

타이코(Taiko)

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.

Taiko Alethia란 무엇인가?

이더리움은 현재 **비용이 높고 혼잡하다**.

그러나 이더리움의 핵심 원칙인 **검열 저항성(Censorship Resistance)**, **비허가형 접근성(Permissionless Access)**, 견고한 보안성(Robust Security)은 결코 양보할 수 없다.

진정한 확장성 솔루션은 신뢰 가정(trust assumption)이나 중앙화, 혹은 그 밖의 트레이드오프를 도입하지 않고도 이러한 특성을 확장해야 한다.

Taiko Alethia 소개

Taiko Alethia는 이더리움의 근본적 특성을 손상시키지 않으면서 확장성을 제공하기 위해 설계된 **이더리움 등가(Ethereum-equivalent) 비허가형(permissionless) 롤업**이다.

기존 롤업들이 중앙화된 시퀀서(sequencer)에 의존하는 것과 달리, Taiko Alethia는 **시퀀싱(sequencing) 기능을 이더리움 자체에 위임**하여, 블록 순서 결정이 탈중앙화되고 검열에 강하도록 한다.

Taiko Alethia의 특징

- **완전한 이더리움 등가성 (Fully Ethereum-equivalent):**
수정되지 않은 이더리움 실행 레이어를 그대로 실행하므로, 개발자는 스마트 컨트랙트 및 개발 도구를 손쉽게 마이그레이션할 수 있다.
- **중앙화된 시퀀서 부재 (No centralized sequencer):**
이더리움 L1 검증자(Validators)가 탈중앙화된 방식으로 트랜잭션을 순서대로 정렬한다.
- **멀티프루빙 아키텍처 (Multiproving architecture):**
ZK 증명(ZK proofs)과 신뢰 실행 환경(TEE, Trusted Execution Environment) 증명을 모두 지원하여, 단일 증명 방식 롤업보다 훨씬 유연하다.

- **구성 가능한 증명 시스템 (Configurable proof system):**
보안성과 성능 간의 트레이드오프에 따라 **ZK 롤업**, **옵티미스틱 롤업**, 혹은 **하이브리드 형태로** 운영될 수 있다.
- **탈중앙화된 블록 제안 및 검증 (Decentralized proving & proposing):**
비허가형 블록 제안 및 검증(permissionless block proposing and proving) 구조를 채택하여, 화이트리스트된 참여자에 대한 의존성을 제거한다.

Taiko Alethia의 핵심 개념

- **Based Rollup:**
이더리움 L1 검증자(Validators)가 블록을 시퀀싱(sequencing)하는 롤업 구조로, 중앙화된 시퀀서의 필요성을 제거한다.

Taiko Alethia의 작동 방식

Taiko Alethia의 핵심은 이더리움 L1에 배포된 일련의 스마트 컨트랙트 집합으로, 실행 규칙을 강제하고, 증명을 관리하며, 롤업 운영을 지원한다.

- **배치 제안(Proposing Batches):**
이더리움의 시퀀싱 규칙을 따르는 한, 누구나 비허가형(permissionless) 방식으로 트랜잭션 배치를 제안할 수 있다.
- **배치 증명(Proving Batches):**
증명자(Provers)는 제안된 블록의 정확성을 확인하기 위해 **TEE + TEE** 또는 **ZK + TEE** 조합의 유효성 증명(Validity Proofs)을 제출한다.

Taiko Alethia의 거버넌스 및 조직 구조

탈중앙화 조직(Decentralized Organizations)

Taiko Alethia는 DAO, 커뮤니티 검증자(Validators), 탈중앙화 인센티브 시스템을 통해 운영되는 완전한 탈중앙화 프로토콜이다.

조직(Organization)	기능(Functionality)
Taiko Community	Discord, Twitter, Forum 등에서 운영되는 공개 커뮤니티 및 토론 공간
Taiko Labs	Taiko Alethia 프로토콜을 지원하는 연구 및 개발 기관
Taiko Treasury	L2 혼잡도(congestion) 수수료를 수집하고, 개발 자금을 배분
Taiko DAO	스마트 컨트랙트 업그레이드, 네트워크 파라미터, 프로토콜 자금을 관리하는 거버넌스 본체
Taiko Foundation	기술 개발, 파트너십, 생태계 확장을 위한 재단
Taiko Security Council (진행 중)	핵심 프로토콜 보안 및 긴급 네트워크 의사결정을 담당

Taiko Labs가 운영하는 인프라

Taiko Labs는 비핵심(Non-critical) 및 핵심(Critical) 인프라를 모두 운영하지만, Taiko의 **오픈소스(Open-source)** 및 **비허가형(Permissionless)** 특성 덕분에 누구나 이러한 구성 요소를 실행할 수 있다.

