙관적 롤업을 다양한 혁신적 데이터 가용성 솔루션과 결합하여 이더리움의 보안을 계승하면서 더 저렴하고 접근 가능한 데이터 가용성을 제공합니다.

우리의 프로토콜 설계 철학은 사용자에게 더 저렴하고 사용자 친화적인 경험을 제공하고, 개발자에게는 더 단순하고 유연한 개발 환경을 제공하며, 차세대 대규모 채택 디앱을 위한 포괄적인 인프라 세트를 제공하는 것을 목표로 합니다.

맨틀 네트워크의 주요 기능

- **롤업 기반**
 - 이더리움 검증자 및 합의 프로토콜을 활용하여 가스비를 크게 절감하고, 지연 시간을 줄이며, 처리량을 증가시킵니다. 사용자는 최소한의 보안 설정으로 거의 실시간에 가까운 확인 지연(latency)을 제공하기 위해 거래 확인 요건을 맞춤화할 수 있습니다.
- **모듈식 아키텍처**
 - 거래 실행, 합의, 결제, 저장을 동일한 네트워크 계층에서 처리하는 기존 모놀리식 체인과 달리, 맨틀은 이러한 기능을 모듈식 체인으로 분리합니다. 여기에는 거래 실행을 담당하는 맨틀이 개발한 EVM 호환 실행 레이어, 이더리움에서 수행되는 합의 레이어와 결제 레이어, 그리고 외부 DA 구성 요소(현재는 EigenDA 기술로 구동되는 맨틀 DA; EigenDA 메인넷이 안정적으로 출시되면 EigenDA로 전환 예정)가 포함됩니다.
- **이더리움 보안 기반**
 - L2 상태 전환은 이더리움 검증자에 의해 검증되며, L1 거래와 동일한 합의 및 결제 과정을 거칩니다.
- **모듈식 데이터 가용성**
 - EigenDA 기술과 같은 독립적인 DA 모듈. 내부 평가에 따르면, 이는 온체인 L1 대비 **90% 이상**의 비용 절감 효과를 제공합니다.

맨틀 OP Succinct 메인넷 업그레이드 및 출금 기간 전환

맨틀은 다가오는 **OP Succinct** 메인넷 업그레이드를 기쁜 마음으로 발표합니다. 업그레이드는 **2025년 9월 16일** 시작 예정입니다. 이번 업그레이드는 맨틀을 생태계 최대의 영지식 유효성 레이어 2로 전환하는 중대한 단계입니다. 상태 검증을 위해 영지식 증명을 통합함으로써 보안을 강화하고 사용자 경험을 근본적으로 개선합니다. 업그레이드 기간 동안 필수적인 계약 업데이트가 배포될 예정입니다. 사용자에게 가장 큰 영향은 맨틀 Canonical Bridge 출금 프로세스의 획기적인 개선입니다. 전환 과정에서의 투명성을 보장하고 혼란을 방지하기 위해, 출금 처리 방식을 확인해 주시기 바랍니다.

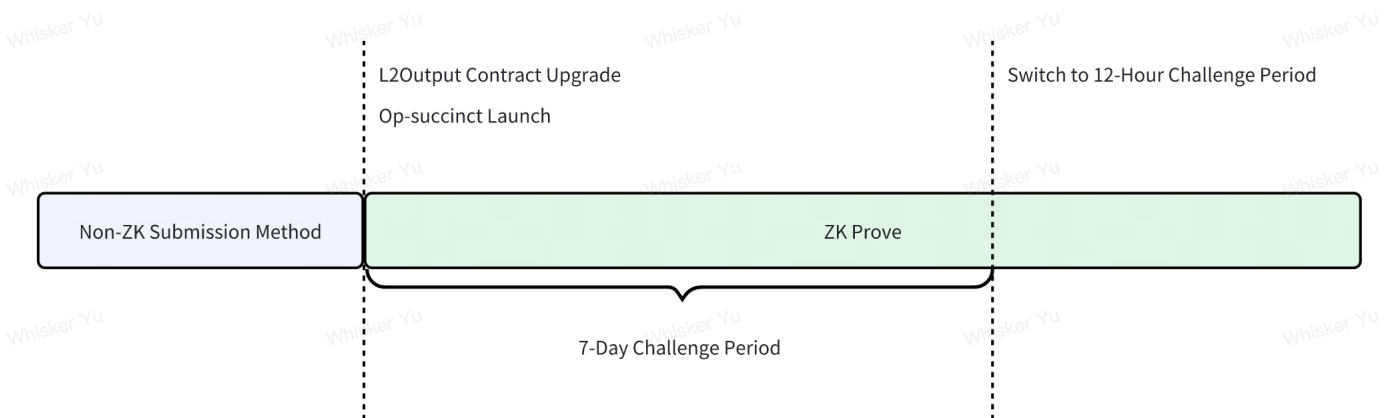
핵심 변화: 7일에서 12시간 출금으로 단축

이전에는 옵티미스틱 L2로서, 맨틀은 Canonical Bridge를 통한 모든 출금에 대해 7일간의 "챌린지 기간"을 요구했습니다. 이 지연은 모든 옵티미스틱 롤업에서 표준 보안 메커니즘으로, 네트워크 관찰자가 잠재적으로 부정확한 상태 전환을 검증할 수 있는 시간을 제공합니다. 영지식 유효성으로 전환하면서 네트워크 상태는 챌린지 기간 대신 암호학적 증명으로 확정됩니다. 이를 통해 출금 확정 기간을 7일에서 단 **12시간**으로 줄일 수 있습니다. 그러나 이 변경은 기존 시스템을 안전하게 종료하고 새로운 시스템을 활성화하기 위한 특정 전환 기간이 필요합니다.

왜 12시간으로 설정했는가?

12시간 챌린지 기간의 보안적 근거 영지식 증명 시스템은 이론적으로 훨씬 짧은 챌린지 기간을 허용하지만, 이를 12시간으로 설정한 것은 의도된 보안 조치입니다. 이 기간은 공식 브리지를 위한 중요한 안전 완충 역할을 합니다. 해킹과 같은 극단적인 보안 사건 발생 시, 이 시간은 팀이 대응하고 위험을 완화할 수 있는 충분한 시간을 제공하여 사용자 자산에 최대한의 보호를 보장합니다.

전환 타임라인 설명



업그레이드는 다단계 전개를 포함합니다. 요약하면, 7일 대기 기간의 근거는 다음과 같습니다. 영지식 Proposer 출시 이전에는 L2 상태 출력이 비-영지식 방식으로 제출되었습니다. 보안 모델에 따르면 이러한 과거 출력은 최종성과 보안을 보장하기 위해 원래의 7일 챌린지 기간을 완료해야 합니다. 따라서 매개변수 업데이트는 영지식 Proposer가 활성화된 후 7일 뒤에 실행되어, 비-영지식 방식으로 제출된 모든 데이터가 안전하게 확정되었음을 보장합니다. 아래는 정확한 일정과 출금을 시작하는 사용자가 예상해야 할 사항입니다:

- 1단계: 영지식 증명 시작 (2025년 9월 16일 ~15:00 UTC*)** 9월 16일부터 맨틀의 모든 새로운 상태 루트는 영지식 증명을 사용하여 제출 및 검증됩니다.
- 2단계: 전환 기간 (9월 16일 – 9월 23일)** 이 1주일 전환 기간 동안 새로운 상태 루트는 영지식으로 증명되지만, 브리지 계약에서는 기존의 7일 챌린지 기간 로직이 **유지**됩니다. 이는 옵티미스틱 시스템의 잔여 상태를 안전하게 확정하기 위해 필요합니다.
- 3단계: 새로운 표준 (2025년 9월 23일 ~15:00 UTC*)** 9월 23일 최종 계약 업그레이드가 활성화되면 새로운 12시간 출금 로직이 적용됩니다. 이후 이 짧아진 확정 기간은 **모든 진행 중 및 새로운 출금**에 적용됩니다.

*참고: 15:00 UTC (오후 3시 UTC)는 목표 활성화 시간입니다. 실제 활성화는 네트워크 상황에 따라 약간 다를 수 있습니다.

출금 시나리오: 내 자금은 어떻게 되는가?

이를 명확히 하기 위해, 업그레이드 동안 모든 시나리오를 실질적 예시로 설명합니다.

시나리오 1: 업그레이드 이전에 출금 시작 (예: 9월 14일)

- **상태:** 9월 16일 업그레이드 시작 전에 이미 출금이 챌린지 기간에 들어가 있습니다.
- **결과:** 기존 7일 챌린지 기간 전체를 기다려야 합니다. 새로운 로직은 구 옵티미스틱 시스템에서 이미 확정된 출금에는 소급 적용되지 않습니다.

시나리오 2: 전환 기간 동안 출금 시작 (예: 9월 18일)

이것이 가장 중요한 시나리오입니다. 영지식 증명이 시작된 이후, 그러나 12시간 규칙이 활성화되기 전에 출금을 시작했습니다.

- **9월 18일 – 9월 23일 동안:** 출금은 기존 7일 챌린지 기간에 들어갑니다. UI에는 "6일 남음," "5일 남음" 등 7일 카운트다운이 표시됩니다.
- **9월 23일 ~15:00 UTC 이후:** 새로운 12시간 규칙이 모든 진행 중 출금에 적용됩니다. 9월 18일부터 23일까지 이미 12시간 이상이 경과했으므로, 업그레이드가 완료되는 순간 출금은 **즉시 청구 가능** 상태가 됩니다.

시나리오 3: 최종 활성화 직전에 출금 시작 (예: 9월 23일 14:00 UTC)

최종 업그레이드가 활성화되기 단 1시간 전에 출금을 시작했습니다.

- **14:00 – 14:59 UTC 동안:** UI에는 기존 7일 챌린지 기간이 임시로 표시됩니다.
- **15:00 UTC 이후:** 새로운 12시간 규칙이 활성화됩니다. 시스템은 요구 조건을 재계산합니다. 14:00~15:00 사이 이미 1시간을 기다렸으므로, 출금 타이머는 자동으로 **11시간 남음**으로 업데이트됩니다.

이번 획기적인 업그레이드를 완료하는 동안 인내와 지지를 보내주셔서 감사합니다. 우리는 영지식 유효성의 보안과 훨씬 향상된 브리지 경험을 통해 차세대 확장을 제공하게 되어 매우 기쁩니다.

맨틀 네트워크 메인넷 v2 Everest 업그레이드

맨틀 Tectonic의 1년 이상 안정적 운영 이후, 우리는 자랑스럽게 **Everest 업그레이드**를 발표합니다. 이는 맨틀 네트워크의 중대한 도약입니다. 이번 업그레이드는 기존 인프라를 강화할 뿐 아니라, 다가오는 **이더리움 Pectra 업그레이드**에 완전히 대비하여 맨틀 네트워크와 원활한 호환성을 보장하고 미래 개발을 위한 견고한 기반을 마련합니다. Everest 업그레이드의 핵심 하이라이트 중 하나는 **EigenDA**의 공식 출시로, 이는 네트워크에 혁신적인 데이터 가용성 솔루션을 도입하여 데이터 관리 및 보안 효율성을 크게 향상시킬 것입니다.

맨틀 v2 Everest와 맨틀 v2 Tectonic 비교

EigenDA 통합

맨틀은 EigenDA와 긴밀한 협력을 유지해왔습니다. EigenDA 메인넷 출시 전, 맨틀은 DA 레이어로 EigenDA 기반의 제3자 DA 레이어인 맨틀 DA를 사용했습니다. 따라서 EigenDA가 출시되자, 맨틀은 즉시 테스트넷에서 마이그레이션을 완료하고, 운영 환경 테스트 후 최종적으로 맨틀 메인넷에 마이그레이션했습니다. EigenDA에 대한 자세한 정보는 [여기](#)를 확인하십시오.

이더리움 Pectra 업그레이드에 대한 L2 적응

이더리움은 곧 기대를 모으는 Pectra 업그레이드를 맞이합니다. 이더리움 L2로서, 맨틀은 Pectra 업그레이드로 인한 변화에 즉시 적응 작업을 시작했습니다. 여기에는 EIP-7685에서 블록 헤더에 새로 도입된 RequestsHash 필드와, EIP-7702에서 도입된 새로운 SetCodeTx 거래 유형이 포함됩니다.

