

칼데라(Caldera)

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.

칼데라 메타레이어 문서

롤업을 위한 크로스체인 상호운용성 프레임워크

소개

메타레이어는 칼데라의 크로스체인 상호운용성 프레임워크로, 롤업과 기타 체인 간의 상호작용 방식을 혁신적으로 바꾸기 위해 설계되었습니다. 메타레이어는 크로스체인 운영을 보다 원활하고, 안전하며, 효율적으로 수행할 수 있는 플랫폼을 제공합니다.



왜 메타레이어인가?

메타레이어는 개발자와 프로토콜이 고립된 블록체인 생태계의 한계를 극복할 수 있도록 지원합니다.

- **진정한 상호운용 체인 런칭:** 메타레이어 상호운용성을 기본으로 갖춘 새로운 칼데라 롤업을 처음부터 배포하거나, 기존의 칼데라 체인에 메타레이어를 통합하여 즉시 더 넓은 생태계와 연결할 수 있습니다.
- **정교한 크로스체인 디앱 구축:** 메타레이어의 개발자 도구 키트를 활용하여, 기반 기술과 관계없이 롤업 간의 효율적인 커뮤니케이션과 가치 이전을 가능하게 하는 애플리케이션을 개발할 수 있습니다.
- **통합 유동성(Unified Liquidity) 접근:** 확장 중인 공유 유동성 네트워크에 접근하여, 더 효율적인 시장 형성과 뛰어난 사용자 경험을 애플리케이션에 제공할 수 있습니다.
- **복잡성 추상화:** 개발자는 크로스체인 커뮤니케이션, 최적 경로 설정, 안전한 정산과 같은 복잡한 부분은 메타레이어에 맡기고, 핵심 애플리케이션 로직과 사용자 경험에 집중할 수 있습니다.

핵심 개념

인텐트 엔진(Intent Engine)

인텐트 엔진은 복잡한 작업을 간소화하여, 여러 체인에 걸친 자산 온보딩과 선언적 실행을 빠르게 처리할 수 있도록 지원합니다.

메시지 전달(Message Passing)

하이퍼레인(Hyperlane) 기반의 보안 메시지 전달 프로토콜로, 1:1 메시지 전달과 다수-대-단일 조회(many-to-1 read)를 모두 지원합니다.

칼데라는 업계 선도 기업들과 협력하여 메시징 및 정산 인프라를 개발하였습니다. 인텐트 기반 브릿징은 어크로스(Across), 에코(Eco), 릴레이(Relay)의 기술로 구동되며, 하이퍼레인을 활용한 낮은 지연(low-latency) 정산을 통해 수 초 내 메시지 전달이 가능합니다.

개념

메타레이어에 대해 더 깊이 이해해보십시오.

체인(Chains)

메타레이어 프로토콜에서는 각 블록체인 네트워크가 고유한 체인 번호로 식별됩니다. 이 체인 식별자는 크로스체인 메시지 전송 시 대상 체인을 지정하는 데 사용됩니다.

크로스체인 작업(Cross-Chain Operations)

메타레이어 메시징은 두 가지 유형의 크로스체인 작업을 지원합니다:

- 쓰기(Write): 체인을 넘나들며 메시지를 전송하고 함수를 실행합니다.
- 읽기(Read): 다른 체인의 컨트랙트에서 데이터를 조회합니다.

메시지 구성 요소(Message Components)

- 대상 도메인(Destination Domain): 메시지를 전송할 대상 블록체인 네트워크
- 수신자 주소(Recipient Address): 메시지를 수신할 컨트랙트 주소
- 읽기 작업(Read Operations): 다른 체인에서 실행할 선택적 조회 작업
- 쓰기 호출 데이터(Write Call Data): 대상 체인에서 실행할 함수 호출
- 완결성 플래그(Finality Flag): 소스 체인에서 완결성이 확인될 때까지 릴레이를 대기할지 여부

전체 사양은 [Contract Interfaces 문서](#)를 참조하십시오.

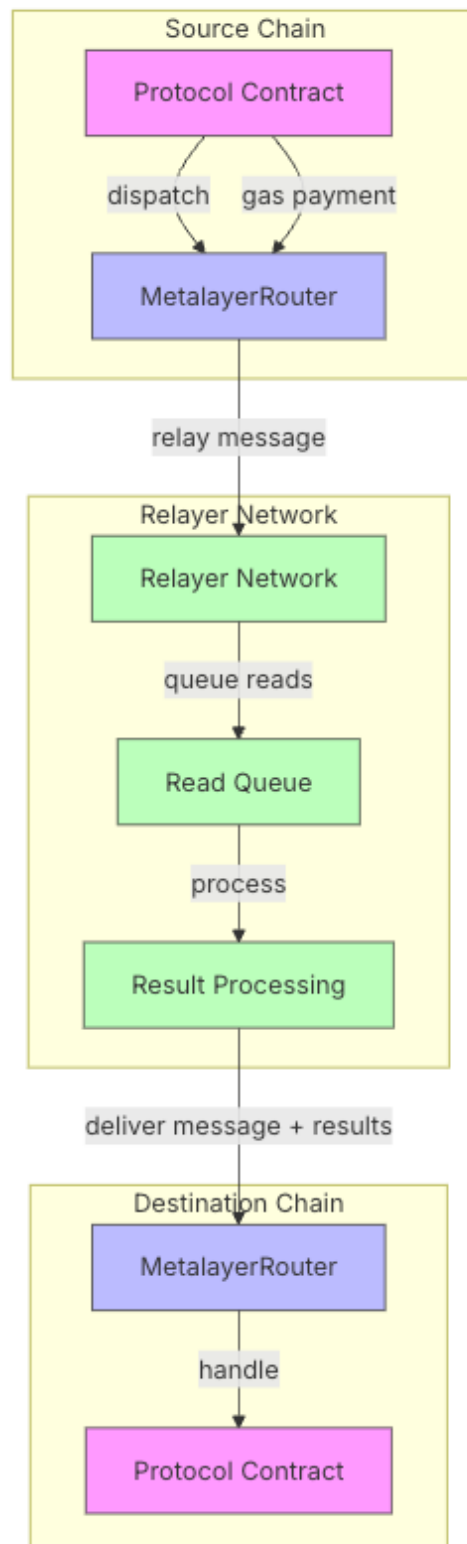
가스 추상화(Gas Abstraction)

메타레이어는 크로스체인 가스 비용을 처리하여, 개발자가 소스 체인의 네이티브 토큰으로 대상 체인에서의 실행 비용을 지불할 수 있도록 지원합니다.

시스템 아키텍처(System Architecture)

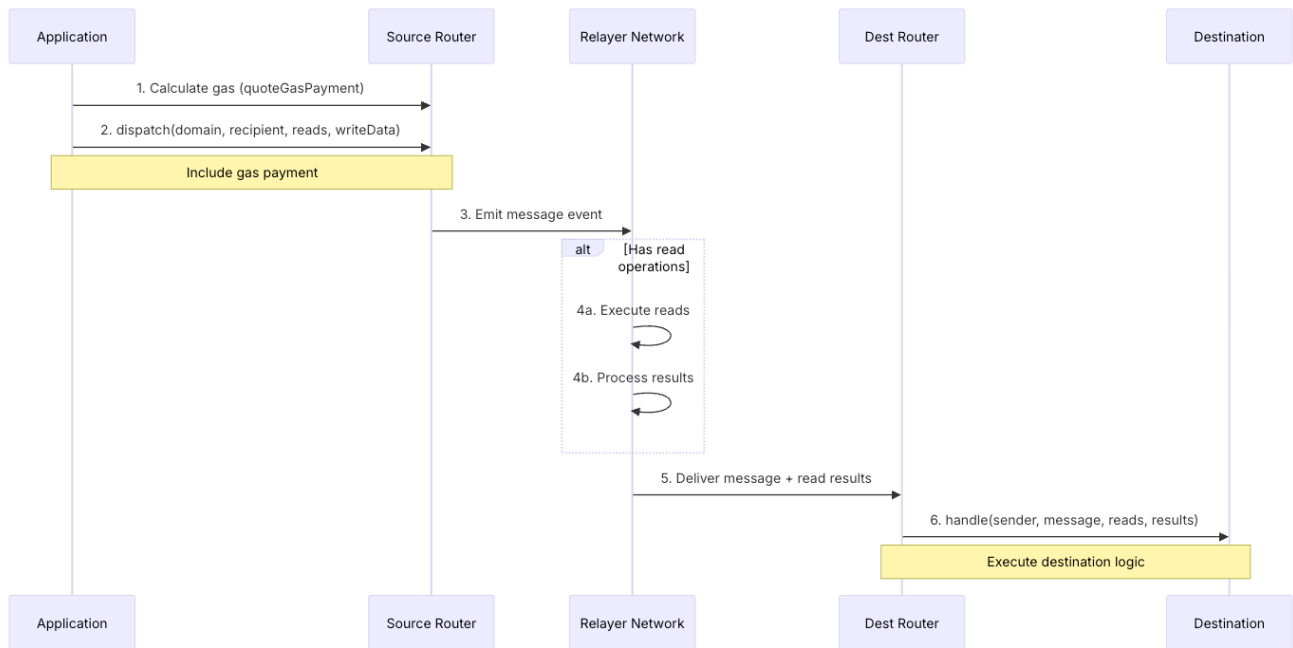
구성 요소 아키텍처(Component Architecture)

아래 다이어그램은 메타레이어 시스템의 주요 구성 요소들과 그 상호작용 방식을 보여줍니다.