비핵심 인프라 (Non-Critical Infrastructure)

이 서비스들은 오픈소스로 제공되며, 누구나 이를 복제하거나 개선할 수 있다.

프론트엔드 (Frontends)

- **Bridge UI** → L1과 L2 간 자산 전송을 위한 인터페이스
- **Network status** → Taiko Alethia 네트워크의 실시간 상태 업데이트 제공
- **Homepage** → 공식 웹사이트 및 생태계 포털
- **Geth fork diff** → 이더리움 등가성(Ethereum-equivalence)을 위한 포크 비교 도구

백엔드 (Backends)

- **Event Indexer** → 롤업 트랜잭션 및 이벤트를 추적
- **Bridge Relay** → 최소 신뢰(Trust-minimized) 기반의 브릿징을 지원

- Taiko Alethia, Taiko Hekla 및 Taiko Hoodi P2P 부트스트래핑 노드 → 탈중앙화 피어들이 네트워크와 동기화하도록 지원 (각 네트워크별 .env.sample 파일에 구성 정보 포함)
- Taiko Alethia Taiko Labs의 제안자(Proposers) 및 증명자(Provers)

Taiko Alethia가 기존 롤업보다 우수한 이유

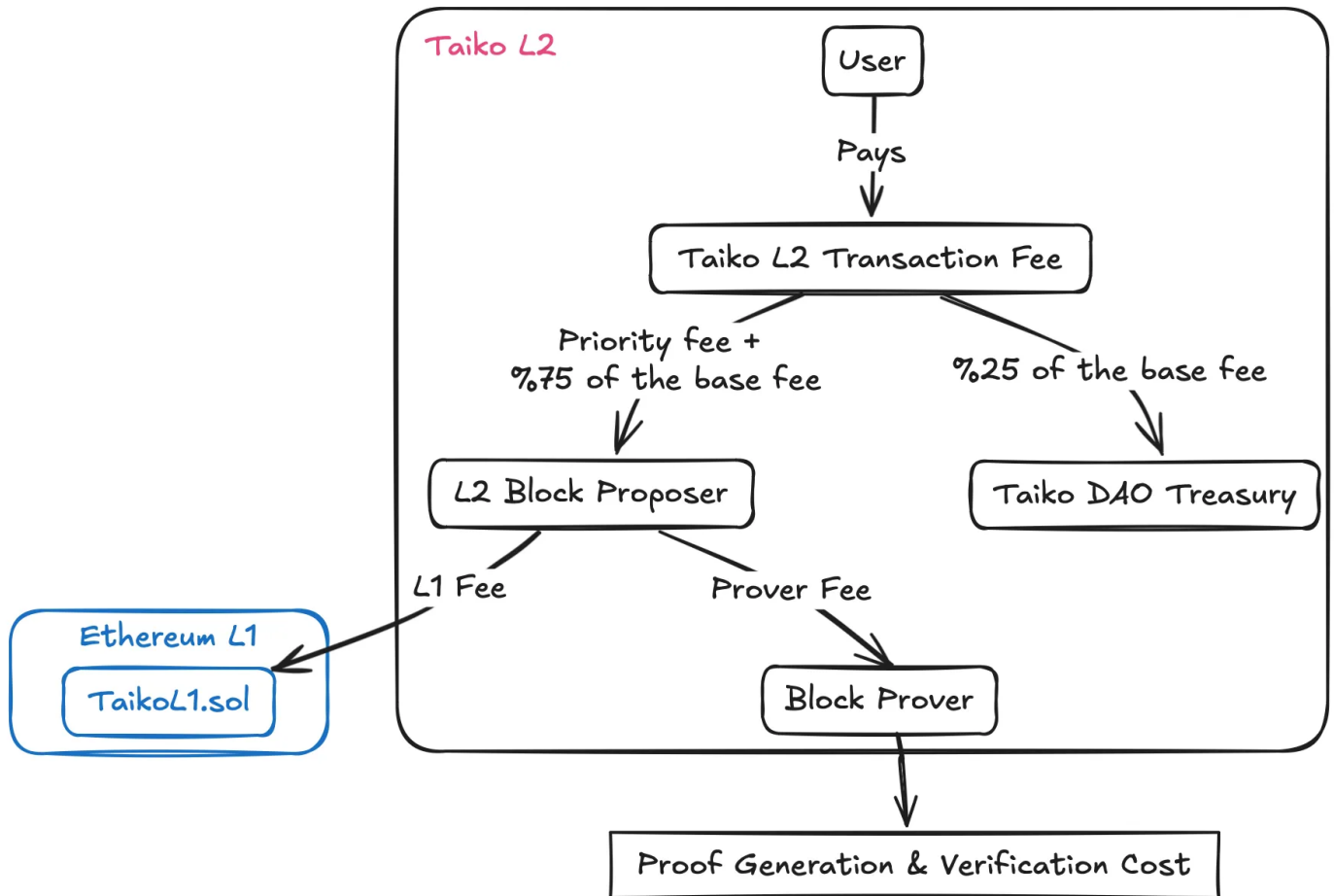
항목(Feature)	기존 롤업 (Traditional Rollups)	Taiko Alethia
시퀀싱(Sequencing)	중앙화(단일 시퀀서 사용)	탈중앙화(L1 검증자가 시퀀싱 수행)
증명 시스템(Proof System)	단일 증명 유형(ZK 또는 Optimistic)	다중 증명 구조(TEE + TEE 또는 TEE + ZK)
검열 저항성(Censorship Resistance)	운영자가 트랜잭션을 검열할 수 있음	비허가형 트랜잭션 포함 (Permissionless inclusion)
스마트 컨트랙트 등가성(Smart Contract Equivalence)	수정된 이더리움 (Geth 수정 필요)	100% 이더리움 등가 (Ethereum-equivalent)
탈중앙화(Decentralization)	멀티시그 거버넌스에 의존	DAO 중심의 개방형 참여(Open participation) 거버넌스