새로운 기능 소개

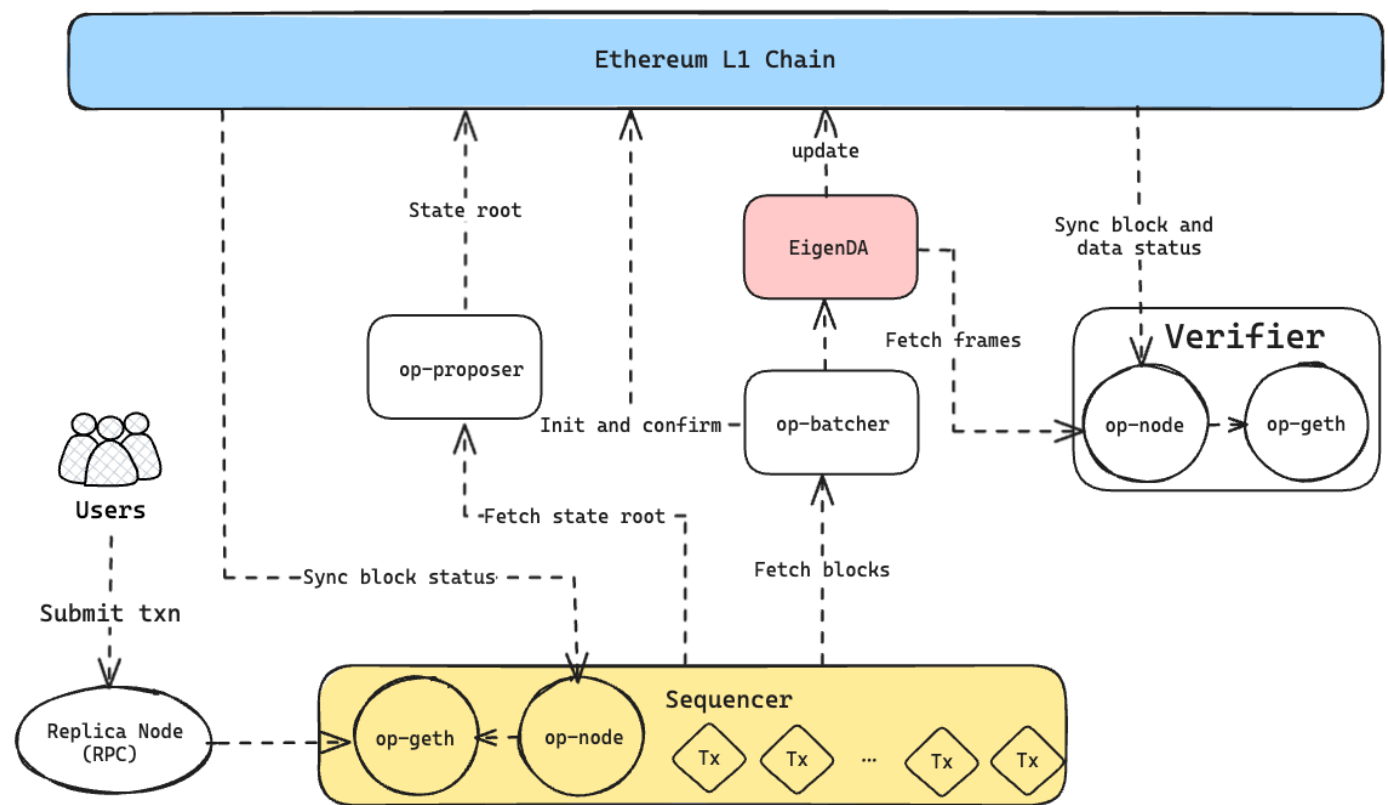
OP Stack Bedrock 위에서 빌드한 이후, 맨틀은 확장성 개발을 통해 op-geth의 기능 향상에 전념해 왔습니다. 이번 업그레이드에서는 새로운 RIP-7212 프리컴파일드 컨트랙트 지원이 도입되었으며, eth_getBlockReceipts jsonRPC 인터페이스가 추가되었습니다.

MetaTX 기능 지원 종료

맨틀이 독자적으로 개발한 MetaTX는 가스비 후원 기능을 제공하여 사용자가 맨틀 생태계에 진입하는 장벽을 최소화하는 것을 목표로 했습니다. 이더리움 Pectra 업그레이드에서 EIP-7702가 도입됨에 따라, 맨틀은 이를 기반으로 동일한 가스비 후원 기능을 제공할 예정이며, 따라서 MetaTX는 더 이상 지원되지 않습니다.

아키텍처

아키텍처 개요



이 다이어그램은 맨틀 v2 Tectonic에서 서로 다른 네트워크 모듈과 구성요소가 거래 실행을 통해 어떻게 상호작용하는지를 보여 줍니다. 이는 EigenDA가 지원하는 맨틀 데이터 가용성(DA)과 상호작용하여 롤업 데이터를 저장하고, 최종적으로 업데이트된 상태 데이터를 이더리움 L1에 게시하는 과정을 묘사합니다.

각 모듈의 동작을 더 잘 이해하기 위해 거래 처리 과정을 검토해 봅시다.

1. 사용자는 사용 가능한 RPC 노드를 통해 서명된 거래를 전송합니다.
2. 시퀀서는 거래를 수신하고 이를 블록으로 패키징합니다. op-batcher는 시퀀서로부터 데이터를 가져와 인코딩 및 압축을 수행한 뒤, 이를 DA 모듈에 전송하고 데이터 유효성 정보를 L1 컨트랙트에 제출합니다.

3. 마찬가지로, `op-proposer`는 시퀀서를 통해 패키징된 블록의 상태 루트를 가져와 L1의 관련 컨트랙트 `L2OutputOracle`에 전송합니다.
4. 롤업 거래 데이터는 맨틀 DA에 저장됩니다. 검증자는 언제든지 이 데이터를 검색하여 그 유효성을 검증할 수 있으며, 이는 사기 방지 증명(fraud-proof) 챌린지를 제기할 때 수행되는 과정입니다.

맨틀 네트워크의 온체인 및 오프체인 설계에 대해 더 알고 싶다면 [온체인 시스템](#)과 [오프체인 시스템](#) 페이지를 확인하십시오!

맨틀의 트랜잭션 풀

맨틀 v2 Tectonic에서는 거래가 블록에 포함될 때까지 임시로 저장하기 위해 이더리움의 메모풀과 유사한 트랜잭션 풀 구조가 도입되었습니다. L2에서 트랜잭션 풀을 도입한 목적은 거래 패키징을 개선하기 위함입니다. 맨틀 v2 Tectonic은 [EIP-1559](#) 거래 유형을 지원하므로, 사용자는 거래의 우선순위 수수료(priority fee)를 조정하여 거래 패키징 속도를 제어할 수 있습니다. 트랜잭션 풀은 아직 패키징되지 않은 거래를 임시로 저장하는 데 사용됩니다.

그러나 트랜잭션 풀 도입은 Miner Extractable Value(MEV)의 영향과 같은 특정 과제를 야기하기도 합니다. 따라서 맨틀 v2 Tectonic에서는 TX 풀을 프라이빗으로 설계했습니다. 거래를 제출하려면 `op-geth`를 구성하여 거래를 시퀀서로 전송해야 합니다. 그러면 시퀀서는 기본 수수료(base fee)와 우선순위 수수료(priority fee)의 순서에 따라 트랜잭션 풀의 거래를 처리합니다.

트랜잭션 라이프사이클

L2 -> L1 워크플로우

1. 시작 단계

월렛 사용자, 디앱, 또는 일부 스크립트는 자금 이체 또는 작업 실행을 위해 블록체인 기반 시스템을 활용하고자 할 수 있습니다.

- 사용자 측에서는, 지갑에 시퀀서 노드의 RPC 엔드포인트를 추가하여 맨틀 네트워크에 연결했습니다.
- 반면 디앱은 [맨틀 SDK](#)를 통합하고 이를 인스턴스화하여 맨틀 네트워크와 통신합니다. 이들은 수신자 주소와 전송하려는 금액을 포함하는 요청을 전송할 준비가 되어 있습니다.

다른 서비스와 마찬가지로, 이 작업에는 비용 지불이 필요합니다. 이는 단지 이체 자체를 위한 것뿐만 아니라, 누구나 검증할 수 있는 영구적이고 불변의 공공 기록을 유지하기 위한 비용이기도 합니다. 이들의 월렛 또는 디앱은 이 작업을 실행할 충분한 잔액이 있는지 확인해야 합니다.

- 월렛의 경우, 요구되는 수수료를 계산하기가 더 쉬우므로 상황이 단순합니다.
- 디앱은 보다 상세한 계산이 필요합니다. 자세한 내용은 이 [섹션](#)을 참조하십시오.

이들은 수중의 도구를 사용해 요청을 구성하고, 개인 키로 서명한 뒤, 시퀀서가 이를 처리할 준비가 되어 있는 맨틀 네트워크로 전송합니다. 이 지점이 거래가 처음으로 맨틀에 진입하는 곳입니다. 자세한 내용은 [여기](#)를 참조하십시오.

2. 처리 단계

거래는 이들 노드에서 실행되는 이더리움 가상머신(EVM) 소프트웨어(`op-geth`)에 의해 표준 상태 검증 과정을 트리거합니다. 이는 거래가 근본적으로 유효하며, 필요한 수수료가 지불되었고, 예외적인 상황이 발생하지 않았음을 보장하기 위한 것입니다. 상태 전이가 완료된 후, `op-proposer`는 새로운 상태의 머클 루트를 제안하고 해당 L1 컨트랙트에 제출합니다.

상태 제출은 모든 거래마다 수행되어야 하는 것은 아니며, tx-batch 이후에 제출하도록 선택할 수 있다는 점에 유의해야 합니다.

거래는 로컬 상태(원장)를 업데이트하고 보류 중인 블록의 일부로서 추가 처리를 기다립니다. 지금까지의 과정은 특히 빠릅니다. 이러한 보류 블록 다수가 결합되어 배치(batches)를 형성하고, 이는 `op-batcher`에 의해 인코딩 및 압축되어 최종 결제를 위해 이더리움으로 전송됩니다. L2는 하나의 배치에 포함된 다수의 거래에 고정 비용을 분산함으로써 낮은 거래 수수료를 달성합니다.

op-batcher의 인코딩 및 압축 과정에 대한 자세한 내용은 이 [페이지](#)를 참조하십시오.

3. 저장 단계

일반적인 롤업과 달리, 맨틀 네트워크는 보다 효율적이고 비용 효율적인 데이터 가용성(DA) 보장을 목표로 합니다. 따라서 제3자 DA 구성요소를 기반으로 개발된 EigenDA를 선택합니다. op-batcher는 L2 네트워크의 무결성과 유효성을 보장하기 위해 모든 거래 데이터(원시 거래가 아님)를 EigenDA에 제출해야 합니다. DA 노드들은 블록 데이터를 동기화하고, 이 서비스를 제공한 대가로 보상을 받는 동시에 언제든지 해당 데이터에 접근할 수 있도록 보장합니다. 더 자세한 정보는 이 섹션을 참조하십시오.

EigenDA는 데이터 저장과 역파생(reverse derivation)을 지원하여 데이터 가용성을 보장합니다. 데이터 저장 외에도 상태 저장 역시 중요합니다.

이더리움에서는, 컨트랙트에 저장된 업데이트된 상태 루트를 검증할 준비가 된 완전한 신뢰 네트워크가 존재합니다. 블록이 이더리움의 합의 메커니즘을 통과하면, 이는 보안 체인에 기록됩니다. 업로드된 상태 루트가 챌린지 기간(일반적으로 7일)을 통과하면 상태 전이는 유효한 것으로 간주됩니다.

온체인 시스템

컨트랙트 소개

맨틀 네트워크의 온체인 모듈에는 블록체인에서 실행되어 탈중앙화되고 신뢰할 수 있는 실행을 보장하는 일련의 스마트 컨트랙트가 포함됩니다. 이 컨트랙트들은 블록체인과 상호작용하는 다양한 디앱의 로직을 처리하며, 오프체인 시스템과 온체인 시스템 간의 상호작용(자산 이전, 자산 스왑 등)을 포함합니다.

컨트랙트 설명

L1CrossDomainMessengerProxy

이 컨트랙트는 L2의 L1CrossDomainMessenger 컨트랙트에 대한 프록시이며, L1에서 L2 컨트랙트와의 상호작용에 사용할 수 있습니다.

L1CrossDomainMessenger 컨트랙트는 맨틀 네트워크(L1에서 L2)로 메시지를 보내고 수신하기 위한 상위 수준 인터페이스입니다.

L1StandardBridgeProxy

이 컨트랙트는 L2의 L1StandardBridge 컨트랙트에 대한 프록시이며, L1에서 L2 브리지와의 상호작용에 사용할 수 있습니다.

L1StandardBridge는 맨틀 네트워크/에서 ERC20 토큰을 전송하기 위한 표준화된 컨트랙트입니다.

L1ERC721BridgeProxy

맨틀 네트워크/에서 ERC721 토큰을 전송하기 위한 프록시 컨트랙트입니다.

L2OutputOracleProxy

맨틀 네트워크의 상태에 대한 커밋먼트를 저장하는 프록시 컨트랙트로, L1의 컨트랙트가 L2 상태에 접근하는 데 사용할 수 있습니다.

OptimismMintableERC20FactoryProxy

ERC20 토큰을 발행하는 팩토리 컨트랙트의 프록시 컨트랙트입니다.

OptimismPortalProxy

저수준 메시지 전달 인터페이스의 프록시 컨트랙트입니다.

ProxyAdmin

컨트랙트의 관리자 컨트랙트로, 모든 프록시 컨트랙트의 소유자입니다. 이는 맨틀의 대부분 시스템 컨트랙트를 업그레이드하는 데 사용할 수 있습니다.

SystemConfigProxy

온체인 시스템을 위한 구성 값을 저장하는 시스템 컨트랙트의 프록시 컨트랙트입니다.

AddressManager

AddressManager는 맨틀 시스템의 구버전에서 문자열 이름을 주소에 매핑하는 레지스트리를 관리하는 데 사용되던 레거시 컨트랙트입니다.

오프체인 시스템

컨트랙트 소개

오프체인 시스템은 맨틀 네트워크의 또 다른 핵심 모듈입니다. 이는 블록체인 외부의 환경에서 특정 작업과 로직을 실행하는 책임을 지며, L2가 L1을 확장하고 더 효율적이고 빠른 응답 및 실행을 제공할 수 있게 하는 핵심입니다.

BVM_GasPriceOracle

L2 가스 가격 구성 값을 저장합니다. 가스비를 더 안정적으로 유지하기 위해 tokenRatio 매개변수를 제공합니다.

L1_BLOCK_NUMBER

L1 블록 컨텍스트 정보(예: 최신으로 알려진 L1 블록 해시)를 저장합니다.

L2CrossDomainMessenger

L1로 메시지를 보내고 L1로부터 메시지를 수신하기 위한 상위 수준 인터페이스입니다.

L2StandardBridge[

L1로/에서 ERC20 토큰을 전송하기 위한 표준화된 시스템입니다.

L2_TO_L1_MESSAGE_PASSER

저수준 메시지 전달 인터페이스입니다.

BaseFeeVault

L2 BaseFee 거래 수수료를 위한 금고(vault)입니다. 자세한 내용은 [여기](#)를 참조하십시오.