메시지 흐름

아래 시퀀스 다이어그램은 크로스체인 메시지를 전송하는 단계별 과정을 보여줍니다.



인텐트(Intent)

개요 및 아키텍처

메타레이어는 롤업을 위한 자산 온보딩과 선언적 크로스체인 실행을 빠르게 처리할 수 있는 종단 간(인텐트 기반) 실행 엔진을 포함하고 있습니다.

인텐트 기반 크로스체인 실행

메타레이어의 인텐트 기반 실행 엔진은 개발자가 저수준 트랜잭션이 아닌 고수준의 인텐트를 명시함으로써, 크로스체인 상호작용을 간소화하도록 설계되었습니다. 이러한 접근 방식은 자산 온보딩과 크로스체인 실행 절차를 단순화하며, 다음과 같은 주요 이점을 제공합니다:

- **선언적 실행(Declarative Execution):** 개발자는 다양한 체인에서 어떤 방식으로 실행할지를 명시하지 않고, 자신이 달성하고자 하는 바(의도)만 정의할 수 있습니다. 이러한 추상화는 크로스체인 작업의 복잡성과 오류 가능성을 줄여줍니다.
- **빠른 자산 온보딩(Fast Asset Onboarding):** 메타레이어는 새로운 자산을 크로스체인 생태계에 신속하게 통합할 수 있도록 하여, 개발자가 애플리케이션의 범위와 기능을 빠르게 확장할 수 있게 합니다.
- **매끄러운 상호운용성(Seamless Interoperability):** 메타레이어 인프라를 활용하면, 최소한의 마찰로 여러 체인에 걸쳐 인텐트를 실행할 수 있어, 사용자에게 원활한 경험과 일관된 성능을 제공합니다.
- **보안성과 신뢰성(Security and Reliability):** 메타레이어의 아키텍처는 견고한 보안 프로토콜을 기반으로 구축되어, 모든 지원 체인에서 인텐트가 안전하고 안정적으로 실행되도록 보장합니다.
- **유연성과 확장성(Flexibility and Scalability):** 이 시스템은 다양한 사용 사례를 수용할 수 있도록 설계되었으며, 애플리케이션 및 사용자 기반이 성장함에 따라 그 수요를 충족시킬 수 있는 확장성을 갖추고 있습니다.

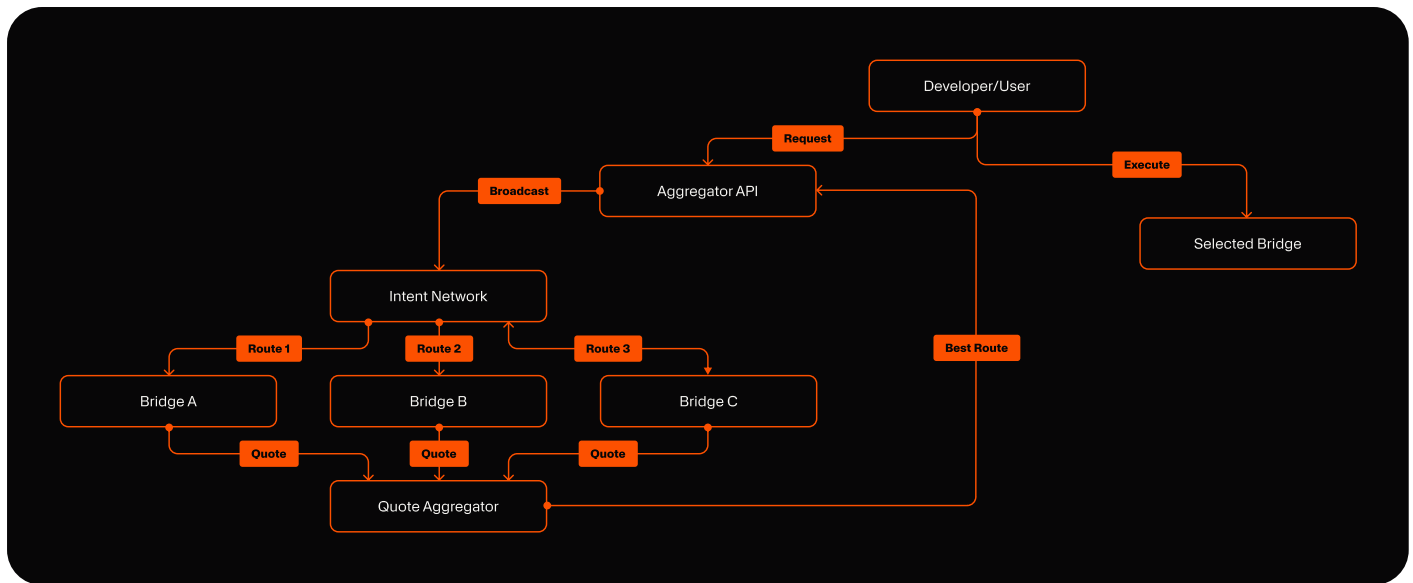
메타레이어의 인텐트 엔진은 복잡한 크로스체인 애플리케이션을 구축하고자 하는 개발자에게 매우 강력한 도구이며, 복잡한 작업을 손쉽게 안정적으로 실행할 수 있는 인프라를 제공합니다.

집계 계층(Aggregation Layer)

집계 계층은 API 및 UI 를 통해 전체 브릿지 네트워크에 대한 접근을 통합합니다. 개발자가 API 또는 SDK 를 통해 요청을 제출하면, 시스템은 해당 인텐트를 통합된 브릿지들에 송출합니다. 칼데라의 견적 집계기는 각 브릿지의 응답을 수집하고 비교하여, 비용, 속도, 신뢰성을 기준으로 최적의 경로를 자동으로 선택합니다.

메타레이어 베타에서는 사용자 비용 절감이 최우선 과제입니다.

구조



UI (사용자 인터페이스)

집계 계층의 UI 는 최종 사용자들이 메타레이어의 브릿지 네트워크와 손쉽게 상호작용할 수 있도록 구성된 사용자 친화적인 인터페이스를 제공합니다. 이를 통해 사용자는 다음과 같은 작업을 수행할 수 있습니다:

- **사용 가능한 경로 탐색:** 사용자는 다양한 브릿징 경로를 탐색할 수 있으며, 각 경로에 대한 비용, 속도, 신뢰성 지표 등의 상세 정보를 확인할 수 있습니다.
- **선호 경로 선택:** 사용자는 자신의 우선순위(예: 낮은 비용, 빠른 트랜잭션 처리 시간 등)에 따라 원하는 경로를 선택할 수 있습니다.
- **트랜잭션 진행 상황 추적:** 사용자는 크로스체인 트랜잭션의 상태를 실시간으로 모니터링할 수 있으며, 문제 발생이나 업데이트에 대한 상세 로그 및 알림을 확인할 수 있습니다.
- **설정 개인화:** 사용자는 비용과 속도에 대한 허용 기준을 설정하는 등, 경로 선택에 대한 자신의 선호를 자유롭게 조정할 수 있습니다.

개발자는 이 UI 를 완전히 화이트라벨링하여 자체 사용은 물론, 생태계 내 애플리케이션에 적용할 수 있습니다. 이를 통해 다양한 플랫폼에서 일관된 사용자 경험과 매끄러운 통합을 구현할 수 있습니다.

이 UI 는 직관적으로 설계되어 초보 사용자와 숙련된 사용자 모두에게 매끄럽고 편리한 경험을 제공합니다.

라우팅 API (Routing API)

라우팅 API 는 개발자가 집계 계층의 기능에 프로그래밍 방식으로 접근할 수 있도록 하는 강력한 도구입니다. 주요 기능은 다음과 같습니다:

- **인텐트 제출:** 개발자는 소스 체인과 대상 체인, 자산 유형, 원하는 결과와 같은 파라미터를 명시하여 크로스체인 인텐트를 API 를 통해 제출할 수 있습니다.
- **견적 조회:** API 는 통합된 브릿지들로부터 실시간 견적을 제공하여, 개발자가 비용, 속도, 신뢰성을 기준으로 다양한 옵션을 비교할 수 있도록 합니다.
- **트랜잭션 실행:** 경로가 선택되면 API 는 트랜잭션 실행을 지원하여, 안전하고 효율적인 크로스체인 전송이 이루어지도록 합니다.
- **알림 수신:** 개발자는 웹훅(webhook) 또는 콜백(callback)을 설정하여 트랜잭션 상태에 대한 업데이트를 실시간으로 수신할 수 있으며, 변경사항이나 문제 발생 시 즉시 인지할 수 있습니다.