경제 구조 (Economics)

Taiko Alethia의 **Based Rollup 설계**와 **Multiproving 아키텍처**는 고유한 경제적 순환 구조를 형성한다.

이 프로토콜은 블록 제안자(Block Proposer)와 블록 증명자(Block Prover) 모두에게 공정한 보상을 제공하며, **Taiko DAO Treasury**를 통해 네트워크의 지속 가능한 운영을 보장한다.

아래 다이어그램은 Taiko Alethia의 **트랜잭션 수수료 흐름(Transaction Fee Flow)**을 나타낸다:



트랜잭션 수수료 및 배분 구조

Taiko L2에서 사용자가 트랜잭션을 제출하면, 수수료는 다음 두 가지로 구성된다:

1. 우선 수수료(Priority Fee) → L2 블록 제안자에게 직접 전송된다.
2. 기본 수수료(Base Fee) → L2 블록 제안자와 Taiko DAO Treasury 간에 분배된다.

수수료 구조 (Fee Breakdown)

구성 요소(Component)	수취자(Recipient)	용도(Purpose)
우선 수수료(Priority Fee)	L2 블록 제안자(Block Proposer)	트랜잭션의 신속한 포함을 유도하기 위한 인센티브 제공
기본 수수료의 75%(75% of Base Fee)	L2 블록 제안자(Block Proposer)	블록 제안에 대한 보상
기본 수수료의 25%(25% of Base Fee)	Taiko DAO Treasury	생태계 개발 및 네트워크 지속 가능성 자금 지원

L2 블록 제안자의 역할 및 비용 (Block Proposer Responsibilities & Costs)

L2 블록 제안자(L2 Block Proposer)의 주요 역할은 다음과 같다:

- 트랜잭션을 집계(Aggregate)하고 순서를 정렬하여 L2 블록으로 구성한다.
- `TaikoInbox.sol`의 `proposeBlock` 함수를 호출하여 L2 블록을 이더리움 L1에 제출한다.

L2 블록 제안자가 부담하는 비용

1. L1 수수료(L1 Fee) → L2 블록 제안 시 `TaikoInbox.sol`을 통해 이더리움 L1에 지불.
2. 증명자 보수(Prover Fee) → 블록의 정확성을 검증하는 블록 증명자에게 지급.

블록 증명자의 역할 및 비용 (Block Prover Responsibilities & Costs)

블록 증명자(Block Prover)의 주요 역할은 다음과 같다:

- 제안된 L2 블록의 정확성을 검증하기 위한 암호학적 증명(Cryptographic Proofs)을 생성한다.
- 생성된 증명을 이더리움 L1에 제출하여 검증을 받는다.

블록 증명자가 부담하는 비용

1. 연산 비용(Computation Costs) → 증명 생성에는 막대한 계산 자원이 필요하다.
2. 가스 비용(Gas Costs) → 증명을 이더리움 L1에 게시할 때 가스 수수료가 발생한다.