BVM_SequencerFeeVault

BaseFee를 제외한 L2 거래 수수료를 위한 금고입니다. 자세한 내용은 [여기](#)를 참조하십시오.

L1Block

L1Block은 사용자에게 마지막으로 알려진 L1 블록에 대한 정보 접근을 제공합니다.

OptimismMintableERC20Factory

OptimismMintableERC20Factory는 배포된 네트워크에서 OptimismMintableERC20 컨트랙트를 생성하는 팩토리 컨트랙트입니다.

노드 소개

네트워크 역할

Sequencer

시퀀서는 네트워크의 블록 제작자 역할을 하며, 맨틀에서는 [op-node](#)와 [op-geth](#)로 구성되며 다음 기능을 수행합니다:

- 사용자로부터 오프체인 거래를 수락
- L1에서의 사용자 예치 거래를 모니터링
- L2에서 블록 생성

Verifier

검증자는 네트워크에서 사용자에게 롤업 데이터를 제공하기 위해 존재하며, 역시 [op-node](#)와 [op-geth](#)로 구성되고 다음 기능을 수행합니다:

- 맨틀 DA로부터 롤업 데이터를 동기화
- L2에서 op-proposer가 제출한 상태 루트를 검증
- 잘못된 상태 데이터가 감지되면 사기 증명(fraud proof)을 개시
- 검증된 블록 데이터와 상태를 사용자에게 제공

op-batcher

op-batcher는 네트워크에서 DA 제공자와 상호작용하는 핵심 구성요소입니다. 또한 거래 패키징과 L1 업로드를 처리하며, 구체적인 기능은 다음과 같습니다:

- 시퀀서에서 데이터를 가져와 다양한 구성에 따라 프레임으로 처리(인코딩 및 압축)하고, 프레임을 [채널](#)로 저장
- 채널을 통해 DA 제공자와 상호작용하여 배치된 거래 정보를 제공
- 처리된 배치 거래를 L1에 업로드

op-proposer

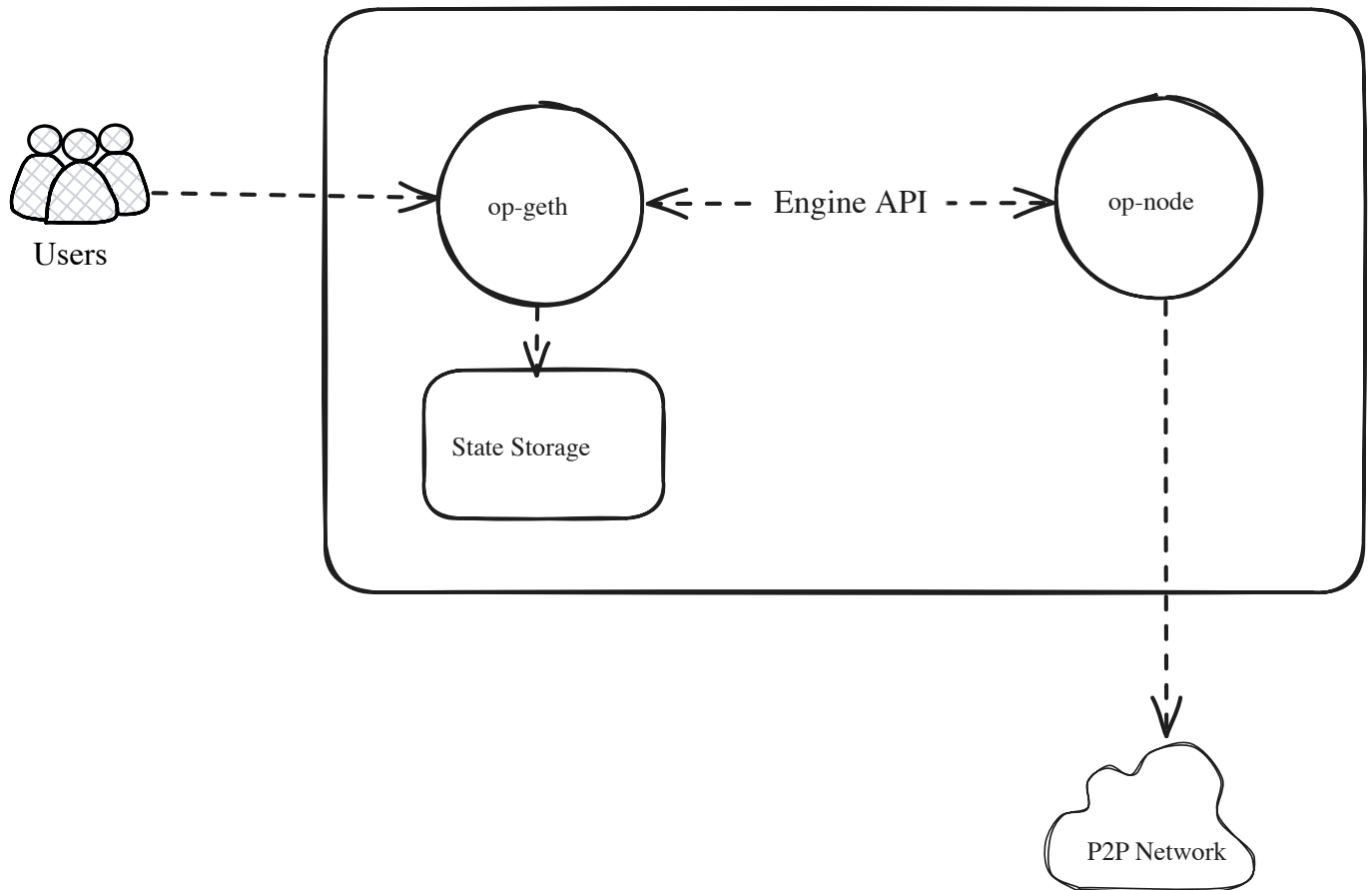
op-batcher와 유사하지만 상태 루트 정보를 제공합니다. 단일 또는 배치 거래를 제출할 때, op-proposer는 op-geth를 통해 상태 변화를 완료하고, L1의 L2OutputOracle로 전송되는 상태 커밋먼트를 기록해야 합니다.

DA 노드

맨틀 DA의 노드들은 DA 네트워크를 형성하며 맨틀 거래 데이터의 사본을 저장할 책임이 있습니다. 이들은 자신들이 제공하는 블록 데이터에 BLS 서명 스킴을 사용해 서명하여 가용성에 대한 커밋을 수행합니다. 이러한 서명은 이더리움의 EigenDA 컨트랙트에 의해 검증됩니다.

노드 심층 분석

시퀀서와 검증자 내부에는 서로 다른 두 구성요소가 존재합니다:



op-geth

맨틀 네트워크의 실행 클라이언트로서, op-geth는 다음 기능을 수행합니다:

- op-node로부터 수신한 블록을 실행하고 상태를 저장
- 엔진 API를 통해 블록체인 데이터를 조회하고 네트워크에 거래를 제출

op-node

맨틀 네트워크의 합의 클라이언트로서, op-node는 다음 기능을 수행합니다:

- L1로부터 L2 블록을 도출
- 엔진 API를 통해 블록을 op-geth에 전송
- 이후 유효성 검증을 위해 맨틀 DA에서 블록 정보를 가져옴
- P2P 네트워크와 동기화하여 시퀀서가 구성했지만 아직 제출되지 않은 블록을 동기화

EigenDA

소개

아이겐레이어(EigenLayer)란 무엇인가?

아이겐레이어는 이더리움의 기존 신뢰 네트워크를 재스테이킹으로 활용하는 프로토콜로, 어떤 롤업 기반 L2라도 실행 레이어의 데이터 가용성을 보장하면서 이더리움 메인넷과 동일한 보안 수준을 유지할 수 있도록 합니다. 이는 리스테이킹 메커니즘을 통해 달성되며, L1 검증자는 담보로 스테이킹한 ETH를 사용하고 추가적인 성능 조건을 준수하면서 데이터 가용성 서비스를 제공하기로 선택할 수 있습니다.

왜 EigenDA인가

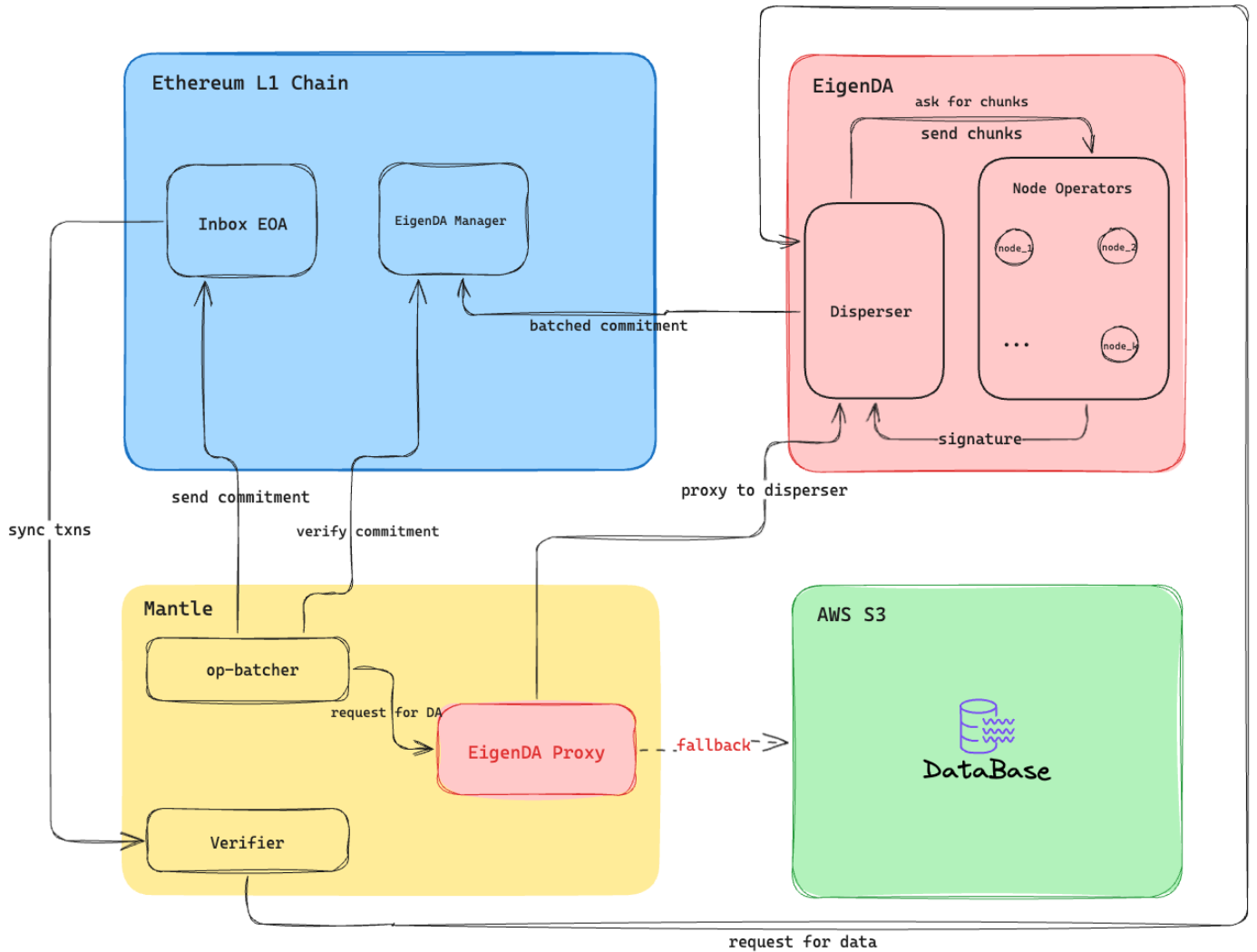
EigenDA는 이더리움 L2를 위해 설계된 초확장형 데이터 가용성(DA) 솔루션입니다. 그 핵심 임무는 L2가 보안과 비용 효율성을 유지하면서 확장성 한계를 극복하도록 돕는 것입니다.

이더리움의 **EIP-4844**가 L2 데이터 가용성 비용을 크게 낮추는 **Blob**을 도입했음에도, **EigenDA**는 다음과 같은 핵심 장점으로 여전히 매력적인 선택지입니다:

- **비용 효율성**
 - Blob이 데이터 가용성 비용을 낮추지만, 특정 상황에서는 EigenDA가 더 경쟁력 있는 가격을 제공할 수 있습니다. 이는 Blob 시장 혼잡도, EigenDA의 운영 효율, 특정 L2 요구사항 등 요소에 따라 달라집니다. EigenDA의 비용은 **MB당 몇 센트** 수준으로, 대체 솔루션보다 현저히 낮습니다.
- **탄력적 확장성**
 - 이더리움이 Blob 용량 확대 방안을 계속 모색하는 동안, EigenDA는 L2의 증가하는 데이터 가용성 수요를 충족할 수 있는 우수한 확장성을 제공합니다. 프로토콜 업그레이드에 의존하지 않고 필요에 따라 동적으로 용량을 확장할 수 있는 아키텍처를 갖추고 있습니다.
- **탈중앙 보안**
 - EigenDA는 경제적 인센티브를 갖춘 탈중앙 설계를 채택하여 데이터 저장의 신뢰성과 보안을 보장합니다. 이는 높은 데이터 무결성과 검열 저항성을 요구하는 L2에 필수적입니다.
- **크로스체인 상호운용성**
 - EigenDA는 L2에 더 큰 상호운용성 가능성을 제공합니다. EigenDA를 통해 L2는 다른 L2나 블록체인 네트워크와 데이터를 공유하여 보다 유연한 크로스체인 상호작용을 구현할 수 있습니다. 이는 상호 연결된 블록체인 생태계를 구축하는 데 필수적입니다.
- **맞춤형 서비스**
 - EigenDA는 L2가 고유한 필요에 맞춰 데이터 가용성 솔루션을 조정할 수 있도록 하여, 다양한 사용 사례에 대해 뛰어난 적응성을 제공합니다.