라우팅 API 는 유연하고 확장 가능한 설계로 되어 있어, 다양한 사용 사례 및 통합 시나리오를 폭넓게 지원합니다.

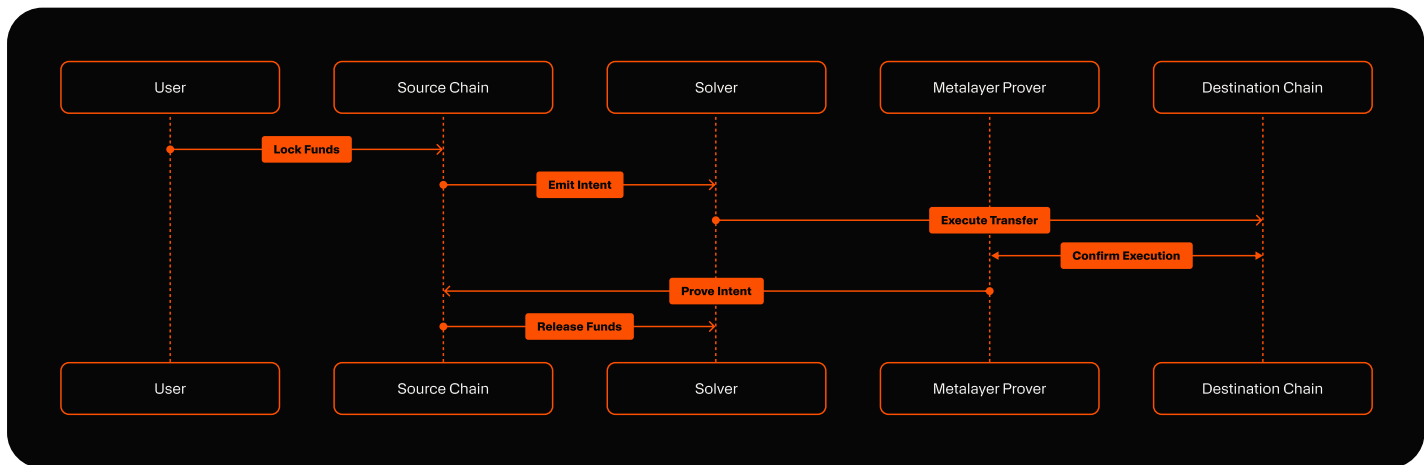
서드파티 브릿지 통합

서드파티 브릿지는 메타레이어를 활용하여 메타레이어가 지원하는 체인 간의 인텐트 이행을 증명하도록 권장됩니다. 이 증명 절차는 일반적으로 정산(settlement) 이라고 하며, 대상 체인에서 소스 체인으로 크로스체인 메시지를 다시 전송하는 방식에 기반합니다. 대부분의 구현에서는, 해당 메시지를 수신함으로써 에스크로에 보관되어 있던 브릿지 자금이 솔버(solver)의 지갑으로 해제됩니다.

브릿지 개발자들은 종종 롱테일 체인이나 신규 체인에 배포할 때 어려움을 겪습니다. 이는 메시지 전달 시스템이 존재하지 않거나, 각 배포 환경마다 보안 보장이 일관되지 않기 때문입니다. 메타레이어는 이러한 문제를 해결하기 위해 모든 칼데라 체인에서 사용할 수 있는, 보안성 있고 신뢰할 수 있으며 조합 가능한 메시지 전달 시스템을 제공합니다.

또한 인텐트 프로토콜과 솔버는 메시지 전달 레이어(Message Passing Layer)에 의해 강제되는 완결성 요건(finality requirements) 을 지정할 수 있어, 더욱 정교한 정산이 가능합니다.

예를 들어, 에코 라우트(Eco Routes)는 메타레이어를 인텐트 정산 옵션으로 지원하도록 수정되었으며, 메타레이어의 일환으로 모든 칼데라 체인에 배포될 예정입니다.



이러한 아키텍처를 통해 메타레이어는 기존 체인에 즉각적인 가치를 제공하는 동시에, 향후 크로스체인 기술의 발전을 위한 기반을 마련합니다.

인텐트(Intent) 중심의 설계는 새로운 검증 방식이나 브릿지 프로토콜이 등장하더라도, 생태계 내 모든 참여자가 통합 구조를 변경할 필요 없이 자동으로 그 혜택을 누릴 수 있도록 보장합니다.

정산 계층(Settlement Layer)

정산 계층은 메타레이어 생태계 내에서 크로스체인 메시지와 인텐트 실행에 대한 보안 완결성(finality) 를 제공합니다.

이 계층은 크로스체인 메시지 전달 및 인텐트 실행을 위한 보안의 중추(backbone) 역할을 하며, 체인 간 신뢰할 수 있는 파이널리티를 보장하고 다양한 요구사항에 맞는 유연한 보안 옵션을 제공합니다.

핵심 구성 요소

메시지 보안(Message Security)

- 인터체인 보안 모듈(Interchain Security Module, ISM)을 활용하여 메시지를 검증하고 보안을 확보합니다.
- 다중 서명 기반의 완결성 메커니즘을 사용하여 보안성과 효율성 간의 균형을 유지하며, 메시지 무결성을 위한 강력한 프레임워크를 제공합니다.

인텐트 정산(Intent Settlement)

- 검증 이후의 최종 실행을 관리합니다.
- 체인 간 원자적(atomic) 정산을 보장하여 부분 실행 상태를 방지하고 일관성을 유지합니다.

브릿지 통합(Bridge Integration)

- 고가치 트랜잭션을 위한 정산 경로 최적화를 위해 네이티브 브릿지 프로토콜과 통합됩니다.
- 기존 인프라를 활용하여 매끄러운 크로스체인 상호작용을 실현합니다.

보안 모델(Security Model)

보안 모델은 매우 유연하게 구성할 수 있도록 설계되어 있습니다. 사용자는 자신에게 적합한 보안 수준을 선택할 수 있으며, 이는 솔버의 견적(quote)에 비용 요소로 반영됩니다. 이로써 비용과 보안 간의 트레이드오프를 정량적으로 판단할 수 있습니다. 정산 계층은 가능한 경우 기존 체인의 보안 메커니즘을 우선 활용하며, 기존 보안이 충분하지 않은 경우에는 보완 메커니즘(fallback)을 통해 무결성을 유지합니다.

정산 절차(Settlement Process)

- 검증(Validation):** 실행 전 모든 전제 조건과 보안 요건을 확인하여 준비 상태를 점검합니다.
- 실행(Execution):** 관련된 모든 체인에서 동시에 일괄 정산을 수행합니다.
- 확인(Confirmation):** 모든 작업이 정확하게 완료되었는지를 최종 검증하여 실행의 적절성을 보장합니다.

통합 지점(Integration Points)

메시지 전달(Message Passing)

- 메시지 무결성과 보안을 확보하기 위해 메시지를 검증합니다.
- 메시지의 최종 처리 상태를 확정하여 신뢰할 수 있는 크로스체인 커뮤니케이션을 유지합니다.

인텐트 실행(Intent Execution)

- 인텐트의 최종 정산을 실행합니다.
- 사용자 설정에 따라 선택된 보안 구성을 적용하여 안전한 실행을 보장합니다.

향후 개발 계획(Future Development)

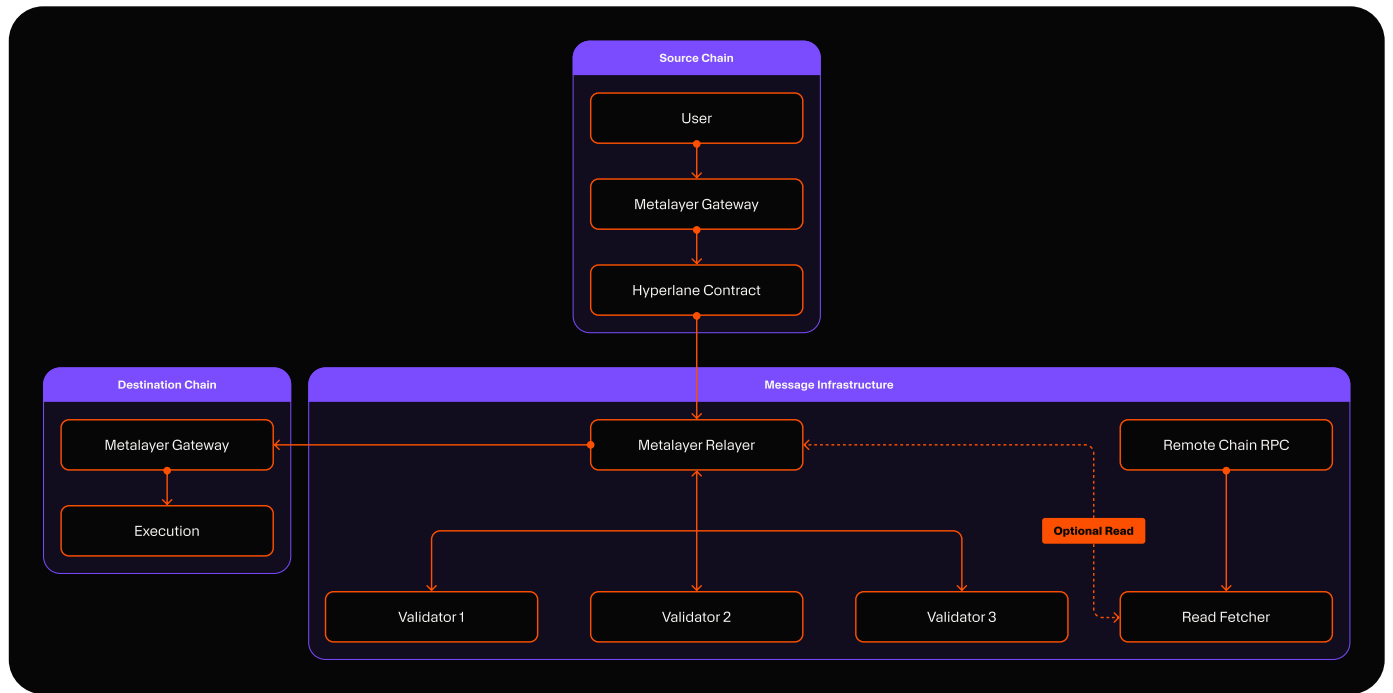
정산 계층은 네트워크의 발전에 맞춰 지속적으로 진화할 수 있도록 설계되었습니다. 향후 계획은 다음과 같습니다:

- 새로운 위협에 대응하고 최신 기술을 활용하기 위해 추가 보안 모듈을 지원합니다.
- 정산을 위한 스택 네이티브 상호운용성 옵션을 통합합니다.
- 복잡한 인텐트, 즉 다수의 크로스체인 작업을 요구하는 실행도 처리할 수 있도록 확장합니다.

메세지 전달(Message Passing)

개요(Overview)

메타레이어는 인텐트 기반 프로토콜의 정산(Settlement) 을 지원하도록 설계되었습니다. 초기에는 브릿징(bridging) 사례를 중심으로 시작하지만, 점차 더 다양한 인텐트 기반 프로토콜을 온보딩할 계획입니다. 메타레이어는 하이퍼레인 위에 구축된 보안 메시지 전달 시스템을 제공하며, 이는 모든 칼데라 체인에 자동으로 배포됩니다. 메시지에는 선택적으로 여러 체인으로부터 상태(state)를 조회하는 기능을 포함할 수 있어, 네트워크 전반에 걸쳐 실시간으로 데이터를 확인할 수 있습니다.



구성 가능한 완결성(Configurable Finality)

메타레이어의 메시지는 두 가지 완결성 모드를 지원하여, 개발자가 속도와 보안 간의 균형을 조정할 수 있도록 합니다:

1. 소프트 완결성 (Soft Finality, 기본값)

- 지연 시간: 약 10 초
- 밸리데이터가 시퀀서가 트랜잭션을 포함시키겠다는 커밋을 확인합니다.
- 빠른 정산이 필요한 대부분의 애플리케이션에 적합합니다.
- 신뢰 모델: 밸리데이터가 시퀀서의 피드 데이터를 정직하게 보고한다는 가정에 기반합니다.

2. 완결 모드 (Finalized Mode)

- 상위 체인(parent chain)에 배치(batch) 제출 및 해당 체인에서의 완결성 확보가 필요합니다.

- 시퀀서의 리오그(reorg) 발생에 대한 보호 기능을 제공합니다.
- 참고: 옵티미스틱 롤업은 여전히 7일간의 이의 제기(dispute) 기간을 유지합니다.
- 신뢰 모델은 소프트 완결성 동일하나, 추가적인 리오그 방어 메커니즘이 적용됩니다.
- 고액 자산 이동 또는 보안이 중요한 애플리케이션에 권장됩니다.

향후 롤업 스택이 스택 네이티브 상호운용성(예: Superchain, ZKSync 의 네이티브 브릿징 등)을 지원하도록 발전함에 따라, 메타레이어는 이러한 메커니즘을 자동으로 활용하도록 업그레이드됩니다. 완결 모드를 지정한 애플리케이션은 코드 변경 없이 향상된 보안 보장의 혜택을 자연스럽게 누릴 수 있습니다. 즉, 개발자가 특정 생태계에 종속되지 않고도, 스택 네이티브 상호운용성(stack-native interop)의 미래 기술을 오늘부터 적용할 수 있게 합니다.

롤업 엔진(Rollup Engine)

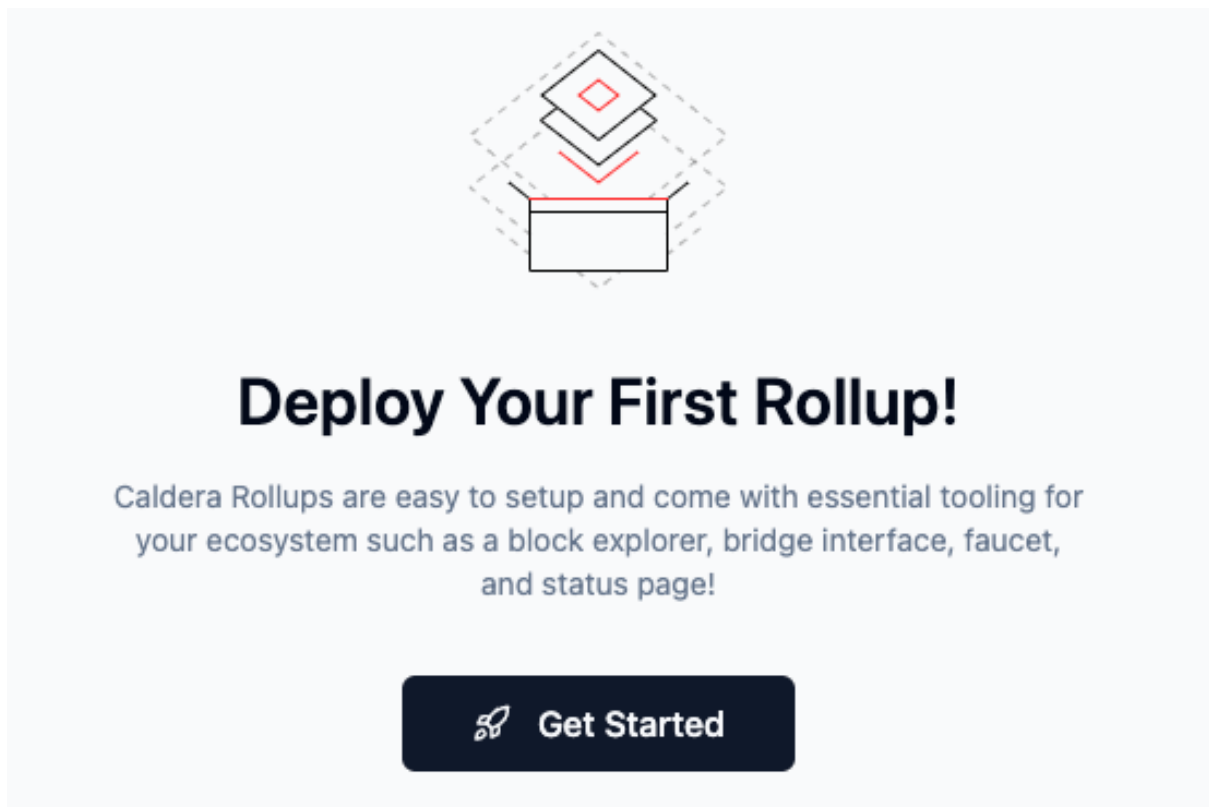
빠른 시작(Quickstart)

칼데라가 호스팅하는 전용 롤업을 배포하려면 다음 절차를 따라 시작할 수 있습니다.