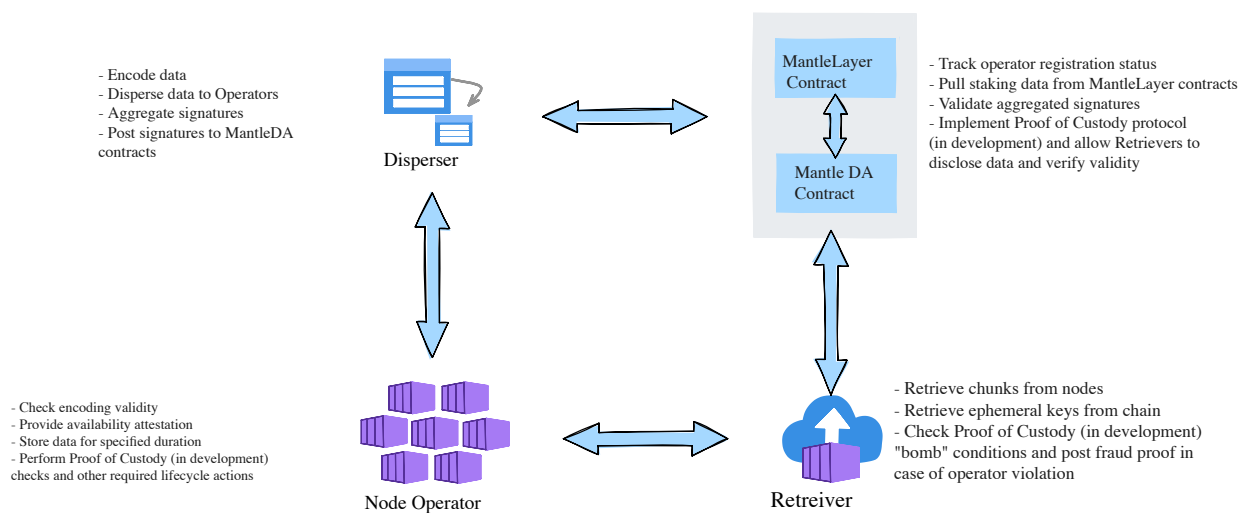
아키텍처

아키텍처 개요



구성요소

EigenDA 기술로 지원되는 맨틀 DA는 상호작용 세트와 함께 네 가지 주요 구성요소로 이루어져 있습니다:



오퍼레이터 노드 / DA 노드:

오퍼레이터는 DA 네트워크의 서비스 제공자로, 아이겐레이어를 통해 참여 담보를 서명으로 확약합니다. 오퍼레이터는 네트워크에서 일정 기간 동안 데이터 청크를 저장하고, 요청 시 해당 청크를 제공하는 노드를 운영합니다. EigenDA 오퍼레이터의 [주소 목록은 여기에서](#) 확인 할 수 있습니다.

디스퍼서(Dispersers)

EigenDA 서비스의 역할로서, 자신의 데이터 가용성에 대한 재정적 보증을 위해 비용을 지불합니다. 이 역할은 롤업 시퀀서가 수행할 수 있습니다. 디스퍼서는 다음 작업을 수행합니다:

- 데이터를 청크로 인코딩하고, 정해진 기간 동안 데이터 가용성을 보장하기 위한 자금을 제공하며, 인코딩된 청크를 EigenDA 오퍼레이터에게 배포
- 오퍼레이터의 서명을 집계하고 블록체인에 증명을 게시하여, 특정 기간 동안 관심 데이터의 가용성을 확정

리트리버(Retrievers)

Proof of Custody 프로토콜에서 중요한 역할을 수행하는 이해관계자입니다. 리트리버는 다음 작업을 수행합니다:

- EigenDA 오퍼레이터의 블록 청크를 조회하고, 블록 청크가 정확한지 검증하며, 사용자를 위해 원본 블록을 재구성
- 무허가(permissionless) 방식으로 유해(toxic) 운영을 온체인에서 해결하도록 강제하여 오퍼레이터의 스테이크를 슬래시

현재 맨틀에서는 리트리버 기능이 디스퍼서에 통합되어 있어, 별도의 리트리버 노드는 없습니다.

EigenDA 매니저 및 인박스 스마트 컨트랙트:

이더리움에서 실행되는 DA 관련 스마트 컨트랙트 모음은 다음을 담당합니다:

- EigenDA Manager는 디스퍼서가 제출한 블록 커밋먼트를 수신하고, op-batcher가 블록 커밋먼트를 검증할 수 있도록 지원하는 책임을 집니다.
- 인박스 컨트랙트는 op-batcher의 EigenDA 검증된 커밋먼트를(콜데이터로서) 수신하는 역할을 담당합니다.

워크플로우

데이터 제출

op-batcher는 맨틀 거래 데이터를 EigenDA 프록시를 통해 EigenDA 디스퍼서로 전송합니다.

데이터 샤딩 및 배포

EigenDA 디스퍼서는 수신한 데이터를 청크로 분할하고, 이를 EigenDA 오퍼레이터 노드에 분산하며, 각 노드는 할당된 청크를 저장합니다.

저장 검증 및 커밋 생성

오퍼레이터 노드는 저장 서명을 EigenDA 디스퍼서로 반환하고, 디스퍼서는 이러한 서명을 집계하여 블록 커밋먼트를 생성합니다.

L1로의 배치 커밋 제출

EigenDA 디스퍼서는 주기적으로 블록 커밋먼트(메타데이터 + 서명)를 이더리움 L1의 EigenDA Manager 컨트랙트에 기록합니다 (예: 10분마다).

상태 확인 폴링

op-batcher는 EigenDA에 대한 데이터 제출 성공을 확인하기 위해 EigenDA 디스퍼서의 GetBlobStatus 인터페이스를 폴링합니다.

온체인 커밋 검증

확인되면, op-batcher는 L1의 EigenDA Manager 컨트랙트를 통해 블록 커밋먼트(메타데이터 + 서명)의 유효성을 검증합니다.

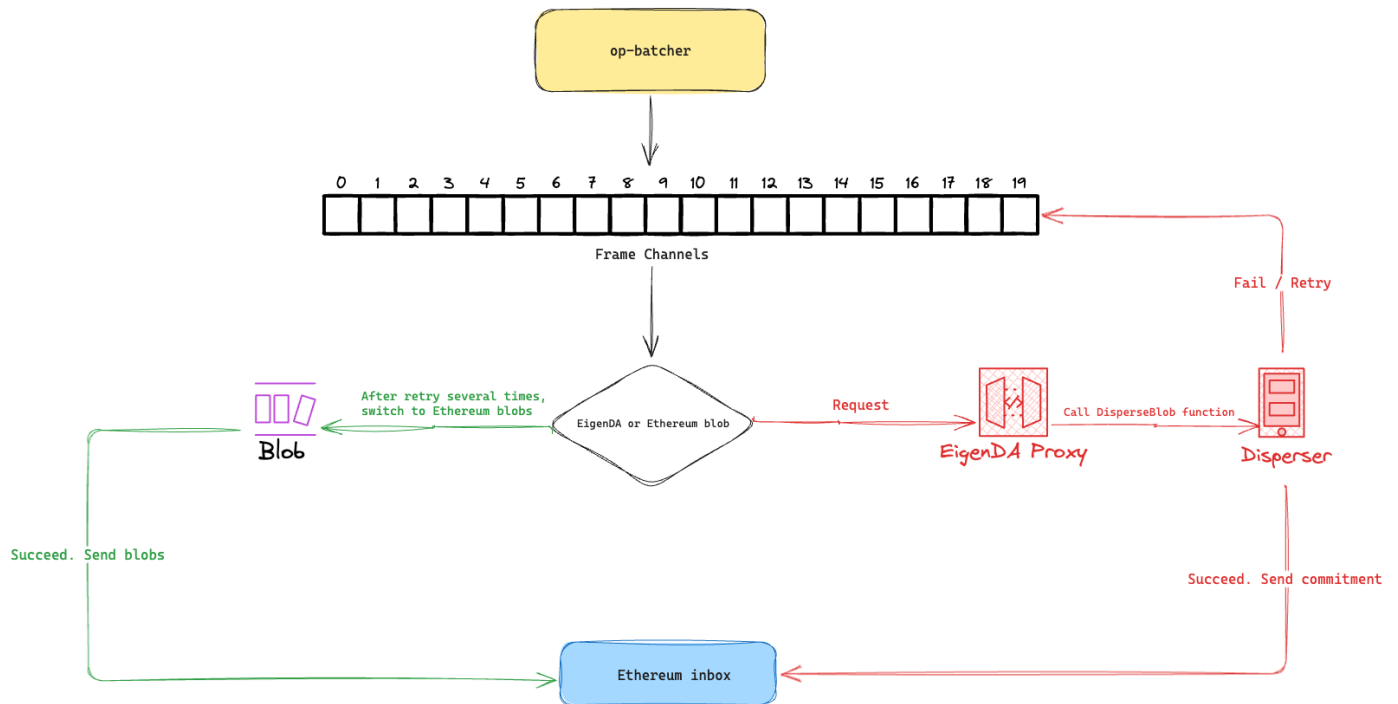
최종 커밋 제출

op-batcher는 EigenDA가 생성한 커밋을 거래 콜데이터로서 L1 인박스 컨트랙트에 제출합니다.

L1 <--> L2 데이터 플로우

강건한 L2를 위해, 안정적인 데이터 플로우에는 L2에서 L1로의 배치 제출과 L1에서 L2로의 도출이 포함됩니다. 맨틀 v2 Tectonic은 Bedrock 업그레이드와의 호환성을 보장하여, EigenDA와의 네이티브 데이터 플로우 및 상호작용을 가능하게 합니다.

배치 제출



배치 제출은 L2에서 DA 레이어로 데이터 프레임 전송하는 과정입니다. 데이터 프레임은 채널 형태로 저장되며 목적지(DA 레이어)로 전송되고, 그곳에서 검증자가 데이터의 가용성을 검증할 수 있습니다.

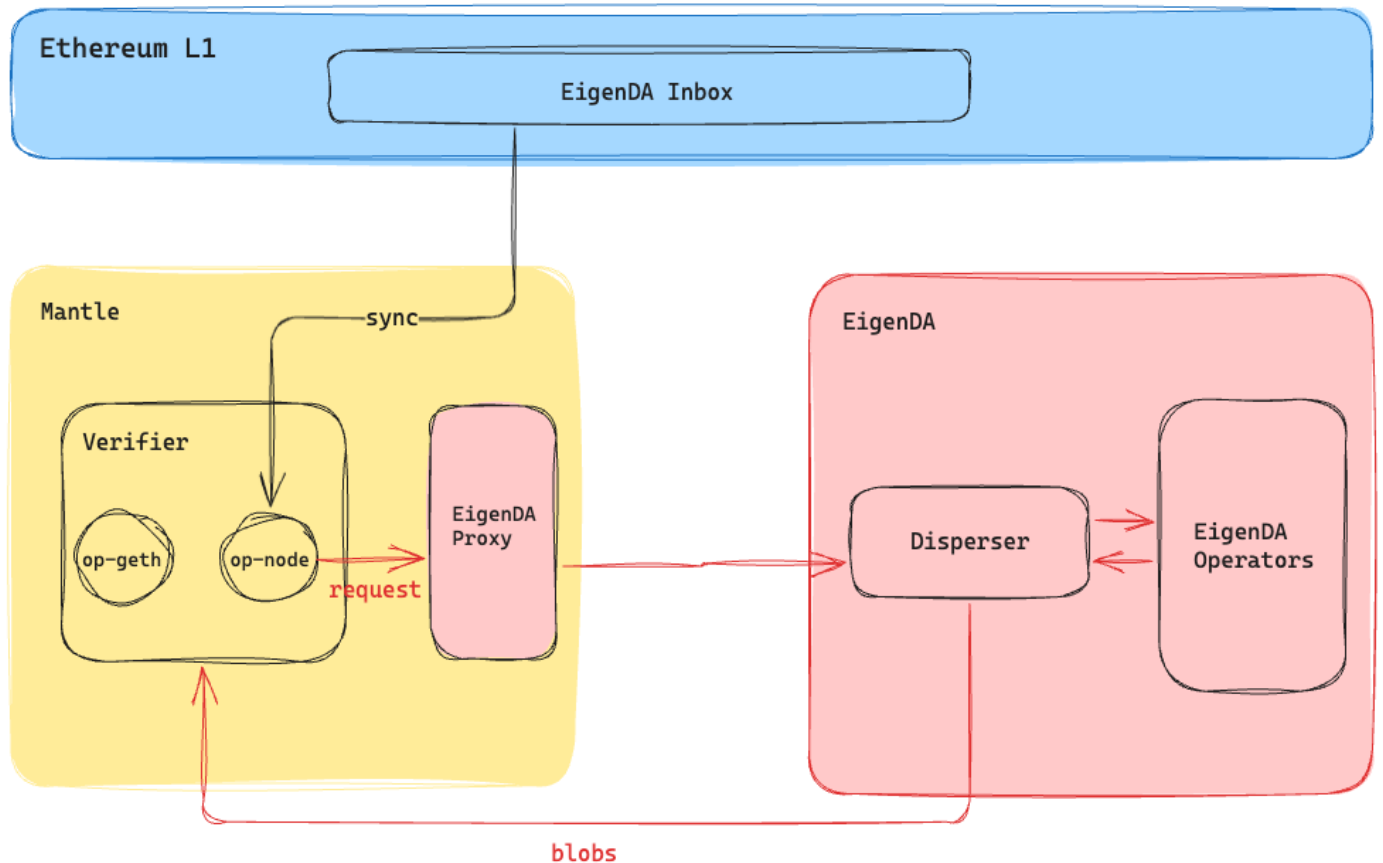
간단히 말해, 맨틀은 우선 EigenDA에 데이터를 커밋하려 시도하고, 오류가 발생하면 이더리움 블록으로 커밋하는 방식으로 폴백하여 맨틀 데이터 가용성을 보장합니다.