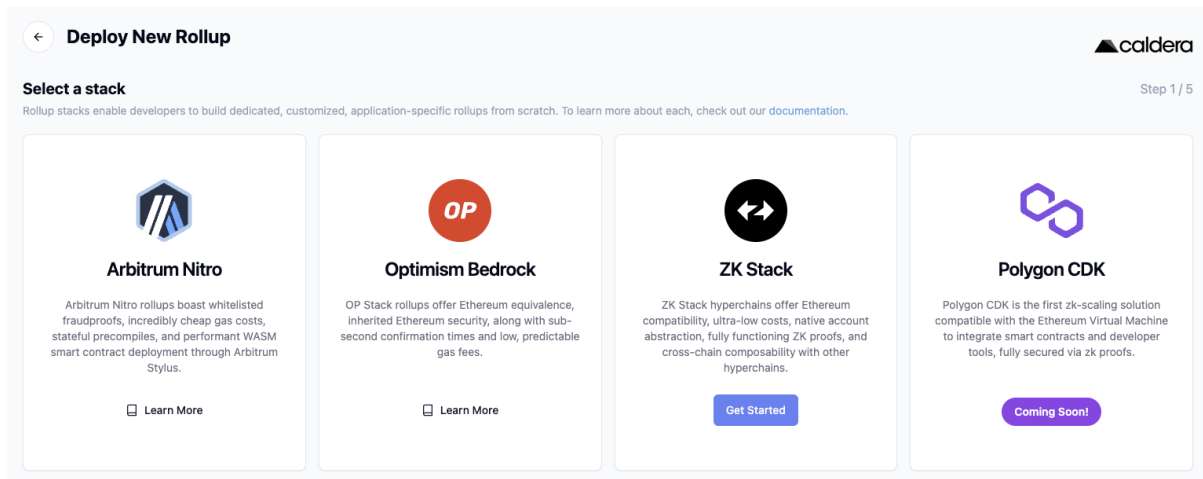
테스트넷(Testnet)

테스트넷 환경에서 시작하려면, 아래 단계에 따라 대시보드에 접속하십시오:

1. 인증 페이지에서 회원가입하거나 로그인합니다.
2. Manage Rollups 페이지에서 “Get Started” 버튼을 클릭합니다.



3. 원하는 롤업 프레임워크(Arbitrum Nitro, Optimism Bedrock, zkSync 의 ZK Stack 중 선택)를 선택한 후, Deploy New Rollup 페이지에서 테스트넷 네트워크 유형을 선택합니다.



- 네이티브 가스 토큰을 선택하고, 롤업 이름(Rollup Name), 서브도메인(Subdomain), 체인 ID(Chain ID) 등 관련 식별자를 설정합니다.
- “Deploy New Rollup” 버튼을 클릭하여 테스트넷 롤업을 시작합니다!

메인넷(Mainnet)

- 프로젝트 요구사항과 앱 롤업(app-rollup)을 고려하는 이유에 대해 논의하고 싶다면 데모를 예약해 주세요. 다양한 지원 방안을 고민해보겠습니다.
- 칼데라는 귀하가 선택한 롤업 프레임워크(Arbitrum Nitro, Optimism Bedrock, ZK Stack 등)와 파라미터, 그리고 체인(Ethereum, Polygon, Cronos, Optimism, Arbitrum 등)을 기반으로 맞춤형 롤업을 배포해드립니다.
- 귀하의 애플리케이션을 칼데라에 통합하세요. 일반적으로 이더리움 기반 앱을 칼데라 체인으로 이전하는 데는 30 분도 채 걸리지 않습니다. 칼데라 팀이 적극적으로 지원해드립니다!
- 프로덕션 수준의 메인넷 롤업이 라이브로 전환되는 시점에 칼데라가 직접 안내드리겠습니다.

칼데라 체인 소개

롤업(Rollups)이란?

롤업은 블록체인 네트워크의 확장성과 효율성을 높이기 위해 설계된 레이어 2 확장 솔루션입니다. 간단히 말해, 롤업은 자체 블록체인이지만, 정산(settlement)은 주로 이더리움(Ethereum)과 같은 레이어 1 블록체인에 의존합니다. 이와 동시에, 기본 체인보다 더 나은 확장성과 성능을 제공합니다.

트랜잭션 묶기(Bundling Transactions)

롤업은 여러 개의 트랜잭션을 하나의 트랜잭션 또는 배치(batch)로 집계(롤업)하여 처리합니다. 이 작업은 레이어 2 블록체인, 즉 기존 레이어 1 위에 구축된 보조 구조에서 수행됩니다.

오프체인 실행(Off-chain Execution)

트랜잭션 실행은 체인 밖에서 수행되므로, 레이어 1에 기록해야 하는 데이터 양이 줄어듭니다. 이 방식은 특히 혼잡한 블록체인 네트워크에서 유리하며, 처리 속도를 높이고 수수료 부담을 낮춥니다.

레이어 1에 게시(Posting to Layer 1)

트랜잭션이 오프체인에서 묶여 실행된 후, 단일 트랜잭션 또는 요약 정보가 레이어 1 블록체인에 게시됩니다. 이렇게 하면 기본 체인의 보안성을 유지하면서도 데이터 부하를 크게 줄일 수 있습니다, 왜냐하면 전체 트랜잭션이 아닌 집계된 결과만 기록되기 때문입니다.

옵티미스틱 롤업(Optimistic Rollups)

칼데라를 통해 Arbitrum Nitro 및 OP Stack 기반의 롤업을 배포할 수 있습니다. 이 두 스택은 모두 “옵티미스틱(Optimistic)” 롤업입니다.

옵티미스틱 롤업의 “옵티미스틱”이라는 용어는 트랜잭션이 올바르다는 낙관적 가정에 기반합니다. 정상적인 경우에는 온체인 상에서의 정확성 증명이 필요하지 않습니다. 하지만 시퀀서가 악의적으로 행동하거나 오류가 발생한 경우, L1 체인에 사기 증명(fault proof)을 제출하여 잘못된 실행을 방지할 수 있습니다.

영지식 롤업(Zero-Knowledge Rollups)

칼데라를 통해 ZK Stack 및 Polygon CDK 기반의 롤업도 배포할 수 있으며, 이 두 스택은 모두 영지식(ZK) 롤업에 해당합니다. ZK 롤업은 옵티미스틱 롤업과 달리, 각 상태 변경(state update)을 위해 유효성 증명(validity proof)을 제출해야 합니다. 이 유효성 증명은 제안된 상태 변경이 실제로 해당 트랜잭션 배치를 실행한 결과임을 암호학적으로

보장합니다. 따라서 ZK 롤업은 트랜잭션 데이터를 모두 온체인에 게시할 필요 없이, 유효성 증명만으로도 이더리움 상에서 트랜잭션을 완결(finality) 지을 수 있습니다.

칼데라 롤업 스택

Arbitrum Nitro

칼데라를 통해 아비트럼 Arbitrum Nitro 스택을 기반으로 전용 롤업을 배포할 수 있습니다. Arbitrum Nitro 는 입증된 옵티미스틱 롤업 스택으로, 대표 체인인 Arbitrum One 과 게임 중심 저비용 체인인 Arbitrum Nova 를 구동합니다. 현재 Nitro 는 운영 중인 여러 체인에서 60 억 달러 이상의 TVL 을 확보하고 있습니다.

주요 이점

- 이더리움 대비 10~100 배 저렴한 트랜잭션 수수료
- 이더리움 호환성(Ethereum equivalence): 이더리움 스마트 컨트랙트와 개발 도구를 완벽히 지원합니다.
- 더 빠른 블록 생성 시간: 고부하 상황에서도 최대 250ms 까지 단축 가능
- 작동하는 사기 증명(Fault Proofs) 시스템 지원
- Stylus 를 통한 WASM 스마트 컨트랙트 선택적 지원
- Arbitrum AnyTrust 또는 Celestia DA 를 통한 추가 비용 절감 기능
- 롤업의 네이티브 토큰을 자유롭게 선택 가능

AnyTrust

Arbitrum AnyTrust 는 Arbitrum Nitro 기술의 변형으로, 부분적인 신뢰 모델을 채택하여 트랜잭션 비용을 낮추는 구조입니다. 표준 Arbitrum 에서는 모든 노드가 레이어 2 의 모든 데이터를 직접 접근해야 하지만, AnyTrust 는 데이터 가용성 위원회(DAC) 를 활용하여 요청 시 데이터 제공 방식으로 운영됩니다. 위원 중 최소 두 명이 신뢰할 수 있다는 가정 하에 동작하며, DACert (데이터 가용성 인증서) 를 통해 지정된 기간 동안 데이터 가용성을 보장합니다.

AnyTrust 를 활용하면 표준 롤업 대비 10~100 배 추가 비용 절감이 가능합니다. 이 구조는 데이터 가용성을 확보하면서도 비용 효율적인 트랜잭션 처리를 가능하게 하며, 이더리움 보안을 기반으로 하는 고성능 롤업 또는 AnyTrust 체인을 구축하는 데 적합합니다.

Stylus

Arbitrum Stylus 는 Arbitrum Nitro 의 기술 발전형으로, 이더리움 가상머신(Ethereum Virtual Machine, EVM)과 동등한 권한의 WASM 가상 머신을 함께 도입합니다. Stylus 는 Arbitrum One, Arbitrum Nova, Arbitrum Orbit 등에서 실행되며, Rust, C, C++ 등 다양한 언어로 스마트 컨트랙트를 작성할 수 있는 환경을 제공합니다.

Stylus 의 WASM 실행 성능은 기존 대비 10 배 이상 가스 절감 효과가 있으며, 검증된 Rust/C/C++ 라이브러리를 그대로 스마트 컨트랙트에 활용할 수 있다는 장점이 있습니다.

옵티미즘 베드록(Optimism Bedrock)

칼데라를 통해 OP 스택(Optimism Bedrock) 기반의 전용 롤업을 배포할 수 있습니다.

OP 스택은 입증된 옵티미스틱 롤업 기술 스택이며, 옵티미즘 메인넷과 코인베이스(Coinbase)에서 출시한 L2 체인인 Base 의 기반이기도 합니다. 현재 OP 스택은 전체적으로 35억 달러 이상의 TVL 을 확보하고 있습니다.

주요 이점

- 이더리움 대비 10~100 배 저렴한 트랜잭션 수수료
- 이더리움 완전 호환성: 스마트 컨트랙트 및 개발 도구를 완벽하게 지원합니다
- 빠른 블록 생성 속도: 블록당 약 2 초
- Celestia DA 를 통한 추가 비용 절감 기능 (선택 사항)
- 매우 유연한 MIT 라이선스 채택
- 옵티미즘의 미래 네트워크인 Superchain 에 참여 가능

슈퍼체인(Superchain)

옵티미즘 슈퍼체인은 옵티미즘 프로토콜 기반의 상호 연결된 체인 네트워크를 지향하며, 레이어 2 블록체인 간의 확장성과 상호운용성을 강화하기 위해 설계되었습니다.

슈퍼체인은 옵티미즘 메인넷과 기타 OP 스택 체인을 하나의 연결된 네트워크로 통합하는 것을 목표로 하며, 브릿징, 탈중앙화 거버넌스, 커뮤니케이션 레이어와 같은 공통 기능을 공유합니다. 이러한 구조는 개별 체인이 통합된 생태계 내에서 유기적으로 작동할 수 있도록 하여, 체인 간의 원활한 커뮤니케이션과 트랜잭션을 가능하게 합니다.

슈퍼체인은 아직 초기 설계 단계에 있으며, 가장 최신의 구조와 세부사항은 옵티미즘 공식 문서를 통해 확인하시길 권장드립니다.

ZK Stack

ZK Stack 은 지케이싱크(zkSync) 인프라를 기반으로 맞춤형 ZK 기반 하이퍼체인을 구축할 수 있도록 설계된 모듈형 오픈소스 프레임워크입니다. ZK Stack 의 핵심은 독립성(sovareignty) 과 매끄러운 연결성(seamless connectivity) 입니다. 각 하이퍼체인은 완전한 독립적 체인으로 동작하며, 이더리움 L1 에만 생존성과 보안을 의존합니다. 모든 하이퍼체인은 공유 브릿지를 통해 상호 연결되어 있으며, 이를 통해 무신뢰(trustless), 빠른 속도(수 분 내), 낮은 비용(단일 트랜잭션 수준)의 상호운용성을 제공합니다.

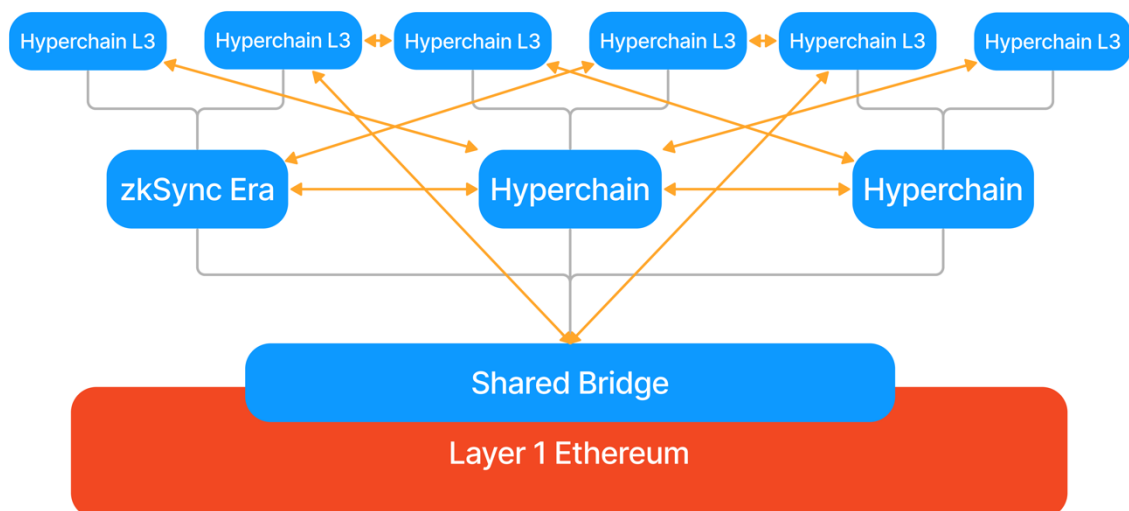
주요 이점

- 이더리움 대비 초저가 가스 수수료
- 이더리움 완전 호환성: 스마트 컨트랙트 및 개발 도구 전면 지원
- 네이티브 계정 추상화(account abstraction)
- 하이퍼브릿지를 통한 네이티브 크로스체인 구성가능성(composability)
- 대체 데이터 가용성(DA) 솔루션을 통한 추가 비용 절감 가능성
- 롤업의 네이티브 토큰을 자유롭게 선택 가능

하이퍼체인(Hyperchains)

하이퍼체인(Hyperchain) 은 L1 메인넷에서 공통 정산을 공유하며, 병렬로 실행되는 프랙탈 구조의 zkEVM 인스턴스입니다. ‘하이퍼브릿지(Hyperbridge)’라는 이름은 웹의 하이퍼링크에서 유래했으며, 사용자가 웹사이트 간을 자유롭게 이동하듯, ZK Stack 롤업들도 하이퍼브릿지를 통해 매끄럽게 연결됩니다.

각 하이퍼체인은 zkSync Era 에 적용된 것과 동일한 zkEVM 엔진을 기반으로 작동하며, 사용되는 ZK 증명 회로(ZKP circuits) 도 완전히 동일하게 유지됩니다. 따라서 누구나 배포하더라도 이더리움 L1 의 보안을 그대로 상속받을 수 있으며, 추가적인 신뢰나 보안 가정이 전혀 필요 없습니다.



맞춤 설정(Customizations)

네이티브 가스 토큰(Native Gas Token)

칼데라 체인을 사용하면, 아비트럼(Arbitrum) 및 지케이싱크(zkSync) 기반 롤업을 맞춤형 네이티브 가스 토큰으로 배포할 수 있습니다.

어떤 토큰을 사용할 수 있습니까?

대부분의 ERC-20 토큰을 롤업의 네이티브 토큰으로 사용할 수 있습니다. 여기에는 귀하의 프로토콜 자체 토큰은 물론, USDC, DAI 와 같은 스테이블코인도 포함됩니다.

단, 공급량이 탄력적으로 변동하는 토큰(elastic tokens) 은 예외입니다. 이러한 토큰은 롤업의 네이티브 토큰으로 사용할 수 없습니다, 하지만 다행히도 실제로 이 설계를 사용하는 토큰은 매우 드뭅니다. 귀하의 네이티브 가스 토큰은 반드시 표준 ERC-20 토큰이어야 합니다.

대체 데이터 가용성(Alternative Data Availability)

※ 이 기능은 베타 버전입니다. 시작을 원하신다면 칼데라 팀에 문의해 주세요.

칼데라는 Celestia, Near, Arbitrum AnyTrust 와의 통합을 통해 대체 데이터 가용성(Alt-DA) 을 지원합니다.

왜 대체 DA 가 필요한가요?