워크플로우

1. op-batcher는 먼저 블록 데이터를 EigenDA Disperser에 기록하려고 시도합니다. 기록이 성공하면, EigenDA는 BatchHeaderHash와 같은 정보를 반환합니다.
2. 동시에, 데이터 보안을 위해 EigenDA Proxy는 백업용으로 블록의 사본을 AWS S3 스토리지에 제출합니다. AWS S3 제출의 성공 여부와 무관하게, 이는 메인 프로세스의 반환 결과에 영향을 주지 않습니다. 이는 EigenDA Disperser에 문제가 발생하더라도 AWS S3에서 데이터를 복구할 수 있도록 보장합니다.
3. op-batcher가 EigenDA Disperser에 블록 데이터를 성공적으로 기록할 수 없는 경우(DisperseBlob 실패), 이더리움 블록 제출로 폴백합니다.
4. 이 경우, op-batcher는 전체 트랜잭션 데이터를 이더리움 블록 트랜잭션으로 제출하고, 블록 트랜잭션의 트랜잭션 해시를 콜대이터로 패키징하여 메인넷 Inbox 컨트랙트에 제출합니다.

서로 다른 커밋 유형을 구분하기 위해, op-batcher는 커밋의 콜대이터에 type 필드를 추가하여 이것이 EigenDA 커밋인지, 이더리움 블록 트랜잭션 커밋인지를 표시합니다.

파생(Derivation)



파생은 DA 레이어에서 데이터를 가져와 L2에서 이를 도출하여 모든 L2 노드의 상태가 일관되도록 보장하는 과정입니다. L2의 **op-node**는 서로 다른 DA 레이어에서 데이터 프레임을 가져와 L2의 상태 재구성을 완료합니다.

워크플로

- op-node는 L1 Inbox 컨트랙트의 트랜잭션을 폴링합니다.
- Inbox 컨트랙트의 트랜잭션 유형에 따라, op-node는 서로 다른 데이터 소스에서 DA 데이터를 가져옵니다:
 - EigenDA 데이터:** EigenDA를 사용하는 트랜잭션인 경우, op-node는 쿼터의 커밋먼트(예: BatchHeaderHash 및 BlobIndex)를 기반으로 EigenDA Proxy에서 데이터를 가져옵니다.
 - 이더리움 블록 데이터:** 블록 트랜잭션(EIP-4844로 폴백)인 경우, op-node는 이더리움 비콘 노드에서 데이터를 가져옵니다.

수수료 메커니즘

맨틀 네트워크에서의 수수료 기본 이해

맨틀 네트워크의 트랜잭션 수수료는 이더리움과 유사합니다. 그러나 맨틀 네트워크가 레이어 2(L2) 블록체인으로 동작하기 때문에, 이더리움의 수수료와 구별되는 새로운 패러다임이 수수료 구조에 존재합니다.

맨틀 네트워크가 지속적으로 EVM 호환성을 향상함에 따라, 디앱은 최소한의 수정으로 변화에 쉽게 적응할 수 있습니다. 맨틀에서의 트랜잭션 비용의 두 가지 원천을 살펴보겠습니다:

- L2 실행 수수료**
 - L2에서 트랜잭션을 실행하는 비용

2. L1 롤업 수수료

- 롤업 상태 루트를 L1에 제출하는 비용(배치에 포함된 사용자들 사이에 균등 분배)
- L1의 DA 컨트랙트에 제출되는 데이터 자격 증명 기록 비용

L2 실행 수수료

이더리움과 유사하게, 맨틀 네트워크의 트랜잭션은 사용된 연산 및 저장 자원에 대한 가스비를 지불해야 합니다. 각 L2 트랜잭션은 일부 실행 수수료를 발생시키며, 이는 트랜잭션에 연관된 가스 가격과 사용된 가스의 곱으로 계산됩니다.

수식으로 나타내면 다음과 같습니다:

$$L2ExecutionFee = L2GasPrice * L2GasUsed \quad (1)$$

이 수수료는 L2 네트워크에서 트랜잭션을 완료하는 데 드는 연산 및 실행 비용을 반영합니다. 사용자가 지불하는 L2 실행 수수료는 자신들의 트랜잭션이 소비한 연산 및 네트워크 자원에 비례합니다.

L1 롤업 수수료

트랜잭션 실행으로 인해 L2에서 생성된 모든 상태 루트는 이더리움에 게시됩니다. 이 단계는 L2의 보안 특성에 필수적이며, L2 네트워크의 최신 블록 데이터가 동기화 노드를 위해 일관되게 이더리움 L1에서 이용 가능하도록 보장합니다.

L2는 상태와 필수 트랜잭션 데이터를 배치로 집계하여 이더리움에 게시하며, 그 비용은 배치에 포함된 사용자들 사이에 분배됩니다. L1 롤업 수수료는 다음과 같은 요소를 기반으로 계산됩니다:

- 이더리움의 현재 가스 가격
- 고정 overhead(L1에 데이터를 커밋하기 위한 고정 비용으로, 자동 조정되어 가스 오라클에 설정됨)
- 스케일링 계수 scalar
- L1에서 콜데이터로 저장되는 트랜잭션 크기와 관련된 매개변수 rollupDataGas

overhead와 scalar와 같은 값은 [BVM_GasPriceOracle](#) 컨트랙트 또는 [SystemConfigProxy](#) 컨트랙트를 통해 얻을 수 있습니다.

overhead와 scalar는 [BVM_GasPriceOracle](#) 컨트랙트에서 조회할 것을 강력히 권장합니다. L1 컨트랙트는 업데이트 지연이 발생할 수 있습니다.

수식으로 나타내면 다음과 같습니다:

$$L1RollupFee = (rollupDataGas + overhead) * L1gasPrice * scalar \quad (2)$$

이 수수료는 L2에서 L1로 트랜잭션 배치를 통합 및 제출하는 데 드는 연산 비용(데이터 저장에 필요한 가스 및 추가 오버헤드 포함)을 포괄합니다. L1 롤업 수수료는 전체 시스템의 안전한 운영을 보장하는 핵심 구성 요소이며, 전체 트랜잭션 비용에도 영향을 미칩니다.

더 심층적인 이해를 위해, 롤업의 수수료에 관한 맨틀 리서치 팀의 연구를 읽어 보시기 바랍니다: [Transaction Fees on Rollups](#)

맨틀 v2에서의 수수료 이해

맨틀 v2에서는 맨틀의 네이티브 토큰 설계에 [tokenRatio](#) 매개변수를 도입하여 수수료를 조정합니다:

$$L2ExecutionFee = L2gasPrice * L2gasUsed * tokenRatio \quad (3)$$

$$L1RollupFee = (rollupDataGas + overhead) * L1gasPrice * tokenRatio * scalar \quad (4)$$

맨틀 v2의 L2 실행 수수료

L2 실행 수수료의 크기는 주로 L2에서 트랜잭션을 실행하는 비용을 직접 형성하는 두 가지 핵심 요소에 의해 영향을 받습니다.

$$L2ExecutionFee = L2gasPrice * L2gasUsed * tokenRatio \quad (5)$$

이 요소들을 자세히 살펴보겠습니다:

L2 gasUsed - 트랜잭션 실행의 복잡도

L2 gasUsed는 레이어 2에서 트랜잭션을 실행하는 데 소비된 가스의 양입니다. 이 값은 트랜잭션의 복잡도와 직접적으로 관련되며, 컨트랙트 실행, 연산, 데이터 처리에 수반되는 작업량을 반영합니다. 결과적으로, 더 복잡한 트랜잭션은 일반적으로 완료에 더 많은 가스를 필요로 하며, 이는 L2 실행 수수료의 크기에 직접적인 영향을 미칩니다. 이 요소는 트랜잭션 수수료가 실제로 사용된 연산 자원에 비례하도록 보장합니다.

L2 gasPrice - 트랜잭션 유형에 따라 달라짐

L2 gasPrice는 L2에서 사용되는 가스의 단가로, 선택한 특정 트랜잭션 유형에 따라 달라집니다. L2 gasPrice는 트랜잭션 유형에 따라 서로 다르게 계산됩니다:

- **EIP-1559 트랜잭션 유형**의 경우, L2 gasPrice는 시퀀서에 대한 보상으로 부여되는 GasTipCap 매개변수의 영향을 받으며, 사용자가 0으로 설정할 수 있고 트랜잭션 패킹에는 영향을 주지 않습니다.
- **레거시 트랜잭션 유형**의 경우, GasTipCap은 기본값(0.1 GWEI)을 사용합니다. 이때 eth_gasPrice는 GasTipCap과 BASEFEE의 합과 같습니다. 이 메커니즘은 트랜잭션 비용의 상대적 안정성을 보장하면서, 사용자에게 기본값을 제공하고 트랜잭션 매개변수 설정을 단순화합니다.

EVM 호환성으로 인해, 맨틀 네트워크의 트랜잭션은 일반적으로 이더리움과 유사한 gasUsed를 가집니다. 가스 가격은 시간과 혼잡도에 따라 변동하지만, 공개 맨틀 대시보드에서 현재 추정 L2 가스 가격을 항상 확인할 수 있습니다. 또한, 맨틀 네트워크의 가스비는 \$MNT로 표시되므로, 동일한 가스 가격이라도 가스 토큰으로 \$ETH를 사용하는 다른 L2 네트워크에 비해 트랜잭션 비용이 현저히 낮게 유지됩니다.

트랜잭션의 정렬(오더링)은 다양한 요인의 영향을 받습니다. 다음은 GasTipCap과 트랜잭션 제출 순서의 역할을 보여 주는 예시입니다:

1. 가령 Alice가 레거시 유형의 송금 트랜잭션 tx_A를 먼저 제출하고, 이어서 Bob이 또 다른 레거시 유형 송금 트랜잭션 tx_B를 제출했다고 가정해 보겠습니다. tx_B가 tx_A 이후에 오므로, 그 순서는 선착순(FCFS) 원칙을 따릅니다.
2. 가령 Alice가 EIP-1559 유형의 송금 트랜잭션 tx_A를 제출하고, 그것이 패킹되기 전에 더 높은 우선 수수료(GasTipCap)를 가진 또 다른 tx_B를 제출했다고 가정해 보겠습니다. 논스 충돌로 인해, 시퀀서는 더 낮은 GasTipCap을 가진 tx_A를 거부하고 tx_B의 패킹을 우선합니다.

맨틀 v2의 L1 롤업 수수료

L1에서의 트랜잭션 비용은 L2에서의 트랜잭션 비용보다 훨씬 높기 때문에, 이는 총 트랜잭션 비용에서 가장 큰 부분을 차지합니다. 또한 L1의 gasPrice 변동성으로 인해 L1 비용 계산은 복잡한 작업입니다.

$$L1RollupFee = (rollupDataGas + overhead) * L1gasPrice * tokenRatio * scalar \quad (6)$$

이 요소들을 자세히 살펴보겠습니다:

rollupDataGas 계산

L1 가스비의 가장 큰 부분은 rollupDataGas이며, 이는 L1에서 콜데이터로 저장되는 트랜잭션의 크기와 관련이 있으며, 일반적으로 L1 GasUsed의 85% 이상을 차지합니다.

맨틀 v2 Tectonic은 Op Stack의 rollupDataGas 계산을 선택하며, 트랜잭션 데이터에서 0 바이트와 0이 아닌 바이트의 개수를 계산합니다. 각 0 바이트는 4 Gas, 각 0이 아닌 바이트는 16 Gas가 소요되므로, 다음과 같습니다:

$$rollupDataGas = count_zero_bytes(tx_data) * 4 + count_non_zero_bytes(tx_data) * 16 \quad (7)$$

EigenDA 모듈이 맨틀 메인넷에 올라오에 따라, 상태 루트와 제한된 필수 트랜잭션 데이터만 L1에 전송되고, 트랜잭션 배치 데이터는 DA 네트워크에 게시됩니다. 가스 소비가 높은 디앱의 경우, 일반 트랜잭션(예: 송금)과 동일한 비용으로 실행될 수 있으며, L2 트랜잭션 실행의 복잡도가 높아져도 L1 수수료는 증가하지 않습니다. 결과적으로, 복잡도가 높은 트랜잭션의 경우 원래의 L1 롤업 수수료 대비 **90%** 이상 비용을 절감할 수 있습니다.

overhead와 scalar 가져오기

overhead와 scalar는 현재 구성값에서 로드되며, 동적 변경을 지원하지 않습니다. 이 값들은 [BVM_GasPriceOracle](#) 컨트랙트에서 조회할 수 있으며, L1gasPrice는 L1 블록으로부터 읽어야 합니다.

tokenRatio의 제어

tokenRatio는 맨틀에서 수수료를 조정하는 매개변수입니다. 여러 가격 오라클로부터 ETH와 MNT의 가격을 취득하고 그 환율(eth_price/mnt_price)을 계산함으로써, 맨틀 v2 Tectonic은 현재 tokenRatio 값을 직전 tokenRatio의 구간으로 제한하여, 환율의 급격한 변동으로 인해 발생할 수 있는 gasPrice의 갑작스럽고 큰 변동을 방지합니다.

맨틀 v2 Tectonic은 레이어 2에 [BVM_GasPriceOracle](#) 컨트랙트를 도입하여 tokenRatio 설정 및 업데이트에 대한 권한을 관리합니다. 권한 보유자(HSM을 통해 관리되는 다중서명 주소)는 L2 트랜잭션을 통해 tokenRatio를 업데이트하여 가스비를 동적으로 조정할 수 있습니다.