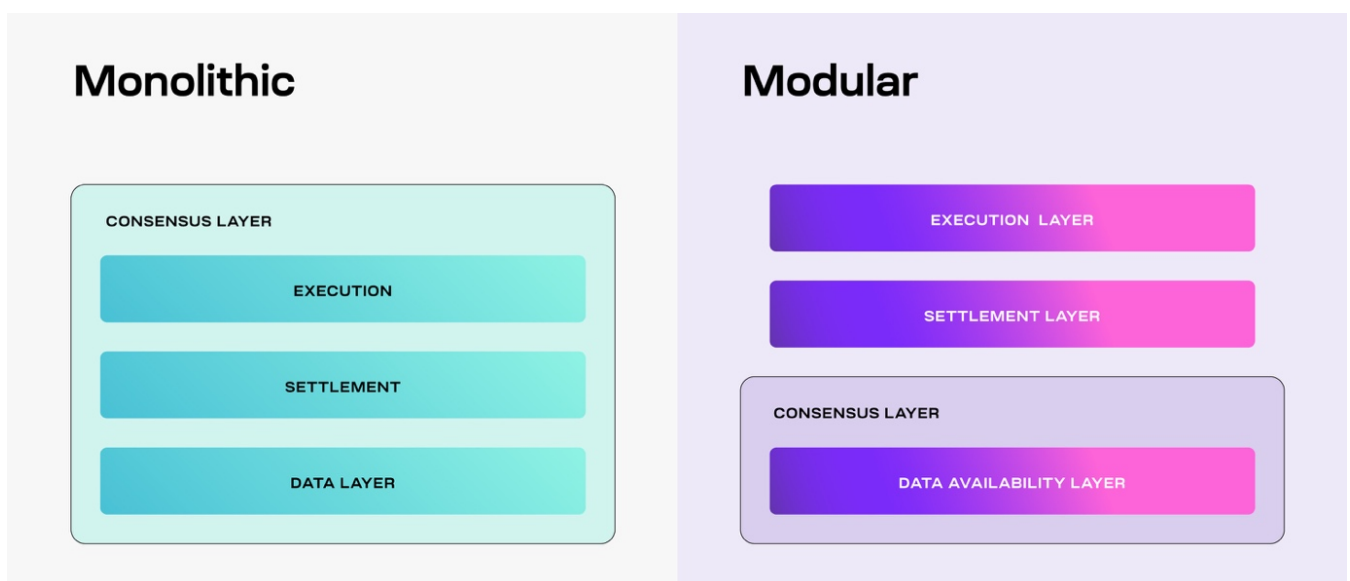
롤업에서 잘못된 트랜잭션이 처리될 경우, 이를 탐지하고 되돌릴 수 있으려면, 해당 롤업 블록의 데이터가 실제로 게시되었는지 확인할 수 있는 수단이 필요합니다.

현재 대부분의 이더리움 롤업은 모든 롤업 블록 데이터를 이더리움 L1 에 게시하고, 이더리움을 데이터 가용성 기반으로 활용함으로써 이 문제를 해결합니다.

그러나 전통적인 이더리움 기반 DA 는 모든 디앱 및 사용자와 제한된 이더리움 블록 공간을 두고 경쟁해야 하기 때문에 비용이 매우 높고 변동성도 크다는 문제가 있습니다. 결과적으로, 롤업 트랜잭션의 전체 비용 중 95% 이상이 데이터 게시에 사용되고 있습니다.

작동 방식

대체 DA 시스템은 데이터 가용성을 체인의 정산(settlement) 기능과 분리함으로써, 관련 비용을 대폭 절감하고 처리량을 높여, 롤업의 장기 확장성을 크게 향상시킵니다. 현재 칼데라는 셀레스티아(Celestia)와 니어(Near)를 모든 체인에서 활용 가능한 대체 DA 솔루션으로 공식 지원하고 있으며, 향후 더 많은 Alt-DA 공급자와의 통합도 예정되어 있습니다. 이들 기술을 통해 칼데라 생태계 내 체인들의 운영 비용을 현저히 줄일 수 있습니다.



탈중앙화 시퀀싱(Decentralized Sequencing)

칼데라는 프리미어 탈중앙 시퀀싱 네트워크인 에스프레소(Espresso)와의 통합을 통해 탈중앙화 시퀀싱을 지원합니다.

왜 탈중앙화 시퀀싱이 필요한가요?

모든 롤업은 트랜잭션의 순서를 정하고 검증하기 위해 시퀀서(Sequencer)에 의존합니다. 기존에는 이러한 시퀀서가 중앙 집중화된 단일 주체 혹은 소수의 그룹에 의해 운영되었습니다. 실제로 현재 운영 중인 대부분의 롤업(예: Arbitrum One, Optimism 메인넷, Base, zkSync 등)은 모두 중앙화된 시퀀서를 사용하고 있습니다.

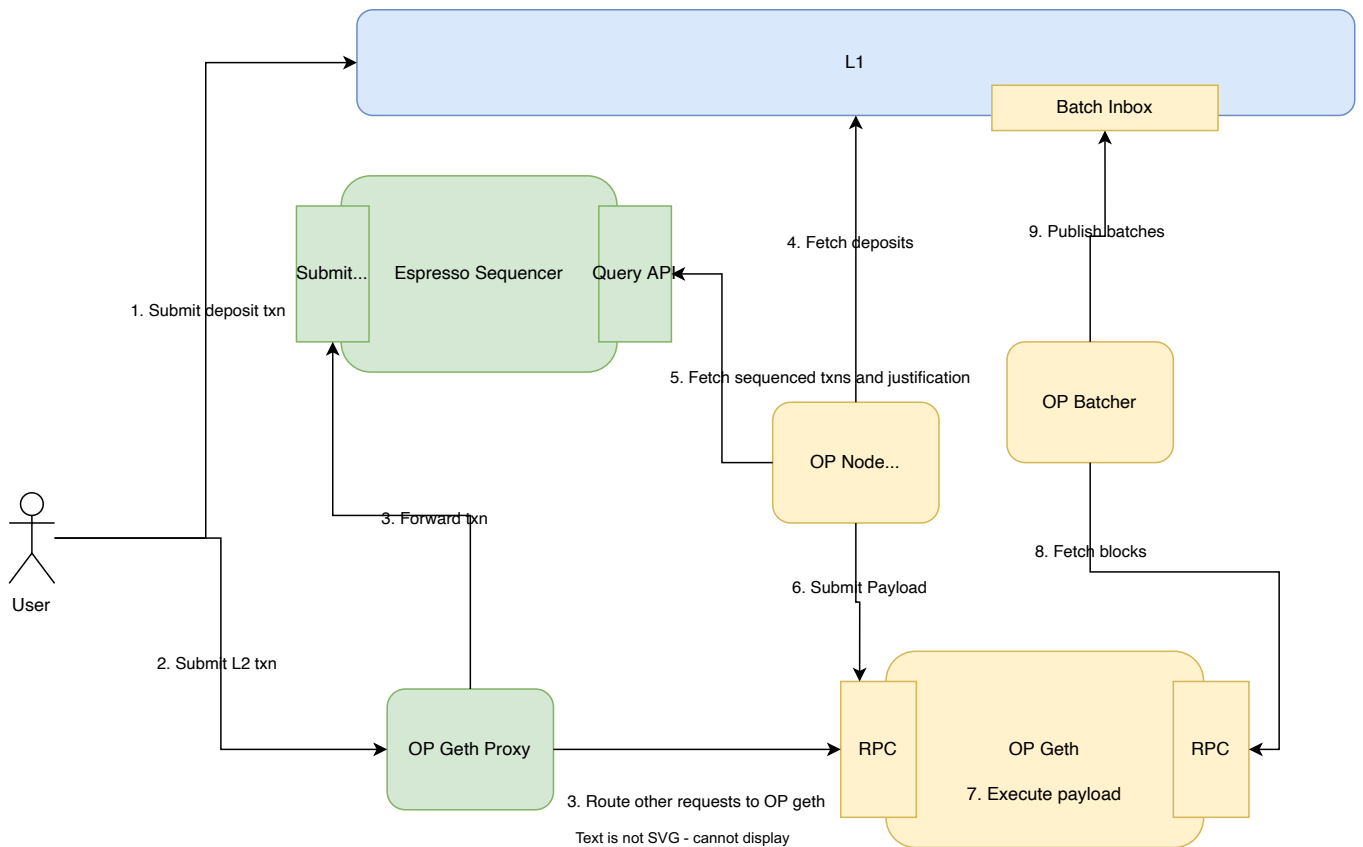
물론 롤업은 자체적인 증명 시스템을 통해 기본 체인의 보안성을 상속받을 수 있지만, 중앙화된 시퀀서는 다음과 같은 문제를 유발합니다:

- 중앙화된 시퀀서는 시스템 내에 단일 장애 지점(single point of failure)을 생성합니다. 시퀀서가 다운될 경우, 트랜잭션을 포함시키기 위해 제출하는 것이 불가능해지거나 지나치게 비싸질 수 있습니다.
- 중앙화된 시퀀서는 트랜잭션을 임의로 검열하거나 지연시킬 수 있으며, 트랜잭션의 순서를 바꿔 MEV를 추출할 수도 있습니다.
- 사용자는 트랜잭션이 어떤 방식으로 정렬되는지에 대한 가시성을 갖지 못합니다.

현재 상태에서는 사용자가 롤업 운영자를 어느 정도 신뢰해야 합니다. 즉, 사용자는 운영자가 시퀀서를 온라인 상태로 유지할 것이라는 점, 시퀀서가 명세에 따라 트랜잭션을 정렬할 것이라는 점, 운영자가 체인에서 MEV를 추출하거나 트랜잭션을 임의로 검열하지 않을 것이라는 점을 신뢰해야 합니다.

작동 방식

높은 수준에서 설명하면, 에스프레소 시퀀서 네트워크는 기존 롤업의 댐풀(mempool) 구현을 대체합니다. 사용자의 트랜잭션은 롤업 노드로 직접 전송되는 것이 아니라 에스프레소 시퀀서로 전송됩니다. 그 후 롤업 노드가 에스프레소 시퀀서 노드로부터 순서화된 트랜잭션을 조회합니다. 이 방식은 공정성을 보장할 수 없는 중앙화 시퀀서에 대한 의존을 제거합니다.



가디언 노드(Guardian Nodes)

칼데라의 가디언 노드 시스템은 제 3 자가 롤업 블록을 검증하고 보상을 받을 수 있는, 업계 최초의 실사용 가능한(production-ready) 시스템입니다. 이 시스템은 아비트럼 롤업을 위한 새로운 형태의 '라이트 검증자(light verifier)' 를 도입하여, 운영자가 전체 아비트럼 노드를 실행하지 않고도 일상적인 하드웨어에서 Nitro 배치를 검증할 수 있도록 합니다.

칼데라는 검증 장벽을 낮추고 보상 인센티브를 분산하는 데 집중함으로써, 아비트럼 롤업의 복원력과 보안성을 향상시키고 있습니다.

주요 이점

1. **수익원 창출** : 가디언 노드는 프로젝트가 직접 수익을 창출할 수 있는 강력한 시장 진입 전략입니다. 예를 들어, HYCHAIN 은 칼데라의 툴링으로 가디언 노드 시스템을 출시한 후, 2 주 만에 약 16,000 개의 노드 키를 판매하고 약 2,000 ETH 를 조달했습니다. 해당 판매는 총 3 년간 진행되며 안정적인 수익 흐름을 제공합니다.
2. **탈중앙화** : EVM 롤업은 확장성 문제는 대부분 해결하였으며, 이더리움 기반의 L2 및 L3 솔루션은 사실상 무한 확장을 가능하게 합니다. 그러나 지금까지는 이 롤업들을 정직하게 감시할 참여자에게 명확한 인센티브가 존재하지 않았습니다. 가디언 노드는 사용자에게 블록을 검증하고 보상을 받도록 허용함으로써, 팀이 롤업을 탈중앙화된 구조로 운영할 수 있게 해줍니다.
3. **토큰 수요 증가** : 더 많은 참여자가 롤업을 감시하고 악의적인 행동을 식별할 수 있게 되면, 네트워크의 보안이 강화되어 체인의 신뢰성 확보에 핵심적인 역할을 합니다. 이로 인해, 검증 참여를 위해 반드시 필요한 네이티브 토큰의 수요가 증가하게 되며, 네트워크에 실질적인 암호경제적 보안 기초를 제공할 수 있습니다.

브릿징된 USDC(Bridged USDC)

칼데라에서는 OP Bedrock 및 Arbitrum Nitro 롤업을 대상으로 써클(Circle)의 브릿징된 USDC 표준을 활용할 수 있습니다. 브릿징된 USDC 는 블록체인, 개발자, 사용자 모두에게 이점을 제공하며, 새로운 블록체인 네트워크의 초기 활성화를 촉진하고, 향후 네이티브 USDC 로의 전환도 간소화합니다.

블록체인을 위한 이점

브릿징된 USDC 를 초기 단계에서 개발자와 사용자에게 제공함으로써, 생태계가 충분히 성숙된 후에는 별도의 유동성 이전이나 커뮤니티 전환 캠페인 없이, 자연스럽게 네이티브 USDC 로 업그레이드할 수 있습니다. 즉, 브릿지 버전에서 네이티브로 전환될 때 발생할 수 있는 시간 소모적인 유동성 마이그레이션 및 사용자 교육 과정을 피할 수 있습니다.

개발자를 위한 이점

- 코드 변경 없이 브릿징된 USDC 를 기반으로 구축 가능하며, 향후 네이티브 USDC 로 업그레이드되더라도 컨트랙트 주소가 유지됩니다.
- 사용자에게는 저장, 결제, 거래, 대출, 예치 기능을 브릿징된 USDC 로 제공할 수 있으며, 업그레이드 시 자동으로 네이티브 USDC 로 전환되므로 별도의 자산 스왑 없이 자연스럽게 이동이 이루어집니다.

신뢰성(Reliability)

가동 시간 SLA(Uptime SLAs)

칼데라는 모든 메인넷 배포에 대해 99.99%의 가동 시간 SLA를 제공합니다.

업계 표준 모범 사례 적용

칼데라는 서비스의 신뢰성과 가용성 확보를 위해 업계 표준의 모범 사례를 채택하고 있습니다.

쿠버네티스(Kubernetes) 설정은 고가용성(High Availability) 구조로 설계되어 있어, 서비스 중단을 최소화하고 인프라 복원력을 유지할 수 있도록 구성되어 있습니다. 이러한 표준과 실무를 준수함으로써, 칼데라는 파트너와 사용자 모두에게 안정적이고 견고한 운영 환경을 제공합니다.

칼데라의 모든 인프라는 아마존 웹 서비스(Amazon Web Services, AWS) 상에 구축되어 있으며, 여러 지역에 분산 배치되어 있습니다. 쿠버네티스 설정은 신뢰성을 최우선으로 고려하여 설계되었으며, 시퀀서 장애 발생 시 자동 페일오버, 트래픽 급증 시 자동 확장(Auto-scaling)이 가능하도록 구성되어 있습니다.

L1 RPC 예비 대체 경로(Fallback)

롤업 운영에서 가장 취약한 연결 중 하나는 레이어 1(이더리움 메인넷) 전체 노드와의 RPC 연결입니다. 이 연결이 장시간 끊기면 롤업 기능이 제대로 작동하지 않게 됩니다.

칼데라는 이와 같은 위험을 줄이기 위해 프록시 기반 로드 밸런싱 서비스를 구축하였습니다. 이 프록시는 여러 상위 RPC 제공자들과의 연결을 통합하며, 장애 발생 시 자동으로 트래픽을 재경로합니다. 이 계층은 외부 네트워크의 중단 상황에서도 지속적인 서비스 접근성과 기능성을 유지하는 데 큰 역할을 합니다.

투명한 상태 페이지(Transparent Status Page)

칼데라는 시스템 성능과 가용성에 대한 완전한 투명성을 지향합니다. 모든 메인넷 배포에는 [Betterstack](#) 기반의 상태 페이지가 제공되며, 해당 페이지에서는 각 롤업의 실시간 운영 상태를 확인하고 알림 구독을 통해 지속적으로 정보를 받아볼 수 있습니다. 서비스 중단이 발생할 경우, 칼데라 엔지니어링 팀 전원이 즉시 경고를 수신합니다.

응답 SLA 및 에스컬레이션 절차(Response SLAs and Escalation Procedures)

칼데라는 신속한 대응과 문제 해결을 통해 고신뢰 서비스를 유지하고자 합니다. 칼데라는 사고 및 문제에 대해 신속하게 대응할 수 있도록, 연중무휴 24 시간 대응을 보장하는 서비스 수준 협약(SLA)을 정의하였습니다. 칼데라의 SLA는 예상 응답 시간과 해결 절차를 명시하고 있으며, 우려 사항을 처리하기 위한 명확한 프레임워크를 제공합니다. 또한, 운영 또는 중재 상황에 대비한 에스컬레이션 절차도 마련되어 있어, 중요 이슈가 적절한 주의를 받고 신속하게 해결되도록 보장합니다.

보안(Security)

메인넷 롤업 컨트랙트의 멀티시그 소유 구조

블록체인 컨트랙트, 특히 고객 자금이 관련된 환경에서는 보안이 최우선입니다. 칼데라는 메인넷 롤업 컨트랙트에 대해 멀티시그(Multisig, 다중 서명) 소유 구조를 적용하고 있습니다. 이는 중요한 작업을 수행하려면 여러 명의 승인이 필요하다는 것을 의미하며, 보안에 있어 추가적인 보호 계층을 제공합니다. 멀티시그 체계를 통해, 설령 시스템이 침해당하는 극단적인 상황이 발생하더라도 고객 자금이 안전하게 보호되도록 보장합니다.

검증된 롤업 스택만을 사용

칼데라는 오직 가장 널리 사용되고 입증된 롤업 스택만을 운영합니다. 여기에는 Optimism, Arbitrum, Polygon CDK가 포함되며, 각 스택은 메인넷 상에서 수백만~수십억 달러의 가치를 보호하고 있습니다. 모두 실사용 환경에서 테스트되고 감사된 기술입니다.

프로덕션 인프라 접근에 대한 이중 승인(Dual Authorization)

칼데라의 모든 프로덕션 인프라는 이중 승인 체계(Dual Authorization Scheme) 아래에 보호됩니다. 이 체계는 어떤 개인도 단독으로 인프라에 접근하거나 수정할 수 없도록 강제합니다. 모든 변경은 반드시 두 명 이상의 칼데라 직원의 승인을 필요로 하며, 이를 통해 내부에서 발생할 수 있는 무단 접근이나 악의적 활동의 위험을 대폭 줄일 수 있습니다.