수수료 최적화

맨틀 v1과 비교하여, 맨틀 v2 Tectonic은 수수료 설계에서 다음과 같은 개선과 최적화를 수행했습니다:

- **EIP-1559 지원:** 맨틀 v2 Tectonic은 EIP-1559를 포함한 다양한 트랜잭션 유형을 지원하여, 사용자가 구형 트랜잭션 구조의 제약에서 벗어나도록 합니다. 자세한 내용은 [여기](#)를 참조하십시오.

L2 트랜잭션에서 baseFee를 0.02 gwei로, priorityfee를 0으로 설정할 것을 강력히 권장합니다. 자세한 내용은 [여기](#)를 참조하십시오.

- **수수료 추정:** 맨틀 v1의 estimateGas API는 L2 가스 비용만 반환하며, L1 가스 추정은 별도로 계산해야 했습니다. 반면 맨틀 v2 Tectonic에서는 사용자의 트랜잭션 총 가스를 직접 반환하는 것을 지원합니다. 개발자는 이 최적화가 트랜잭션 구성에 미칠 영향을 유념해야 합니다. 가스비 계산 방법에 대한 자세한 내용은 [여기](#)를 참조하십시오.

맨틀 v2 수수료 사례

	맨틀 v2 Tectonic	맨틀 v1 Alpha
토큰 전송	0.0047 MNT	0.3715 MNT
ERC-20 컨트랙트 배포	0.1088 MNT	0.1304 MNT

네이티브 토큰 마이그레이션

중요 버전 업데이트인 맨틀 v2 Tectonic은 시스템 네이티브 토큰의 전환을 포함하여 여러 측면의 최적화와 개선에 초점을 맞춥니다. 맨틀 v2 Tectonic에서는 시스템의 네이티브 토큰으로 \$MNT가 사용됩니다. 이 변경은 사용자에게 보다 유연하고 효율적인 트랜잭션 경험을 제공하고, 생태계의 향후 발전을 위한 견고한 기반을 마련하는 것을 목표로 합니다.

왜 맨틀 v2 Tectonic에 변경이 필요한가

맨틀 v2 Tectonic에서 네이티브 토큰을 ERC-20 기반 방식에서 Ether Gas를 사용하는 방식으로 변경하기로 한 결정에는 여러 이유가 있습니다:

1. 이더리움 네이티브 설계와의 더 긴밀한 정렬

ERC-20 토큰을 네이티브 토큰으로 선택했던 맨틀 v1과 달리, 맨틀 v2 Tectonic은 이더리움의 네이티브 설계와 더 밀접한 정렬을 지향합니다. 이는 개발 및 유지보수 과정을 단순화할 뿐 아니라, 맨틀 v2가 이더리움 생태계에 보다 자연스럽게 통합되도록 합니다.

2. 메인넷과 동기화된 L2 노드 업그레이드 촉진

새로운 네이티브 토큰은 L2 노드가 메인넷 코드 업그레이드와 동기화하기를 더욱 용이하게 만듭니다. 이러한 일관성은 맨틀 네트워크 전반의 원활한 협업을 보장하고, 잠재적 향후 EIP를 더 잘 지원하는 데 도움이 됩니다.

3. MNT 토큰의 추가적 활용성 부여

맨틀 v2 Tectonic은 [EIP-1559 유형 트랜잭션](#)을 지원합니다. 이 업데이트는 MNT 토큰이 해당 트랜잭션에서 GasTipCap 토큰 역할을 하여 트랜잭션 우선순위를 제어할 수 있게 합니다. 이 향상은 사용자에게 더 큰 유연성을 제공할 뿐 아니라, MNT 토큰에 추가적인 효용과 잠재력을 부여하여 맨틀 생태계를 한층 강화합니다.

신규 방식 이후의 변화

원장 저장 방식의 전환: 컨트랙트 계정에서 시스템 계정으로

맨틀 v2 Tectonic에서는 MNT 원장의 저장 방식을 컨트랙트 계정에서 시스템 계정으로 전환하는 중대한 변경이 이루어집니다. 단일 컨트랙트 계정의 중앙집중형 저장에서(집중형) 주소 계정에 분산된 일대일 잔액 매핑의 탈중앙 저장으로의 전환은 시스템 유지보수성을 향상시키며, 네트워크 전체의 탈중앙 설계와 더 잘 정렬됩니다.

MNT와 ETH의 동일한 플로 경로 달성

네이티브 토큰의 수정으로, 맨틀 네트워크는 MNT와 ETH의 동일한 플로 경로를 성공적으로 달성했습니다. 이 변경은 맨틀 네트워크에서 MNT의 지위를 격상시켜, 시스템 내에서 동등하고 편리한 지위를 부여합니다. 이제 사용자는 ERC-20 자산처럼 서로 다른 플로 경로를 채택할 필요 없이 ETH와 유사한 사용자 경험을 MNT로 누릴 수 있습니다.

이러한 변화는 맨틀 시스템의 전반적 성능과 사용자 경험에 긍정적인 영향을 미칠 뿐 아니라, 향후 확장 및 생태계 발전을 위한 견고한 기반을 구축합니다.

EIP-1559 지원

[EIP-1559](#)는 이더리움 커뮤니티가 제안한 업그레이드로, 트랜잭션 수수료 구조를 조정하여 네트워크 보안 이슈를 해결하는 것을 목표로 합니다. 이 제안의 핵심 아이디어는 트랜잭션 수수료를 소각하고, 채굴자(또는 지분증명 검증자)에게 보다 신뢰할 수 있는 영구 블록 보상을 제공하여 더 효과적인 인센티브 메커니즘을 만드는 것입니다.

수수료에 영향을 미치는 요소 분석

EIP-1559에서는 BASEFEE와 GasTipCap(또는 MaxPriorityFeePerGas)가 도입되고, 트랜잭션의 안전성을 보장하기 위해 GasFeeCap이 추가되면서 트랜잭션 수수료의 구성에 큰 변화가 발생합니다. 이더리움 프로토콜은 네트워크 혼잡도에 따라 BASEFEE를 동적으로 조정하고, 모든 BASEFEE를 소각함으로써 트랜잭션 패킹에서 외부 가격 발견에 수반되는 잠재적 보안 위험을 해소합니다.

왜 EIP-1559가 도입되었는가

EIP-1559의 도입은 다음과 같은 문제들을 해결하는 것을 목표로 합니다:

- **비효율적 가격 경매:** 네트워크 혼잡도별 가격 경매의 사용은 비효율을 초래하며, 수수료 추정은 매우 부정확합니다.
- **불일치하는 블록 활용도:** 기존 수수료 설계는 블록 활용도의 불일치를 초래합니다. EIP-1559는 블록 활용도 조정을 허용하여 더 장기적인 평균 블록 크기 한도를 가능하게 합니다.

- **네트워크 보안 강화:** 추가 인센티브([GasTipCap](#))는 검증자의 블록 보상 의존도를 줄여 네트워크 보안을 강화합니다.

맨틀 v2에서의 EIP-1559 적용

맨틀 v2에서는 BASEFEE와 [GasTipCap](#)에 대해 다음과 같은 조정을 수행했습니다:

- **BASEFEE 조정 메커니즘:**
 - 맨틀 L2의 BASEFEE는 이더리움 L1의 [SystemConfig](#) 컨트랙트를 통해 설정되는 시스템 매개변수이며, 맨틀 L2로 동기화됩니다. [여기](#)에서 확인할 수 있으며—현재 L2 BaseFee는 20,000,000 wei(0.02 gwei)로 고정되어 있습니다.
 - BASEFEE는 더 이상 소각되지 않으며, [BaseFeeVault](#)에 적립되고 L1로의 인출을 지원합니다.
- **GasTipCap 조정 메커니즘:**
 - 각 트랜잭션에서 GasTip과 ($\text{GasFeeCap} - \text{BaseFee}$)의 최소값에 gasUsed를 곱한 값을 검증자 보상으로 하여, 이를 [SequencerFeeVault](#)에 적립하고 L1로의 인출을 지원합니다.
 - 맨틀 v2 Tectonic은 수수료를 추가로 절감하기 위해 트랜잭션 시퀀싱에서 [FIFO](#) 방식을 선택하여 priorityfee의 영향을 최소화했습니다.

이러한 조정을 통해, 맨틀 v2 Tectonic은 EIP-1559를 기반으로 보다 유연하고 효율적인 트랜잭션 수수료 관리 메커니즘을 제공합니다.

맨틀 v2 Tectonic은 매우 낮은 BASEFEE를 설정하며, EIP-1559 트랜잭션의 MaxPriorityFeePerGas를 0으로 설정할 것을 또한 권장합니다. 이렇게 하면 트랜잭션 수수료가 매우 낮아집니다!\

리스크 관리

맨틀 네트워크는 안전하고 신뢰할 수 있는 레이어-2(L2) 확장 솔루션을 제공하는 데 전념하며, 강력한 리스크 관리는 중요한 안전장치입니다. 맨틀의 리스크 분석은 [데이터 가용성](#), [사기 증명](#), [강제 트랜잭션 포함](#)의 세 가지 핵심 측면으로 구성됩니다.

1. 데이터 가용성

맨틀 네트워크는 데이터의 가용성을 보장함으로써 시스템 보안의 초석을 보전합니다. 혁신적인 데이터 가용성 솔루션을 통해, L2 실행 레이어와 레이어 1(L1) 사이의 데이터 전송 과정에서 데이터의 안전한 가용성을 보장합니다. 이 메커니즘은 네트워크 안정성을 높일 뿐 아니라, 사용자와 개발자에게 보다 신뢰할 수 있는 데이터 보증을 제공합니다.

2. 사기 증명(Fraud Proofs)

맨틀 네트워크는 사기 증명 개념을 도입하여 잠재적인 부정 행위를 대응합니다. 전체 트랜잭션 과정에서 시스템은 데이터의 일관성을 적극적으로 모니터링하고 검증합니다. 데이터 변조 또는 위조 시도가 있으면 시스템이 이를 감지하여 적절히 처리합니다. 이는 시스템의 보안성과 공정성을 보장하여 사용자에게 안전한 거래 환경을 제공합니다.

3. 강제 트랜잭션 포함(Forced Transaction Inclusion)

시스템이 극단적 상황에서 극복하기 어려운 문제에 직면할 경우에 대비하여, 맨틀 네트워크는 강제 트랜잭션 포함 메커니즘을 설계했습니다. 이를 통해 L1로의 신속하고 안전한 롤백이 가능해져 사용자 자산의 안전을 보장합니다. 이 설계는 시스템에 긴급 구제 메커니즘을 제공하여, 언제든지 예측 불가능한 위협에 대응할 수 있게 합니다.

이러한 세 가지 핵심 보안 측면을 통해, 맨틀 네트워크는 견고한 리스크 대응 모델을 구축했으며, 사용자와 개발자에게 신뢰할 수 있는 L2 확장 솔루션을 제공함으로써 탈중앙 생태계 전체의 건전한 발전을 견인합니다.

데이터 가용성(Data Availability)

데이터 가용성이란 무엇인가?

맨틀 네트워크에서 데이터 가용성(DA)은 시퀀서가 게시한 트랜잭션 이력을 어떤 노드든 접근할 수 있는 능력을 의미합니다. 모든 네트워크 참여자가 블록 데이터에 접근할 수 있도록 하는 것은, 특히 롤업 아키텍처에서 구동되는 블록체인 맥락에서, 핵심적인 확장성 이슈입니다. 롤업은 레이어 1(L1)로부터 보안을 상속받고 트랜잭션 데이터를 L1에 게시하므로, 시퀀서는 트랜잭션 데이터를 가용하고 신뢰할 수 있게 만드는 데 중요한 역할을 합니다. DA는 체인의 라이브니스(liveness)를 유지하고 잘못된 트랜잭션을 포착하여 블록 데이터가 악의적으로 은닉될 가능성을 제거하는 데 필수적입니다.

데이터 가용성을 보장하는 것은 그 자체로 하나의 과제임이 드러났습니다. 이것이 어떻게 처리되는지 이해하려면, 데이터 가용성 문제와 소거 코드(Erasure Coding)에 대해 [여기](#)에서 더 읽어볼 수 있습니다.

데이터 가용성을 어떻게 유지하는가?

데이터 가용성을 보장하는 것은 블록체인 업계에서 중대한 과제이며, 이를 해결하기 위해 다양한 혁신적 솔루션이 활용되고 있습니다:

1. 온체인 L1 접근법:

증명 구성을 위해 필요한 모든 데이터를 L1에서 접근 가능하게 함으로써 데이터 가용성을 보장합니다. 가장 높은 수준의 신뢰를 제공하지만, 더 높은 비용과 상대적으로 느린 데이터 검색이 수반될 수 있습니다.

2. 중앙화된 DA 위원회:

필요한 데이터를 제공할 책임이 있는 중앙화된 DA 위원회를 활용합니다. 이 접근법은 온체인 L1 방식에 비해 롤업 비용을 크게 줄이지만, 데이터 비가용성의 잠재적 위험을 도입합니다.

3. DA 샘플링:

DA 샘플링은 라이트 노드가 전체 블록 데이터를 다운로드하지 않고도 데이터 가용성을 검증할 수 있도록 하는 방법입니다. 이 메커니즘은 라이트 노드가 여러 라운드에 걸쳐 블록 데이터의 일부를 무작위로 샘플링하여 데이터 가용성에 대한 신뢰를 높이는 방식입니다. 라이트 노드가 사전에 정한 신뢰 수준(예: 99%)에 도달하면, 해당 블록 데이터를 가용하다고 간주합니다.

4. 독립적인 DA 모듈:

아이겐레이어의 EigenDA 기술로 지원되는 맨틀 DA와 같은 독립적인 DA 모듈을 포함한 혁신적 접근이 있습니다. 이 방법은 보상과 스테이크 슬래싱을 포함하는 DA 경제의 게임이론을 통해 데이터 가용성을 달성합니다. 내부 평가에 따르면, 이 솔루션은 온체인 L1 방식 대비 90% 이상 비용을 절감하면서 경제적 인센티브와 함께 효율적인 데이터 가용성을 제공합니다.

EigenDA

EigenDA란 무엇인가?

이를 이더리움을 위한 미들웨어로 생각해 볼 수 있습니다.

[옵티미스틱 롤업](#)이 경제적 인센티브로 시스템 무결성을 유지하는 것과 유사하게, 이 메커니즘은 이더리움 검증자가 추가 수익 기회를 위해 서비스를 제공하도록 인센티브를 제공합니다. 아이겐레이어에 대해서는 [여기](#)에서 더 알아보십시오.

맨틀 DA란 무엇인가?

EigenLabs가 구축한 EigenDA는 아이겐레이어의 핵심 애플리케이션 중 하나로, 맨틀 네트워크의 데이터 가용성 모듈을 구동하는 기술로 채택되었습니다. 현재 맨틀 DA 버전은 EigenDA 기술의 지원을 받으며 EigenLabs의 승인을 받았습니다. 개발 전반에 걸쳐 맨틀 팀은 이 간소화된 솔루션을 탐구하기 위해 아이겐레이어 팀과 긴밀히 협력해 왔습니다. 표준화된 EigenDA 솔루션이 메인넷 출시 준비를 마치면, 맨틀은 보다 효율적인 데이터 가용성을 위해 DA 구성 요소를 EigenDA로 마이그레이션할 것입니다. 추가로, 맨틀 DA는 맨틀 네트

워크에 데이터 가용성 서비스를 제공하는 권한 있는 노드를 허용하며, 네트워크 보안을 보장하기 위해 \$MNT 스테이킹을 요구합니다. 자세한 내용은 [여기](#)를 참조하십시오.

맨틀 DA의 경우, 롤업 데이터는 다음에서 확인할 수 있습니다: [L1의 상태 루트](#), [L1의 롤업 트랜잭션 데이터](#), 그리고 [L2의 DA 롤업 트랜잭션](#).

맨틀 DA 모듈에 참여하는 다양한 주체가 어떻게 동작하는지 더 알고 싶다면, [DA 노드](#)에 대한 [섹션](#)을 참고하십시오.

맨틀 DA의 특성

- 데이터 가용성 레이어를 합의 레이어로부터 분리할 수 있도록 허용
- 네트워크 참여자 간 데이터 교환에 유니캐스트 채널을 활용하여 데이터 전송과 저장 측면에서 효율성 제고
- 소거율(erasure rate)을 유지하여 L2 및 L1 소스의 블록 데이터 조각이 검증 주체에 의해 완전한 블록 데이터로 재구성될 수 있도록 보장

이 접근법은 블록체인 게임, 탈중앙 소셜 네트워크 등 차세대 애플리케이션을 위한 필요한 고처리량과 낮은 가스비를 제공할 것입니다.

맨틀 익스플로러(Mantle Explorer) 는 L2에서 발생하는 트랜잭션과 마찬가지로, DA 레이어에 저장된 롤업 데이터의 [트랜잭션 배치 상세](#)를 표시합니다.

사기 증명(Fraud Proof)

옵티미스틱 롤업은 반증되기 전까지 모든 레이어 2(L2) 트랜잭션 상태 전이가 유효하다고 가정합니다. 그 결과 이들은 또한 단언(assertions)으로 불리며, 그 유효성은 사전에 결정되지 않습니다. 검증 로직은 잘못된 상태 전이에 대한 증거에 의존하여 검증 과정을 시작하며, 사기 증명은 그러한 증거를 제공하는 매개체 역할을 합니다. 프로토콜은 네트워크 참여자가 자신이 틀렸다고 믿는 상태에 대해 사기 증명을 제출할 수 있는 분쟁 창구(dispute window)를 허용합니다. 대부분의 [옵티미스틱 롤업](#) 프로토콜에서는 이 챌린지 기간이 일반적으로 약 7일 동안 지속됩니다. 기본적으로, 이 기간 내에 분쟁이 없는 모든 트랜잭션은 유효한 것으로 간주됩니다.

사기 증명의 유형

사기 증명은 **비대화형**과 **대화형**의 두 가지 유형으로 구분할 수 있습니다.

비대화형 사기 증명

비대화형 사기 증명은 단언의 오류를 입증하는 데 다른 당사자가 필요하지 않은 방법을 사용합니다. 기본적으로 두 단언 사이의 모든 상태 전이를 실행하여 결과 상태가 일관적인지 여부를 판단합니다. 설계와 구현이 더 간단하지만, 현재 EVM(Ethereum Virtual Machine) 아키텍처의 연산 능력으로 실행할 수 있을 만큼 단언의 크기가 충분히 작아야 한다는 제한을 둡니다.

대화형 사기 증명

반면 대화형 사기 증명은 한쪽은 사기 단언을 주장하고 다른 한쪽은 해당 단언을 방어하는 등 두 개 이상의 당사자가 협력하여 단언을 검증합니다. 검증자는 도전자와 상호작용하여 단언을 단일 상태 전이로 좁힌 다음, 궁극적으로 그 한 전이만 검증하여 유효성을 확립합니다. 이러한 상호작용은 프로토콜에 새로운 수준의 복잡성을 도입하여 안전하게 설계하기가 더 어려울 수 있습니다. 그러나 실제 온체인 실행량이 훨씬 적기 때문에 L1에 제약을 가하지 않는 장점이 있습니다.

맨틀 네트워크의 사기 증명

Cannon이란 무엇인가?

옵티미즘이 개발한 Cannon은 온체인 MIPS 명령어 시뮬레이터입니다. 이는 대화형 분쟁의 일환으로, [op-geth](#)를 사용해 온체인 명령을 한 번에 하나씩 실행함으로써 EVM-등가(fault) 증명을 가능하게 합니다. 이 과정은 온체인 컨트랙트와 오프체인 시뮬레이터의 페어링을 포함합니다.

왜 맨틀에 이것이 필요한가?

현재 널리 쓰이는 사기 증명 모델에서는, 분쟁 해결을 담당하는 온체인 검증자 컨트랙트가 [MIPS](#)나 [WASM](#)과 같은 하위 수준의 가상머신에서만 명령을 실행할 수 있습니다. 이는 이더리움 가상머신(EVM) 클라이언트(예: `op-geth`)가 온체인 검증자가 해석할 수 있도록 사기 증명을 하위 수준 언어(예: MIPS opcode)로 재컴파일하도록 강제합니다. 따라서 Cannon은 온체인 컨트랙트를 구현하여 MIPS opcode를 시뮬레이션함으로써, EVM 환경에서 MIPS 명령 실행의 검증을 가능하게 합니다. 동시에, 어떠한 MIPS 명령에 대해서도 증명을 생성하는 오프체인 시뮬레이터를 구현하여 온체인 검증을 완성합니다.

맨틀 네트워크는 Cannon이 구현한 사기 증명 모델을 사용할 것입니다. 더 알아보려면 [여기](#)를 참조하십시오.

강제 트랜잭션 포함(Forced Transaction Inclusion)

레이어 2(L2) 기술이 점점 더 많은 디지털 자산을 호스팅함에 따라, L2 보안 사고 발생 시 자산의 보안을 보장하는 것이 중요한 관심사가 되었습니다. 견고한 L2는 예기치 못한 상황(예: 시퀀서와 프로포저의 다운타임 또는 오작동 등)에서 L2 자산을 레이어 1(L1)에서 강제로 인출할 수 있는 능력이 필요합니다.

검열 저항성은 특히 시스템의 시퀀서와 관련하여 중요한 보안 기능입니다. 시퀀서가 트랜잭션 요청 실행을 거부하거나 장기간 다운타임을 겪는 상황에서는, 강제 출금 또는 강제 트랜잭션 포함으로 알려진 메커니즘이 사용자 자금 보호를 위해 필수적입니다.

강제 트랜잭션 포함을 어떻게 활성화하는가

모든 OP Stack 체인에는 단 하나의 [OptimismPortal](#) 컨트랙트만 존재합니다. 이 컨트랙트는 EOA(Externally Owned Account) 또는 스마트 컨트랙트가 시퀀서를 거치지 않고 L2 트랜잭션([OptimismPortal](#)의 `depositTransaction`)을 생성할 수 있도록 하며, 이렇게 제출된 트랜잭션은 L2에서 시퀀서가 구성한 트랜잭션과 구분되지 않습니다.

트랜잭션이 L1에 제출되면, 일부 [포함 규칙](#)과 함께 선착순(FIFS) 방식으로 처리됩니다. 트랜잭션이 `sequencer_window` 시간 내에 L1에 게시되지 않으면, L2에서 리오그(reorg)가 발생하고 해당 트랜잭션이 L2 체인에 포함됩니다.

서로 다른 시퀀서 장애 시나리오

실제 적용에서는 다음과 같은 다양한 시나리오를 마주칠 수 있습니다:

시퀀서 완전 다운

이 시나리오에서는 시퀀서가 계속하여 작동하지 못하고 트랜잭션을 처리하지 못합니다. 사용자는 자신의 트랜잭션이 L2 체인에 포함되도록 [OptimismPortal](#) 컨트랙트로 직접 전송해야 합니다. `sequencer_window` 시간(24시간)이 경과하면, 이러한 트랜잭션은 자동으로 L2에 포함됩니다. 자세한 내용은 [여기](#)를 참조하십시오.

시퀀서 일시적 다운

이 시나리오에서는 시퀀서가 일시적으로 장애를 겪었다가 복구됩니다. `sequencer_window` 시간이 아직 경과하지 않았기 때문에, 트랜잭션이 [OptimismPortal](#)에 제출되었더라도 최종적으로 시퀀서에 의해 처리되어 L2에 포함됩니다. 자세한 내용은 [여기](#)를 참조하십시오.

로드맵

맨틀 네트워크는 이제 맨틀 네트워크 메인넷 v2 Tectonic(맨틀 v2 Tectonic)을 출시했으며, 맨틀 네트워크 메인넷 Alpha v1(맨틀 v1)에 대해 여러 개선과 최적화를 제공했습니다. 더 자세한 정보는 아래 표를 참조하십시오.

개요

Category	Situation	What We Have Now	Future Potential Solution
L2 Execution	Environment	EVM-Compatible with patial Shanghai upgrade	[] Upgraded EVM-Compatible with validity proof system
	L2 Gas Fee	\$MNT (Native Token)	[] Custom Gas Token
	L2 Block Producing / Sequencing	Centralized Sequencer	[] Shared Sequencer [] TEE-based Solution
L2 to L1	Batch Submitter	Centralized Batcher	[] Decentralized Batchers
	Data Availability	1. Rollup data stored in Mantle DA powered by EigenDA 2. State root stored in Ethereum L1	[] EigenDA [] Blobs stored in Ethereum L1 [] Other third-party DA [] Other Blobs aggregation solution
L1 Risk Management	L2 Sequencer Failure	L1 Forced Inclusion	[] Fully escape hatch
	L2 Proposer Failure	-	[] Support users to be proposers to propose new root to L1 bridge
	Proofs / State Validation	Without Fraud Proofs	[] zkVM-based Proof System
Architecture	Architecture	OP Stack	[] OP-Succinct

2025 로드맵

2025년 Q1 - 기능 롤아웃 및 보안 강화

기 설계된 기능과 기술적 진보를 롤아웃하고, 네트워크 보안을 향상하며, 사용자 경험을 최적화하고, 개발자 지원을 강화하는 데 집중합니다.

주요 작업

- 보안 강화
 - 맨틀 네트워크는 현재 데이터 가용성(DA) 레이어로 EigenDA로 구동되는 맨틀 DA를 사용하고 있습니다. 아이겐레이어 메인넷이 가동됨에 따라, 더 강력한 DA 보장을 위해 본 분기 내 **테스트넷**과 **메인넷** 모두에서 맨틀 DA를 EigenDA로 업그레이드할 계획입니다.
- 사용자 경험 최적화
 - 더 나은 가격 발견 메커니즘과 체인 불가지론적 사용자 경험을 제공하기 위해, 맨틀 네트워크는 독자적인 체인 추상화 **솔루션**을 도입했습니다. 이 솔루션의 **테스트넷** 및 **메인넷** 배포가 본 분기에 계획되어 있습니다.
- 개발자 지원
 - **RIP-7212**와 같은 높은 기대를 받는 제안들을 네트워크에 통합합니다. 이는 맨틀 생태계에서 작업하는 개발자의 경험을 더욱 향상하기 위해 **테스트넷**과 **메인넷**에 배포될 것입니다.

2025년 Q2 - 이더리움 Pectra 업그레이드 지원

이더리움 **Pectra** 업그레이드에 맞춰, 맨틀 네트워크가 이더리움 생태계와 기술적으로 동기화되도록 보장합니다.

주요 작업

이더리움 Pectra 업그레이드가 진행됨에 따라, 맨틀 네트워크는 이더리움 커뮤니티의 기술적 진전에 발맞춰 다음 작업을 완료할 것입니다:

- ☐ 맨틀 네트워크가 최신 이더리움 가상머신(EVM) 버전을 지원하도록 보장합니다.
- ☐ 필요에 따라 OP Stack을 업데이트 및 최적화합니다.
- ☐ 외부 소유 계정(EOA) 지갑의 배치 및 가스 후원을 지원하기 위해 **EIP-7702**를 구현합니다.
- ☐ 모든 관련 코드 개발을 마치고, 안정적이고 안전한 네트워크 업그레이드를 보장하기 위해 QA 네트워크에서 포괄적인 테스트를 수행합니다.

2025년 Q3 - 증명 시스템 롤아웃 및 애플리케이션 탐색

zkVM 기반 증명 시스템의 테스트넷을 출시하고, 다중 시나리오 체인 추상화 애플리케이션을 탐색하기 위한 추가 개념증명(POC) 실험을 수행합니다.

주요 작업

- ☐ **zkVM 기반 증명 시스템**
 - 맨틀 네트워크는 빠른 파이널리티를 가능하게 하는 **Succinct SP1**을 증명 시스템으로 선택했습니다. 이 기능의 테스트넷 출시는 본 분기에 예정되어 있습니다.
- ☐ **추가 POC 실험**
 - 체인 추상화에서 다음 ZKP 애플리케이션에 대한 POC를 완료합니다:
 - ☐ **의도 정산 증명(Intent Settlement Proof)**: 체인 추상화 내 효율적인 의도 정산 메커니즘을 검증합니다.
 - ☐ **크로스체인 증명(Cross-Chain Proof)**: 크로스체인 자산 발행을 위한 멀티체인 라이트 클라이언트 증명을 구현하여, 크로스체인 자산 상호작용의 보안성과 투명성을 강화합니다.

2025년 Q4 - 체인 추상화 및 개발자 생태계 강화

체인 추상화 기능을 추가로 정교화하고, 개발자 생태계의 확장을 추진합니다.

주요 작업

- ☐ **체인 추상화 기능 검증 및 POC**
 - ☐ **최적 경로 선택**: 다중 크로스체인 브리지 및 DEX에 대한 최적 경로 선택을 구현하여, 크로스체인 작업의 효율성과 사용자 경험을 개선합니다.
 - ☐ **자산 융합**: 다중 토큰과의 통합 상호작용을 지원하여 자산 유연성을 높입니다.
 - ☐ **원클릭 디앱 통합**: 더 많은 디앱이 생태계에 원활히 참여할 수 있도록 체인 추상화 통합 도구를 강화하여 개발 복잡성을 줄입니다.
- ☐ **개발자 생태계 개발**
 - ☐ 포괄적인 개발자 도구와 문서를 제공합니다.
 - ☐ 더 많은 개발자가 맨틀 생태계에 기여하고 체인 추상화 솔루션의 채택을 촉진하도록 기술 워크숍과 해커톤을 조직합니다.

네트워크 역할

노드 배포 서비스에 오신 것을 환영합니다. 본 서비스는 네트워크의 정상 운영과 다양한 기능을 지원하는 여러 유형의 노드를 다룹니다. 아래 지침을 따라 노드를 구성하고 배포하십시오.

사용 가능한 노드 유형

검증자(Verifier) 노드

검증자 노드는 체인상의 트랜잭션과 블록의 유효성을 검증하는 데 사용됩니다. 이는 네트워크의 보안과 신뢰성을 보장하는 핵심 구성요소입니다. 상세한 [검증자 노드 배포 문서](#)가 이미 제공되어 있습니다.

시퀀서(Sequencer) 노드

시퀀서는 트랜잭션을 순차적으로 패키징하여 레이어 2 블록을 생성하고, 트랜잭션에 결정적 순서를 제공합니다. 현재 보안상의 이유로 시퀀서 노드는 아직 공개되어 있지 않습니다.

프로포저(Proposer) 노드

프로포저 노드는 새로운 상태 루트를 생성하여 레이어 1로 전송하는 데 사용됩니다. 현재 보안상의 이유로 프로포저 노드는 아직 공개되어 있지 않습니다.

배치(Batcher) 노드

배치 노드는 다수의 트랜잭션을 하나의 블록으로 묶어 처리 효율을 높이는 데 사용됩니다. 현재 보안상의 이유로 배치 노드는 아직 공개되어 있지 않습니다.

데이터 가용성(DA) 노드

DA 노드는 트랜잭션 데이터의 가용성을 보장합니다. 현재 보안상의 이유로 DA 노드는 아직 공개되어 있지 않습니다.

왜 롤업 검증자 노드를 운영하는가?

롤업 검증자 노드를 운영하는 데에는 여러 장점이 있습니다.

1. 공용 RPC가 그러한 제한에 직면할 수 있는 것과 달리, 속도 제한 없이 로컬에서 L2 트랜잭션을 시뮬레이션할 수 있는 능력 등, 이더리움 노드를 운영할 때의 이점을 다수 제공합니다.
2. 시퀀서가 제출한 출력 루트를 재도출하고 이를 시퀀서가 제출한 값과 비교함으로써, 누구나 시퀀서가 수행한 작업을 검증할 수 있습니다. 불일치가 발생할 경우, 검증자는 맨틀 네트워크 메인넷의 향후 버전에서 사기 증명을 제출하여 결함 검사를 수행하고 보상을 청구할 수 있게 됩니다.

FAQs

일반

- 맨틀 네트워크는 어떤 서명 알고리즘을 사용하나요?

맨틀 네트워크는 이더리움과 동일한 서명 알고리즘을 사용합니다. (secp256k1 곡선 위의 ECDSA)

- 맨틀 네트워크의 블록 가스 한도는 얼마인가요?

블록 가스 한도는 현재 250,000,000,000, 즉 250B 유닛으로 설정되어 있습니다.

- 맨틀 네트워크의 평균 블록 시간은 얼마인가요?

맨틀 네트워크에서는 OP Stack 프레임워크 설계에 따라 L2 블록이 2초마다 생성됩니다.

L1 노드가 600초 이상 새 블록 동기화에 실패하면, L2는 블록 생성을 일시 중지하며, L1 노드가 복구되는 즉시 L2 노드는 정상으로 돌아오고 L2 블록의 타임스탬프는 2초씩 엄격히 증가함이 보장됩니다.

- **맨틀 네트워크에서 트랜잭션 파이널리티는 어떻게 동작하나요?**

- L2의 트랜잭션/블록 파이널리티는 L1에 패키징되어 제출된 트랜잭션의 파이널라이즈드 시점에 의존합니다(2 에폭, 약 15분).
- L1의 트랜잭션/블록 파이널리티는 챌린지 기간과 연결되며, 현재 7일로 설정되어 있습니다.

- **맨틀 네트워크에서 사기 증명은 온라인인가요?**

아직 아닙니다. 사기 증명은 맨틀 v2 Tectonic에서 개발 중입니다. 맨틀 네트워크의 구현에 대한 자세한 내용은 사기 증명 페이지를 확인하세요.

- **모듈러 데이터 가용성은 어떻게 트랜잭션 비용을 낮추나요?**

L2 가스비의 대부분(>70%)은 L1 이더리움에 데이터를 게시하는 비용에서 발생합니다. EigenDA 기술로 구동되는 맨틀 DA에 서는 상태 루트 데이터(매우 제한된 트랜잭션 데이터 포함)만 L1 컨트랙트에 게시하고, 롤업 데이터는 맨틀 DA에 게시하여 전체 비용을 크게 낮춥니다.

- **맨틀 네트워크의 브랜드 리소스는 어디에서 찾을 수 있나요?**

[이 링크](#)를 통해 브랜드 리소스에 접근할 수 있습니다.

프로토콜

- **롤업 검증자 노드는 시퀀서가 처리한 모든 블록 데이터를 검증하나요?**

예. 모든 갠신된 상태 루트는 L1에 롤업 과정의 일부로 제출되기 전에 롤업 검증자에 의해 검증됩니다.

- **롤업 검증자는 시퀀서로부터 롤업 데이터를 동기화하나요?**

아니요. 롤업 검증자는 맨틀 DA로부터 롤업 데이터를 동기화하고, 이를 사용해 상태 루트를 생성한 뒤 L1에 게시되기 전에 시퀀서가 생성한 갠신 상태 루트를 검증합니다.

- **롤업 검증자가 L2 블록 데이터와 L1 간 불일치를 감지하면 어떻게 되나요?**

맨틀 네트워크에서 사기 증명이 온라인되기 전까지는, 롤업 검증자가 갠신 상태 루트를 검증하는 과정에서 불일치를 감지하면 L2의 롤업 메커니즘이 일시 중단됩니다. 장애 처리에 대해서는 [여기](#)를 참고하세요.

용어집

배처(Batcher)

Batcher는 L2의 트랜잭션을 배치로 묶어 L1에 업로드하는 노드 역할입니다. 자세한 내용은 [여기](#)를 참고하세요.

브릿지(Bridge)

앱 개발자와 사용자는 일반적으로 레이어 1(L1)과 레이어 2(L2) 사이에서 데이터와 자산을 이동해야 합니다. 두 네트워크 간 데이터와 자산을 이동하는 과정을 “브릿징(bridging)”이라고 부릅니다.

채널(Channel)

Channel은 OP Stack에서 시퀀서 배치를 압축-인코딩해 저장하는 데 사용하는 데이터 구조로, 여러 배치를 함께 저장하여 더 좋은 압축률을 달성하고 데이터 가용성 비용을 줄입니다. 자세한 내용은 [여기](#)를 확인하세요.

EIP-1559 transaction

[EIP-1559](#)는 이더리움 트랜잭션을 위한 새로운 트랜잭션 유형을 도입합니다. 사용자가 가스 가격을 직접 설정하던 기존 방식과 달리, EIP-1559는 네트워크 수요에 기반해 트랜잭션 수수료를 자동 결정하는 메커니즘을 도입합니다.

사기 증명(Fraud proof / Fault proof)

검증자가 개시하는 온체인 챌린지 메커니즘으로, 검증자는 L1에서 상태 루트를 가져와 DA가 제공한 상태 루트와 비교하고, 불일치가 있을 경우 온체인에서 단일/다중 라운드의 대화형/비대화형 증명을 개시합니다.

하드웨어 보안 모듈(Hardware security module (HSM))

하드웨어 보안 모듈은 민감한 정보, 키, 암호 연산을 무단 접근과 공격으로부터 보호하도록 설계된 전용 하드웨어 장치입니다. 맨틀 네트워크에서는 [op-proposer](#), [op-batcher](#) 등의 모듈에서 중요한 계정의 커스터디에 HSM을 사용합니다.

레거시 트랜잭션(Legacy transaction)

[EIP-2718](#)을 사용한 타입 트랜잭션 도입 이전의 트랜잭션 형식을 의미합니다. 이 트랜잭션은 타입 `0x0`으로 식별되며 `nonce`, `gasPrice`, `gasLimit`, `to`, `value`, `data`, `v`, `r`, `s` 등의 파라미터를 포함합니다.

MIPS

MIPS 아키텍처는 Microprocessor without Interlocked Pipeline Stages의 약자로, RISC(축소 명령어 집합 컴퓨팅) 설계 철학을 사용하는 컴퓨터 아키텍처의 한 종류입니다. 자세한 내용은 [여기](#)를 참고하세요.

모듈러 체인(Modular chains)

모듈러 블록체인에서는 블록체인 운영의 핵심 기능(실행, 합의, 결제, 데이터 가용성)이 전문화된 레이어에서 수행됩니다. 이 원칙을 롤업에 적용하면 각 레이어가 전문화된 작업을 수행하므로 솔루션을 최적화할 수 있으며, 그 결과 비용이 낮아지고 전반적인 성능이 향상됩니다.

모놀리틱 체인(Monolithic chains)

전체 블록체인 시스템을 단일하고 강하게 결합된 엔티티로 간주합니다. 이 구조에서는 모든 기능과 프로토콜이 동일한 체인에 내장되어 있습니다.

옵티미스틱 롤업(Optimistic Rollup)

옵티미스틱 롤업(OR)은 이더리움의 처리량을 증가시키도록 설계된 L2 프로토콜입니다. 연산과 상태 저장을 오프체인으로 옮기고 트랜잭션을 배치로 처리함으로써 메인 이더리움 체인의 연산 부하를 줄입니다. OR는 온체인에 게시되는 트랜잭션 배치에 대해 유효성 증명을 게시하지 않고 오프체인 트랜잭션이 유효하다고 가정하기 때문에 “옵티미스틱”이라 불리며, 잘못된 상태를 탐지·처리하기 위해 Fraud proof를 사용합니다.

프로포저(Proposer)

Proposer와 Batcher는 유사한 기능이지만, 트랜잭션 자체가 아니라 트랜잭션 완료 후의 상태를 패키징하고 상태 루트를 L1의 해당 컨트롤러로 전송합니다. 자세한 내용은 [여기](#)를 참고하세요.

리오그(Reorg)

Reorg, 즉 체인 재구성은 네트워크 공격 등 요인으로 인해 일단 수락된 트랜잭션이 이후 거부되는 상황을 말하며, 종종 L1이 공격받은 뒤 발생하는 L2 리오그 상황에서 나타납니다.

시퀀서(Sequencer)

Sequencer는 [op-node](#)와 [op-geth](#)로 구성된 노드 역할로, L2에서 트랜잭션 정렬과 L2 블록 생성을 수행합니다. 자세한 내용은 [여기](#)를 참고하세요.

증명자(Verifier)

Verifier는 [op-node](#)와 [op-geth](#)로 구성된 노드 역할로, 사용자에게 L2의 검증된 트랜잭션과 상태 루트를 제공하며, 온체인과 오프체인 트랜잭션 상태에 불일치가 있을 경우 사기 증명을 개시하여 트랜잭션의 유효성을 보장합니다. 자세한 내용은 [여기](#)를 참고하세요.

WASM

일반적으로 WASM으로 약칭되는 WebAssembly는 고수준 프로그래밍 언어를 위한 이식 가능한 컴파일 타겟 역할을 하는 바이너리 명령어 형식입니다. 웹 브라우저에서의 효율적 코드 실행을 가능하게 하도록 설계되었지만, 웹 환경에 한정되지 않습니다. WASM은 거의 네이티브에 가까운 속도로 코드를 실행할 수 있게 하여, 전통적인 웹 개발 기술과 비교해 성능 향상을 제공합니다. 자세한 내용은 [여기](#)를 참고하세요.