네트워크 지속 가능성 및 Taiko DAO Treasury

- **Taiko DAO Treasury**는 기본 수수료(Base Fee)의 **25%**를 수령하여 프로토콜의 장기적 지속 가능성을 보장한다.
- DAO는 이 자금을 **개발, 연구, 보안, 거버넌스** 지원에 사용한다.
- Taiko Alethia에서 요구되는 **라이브니스 본드(Liveness Bond)** 관련 정보는 네트워크 구성(Network Configuration) 페이지에서 확인할 수 있다.

Taiko Gwyneth란 무엇인가?

Based Rollup은 롤업을 실행하는 데 있어 가장 효과적이고 탈중앙화되어 있으며, 이더리움과의 정렬성이 가장 높은 방식으로 평가된다.

시퀀싱(Sequencing) 작업을 L1에 위임함으로써, Based Rollup은 L1의 **탈중앙화(Decentralization)**, **단순성(Simplicity)**, **생존성(Liveness)** 등을 그대로 상속받는다.

그렇다면, 여기에 이더리움 L1의 네이티브 dApp 확장성(Sharding)을 결합해, Based Rollup의 이점을 극대화할 수 있다면 어떨까?

Taiko Gwyneth 소개

Taiko Gwyneth는 수평적(Ethereum-horizontal) 확장 솔루션이며, 수직적(Vertical) 확장과는 반대되는 개념이다.

Gwyneth는 여러 개의 동일한 이더리움 등가(Ethereum-equivalent) L2 네트워크로 구성된 시스템으로,

기반 시퀀싱(Based Sequencing), 실시간 증명(Real-time Proving), 부스터(Booster) 기능을 결합하여 동기적 합성(Synchronously Composable) 네트워크를 구현한다.

이를 통해 Gwyneth는 다중 롤업 간 유동성 분절(Liquidity Fragmentation) 문제를 해결하면서, 이더리움을 확장하는 균일한 실행 환경(Uniform Execution Environment)을 제공한다.

Taiko Gwyneth의 특징

- **이더리움 등가성(Ethereum-equivalent):**
각 Taiko Gwyneth L2는 완전히 이더리움 등가를 유지하며, 기존 dApp 및 개발 도구와 완벽히 호환된다.
- **Based 구조:**

L1 검증자(Validators)가 시퀀싱을 담당함으로써, **최대 수준의 탈중앙화, L1과의 경제적 정렬(Economic Alignment), 강력한 검열 저항성(Censorship Resistance)**을 보장한다.

- **확장성(Scalable):**
개발자는 네트워크 내에서 필요한 만큼 새로운 롤업을 추가할 수 있으며, 기존 애플리케이션을 방해하지 않고 용량을 확장할 수 있다.
- **비허가형(Permissionless):**
증명 유형에 결함이 있음을 입증할 수 있는 경우, **검증자 레지스트리 스마트 컨트랙트(verifier registry smart contract)** 내에서 누구나 비허가형으로 해당 증명을 비활성화할 수 있다.
- **매끄러운 사용자 경험(Seamless UX):**
사용자는 L1과 L2를 하나의 통합된 시스템으로 경험하며, 체인 간 동일한 주소를 유지한다.
- **안전한 실행(Secure Execution):**
사전 확인(Preconfirmation)과 실시간 다중 증명(Real-time Multi-proving)을 통해 신뢰성 높은 실행 환경을 보장한다.

Taiko Gwyneth의 핵심 개념

- **Based Booster Rollup:**
L1 상태(State)를 활용하며, **이더리움의 실행 샤드(Execution Shard)**로 기능하는 L2 롤업을 의미한다.

Taiko Gwyneth의 작동 방식

Taiko Gwyneth 네트워크는 이론적으로 무한한 처리량(Throughput)을 가지며, 사용자에게는 단일 통합 체인처럼 작동한다.

새로운 L2가 추가될 때마다 병렬 처리 및 저장 용량이 확장되며, 이론상 한계가 없다.

이 확장성을 달성하기 위해, Taiko Gwyneth는 다음의 주요 개념을 활용한다:

동기적 합성(Synchronous Composability)

모든 **Taiko Gwyneth L2**는 서로에게 **동기적(Synchronous)**으로 접근할 수 있다.

또한 L1 제안자(Proposer)의 지원을 통해 L1에도 동기적으로 접근할 수 있다.

이 맥락에서 ‘접근(access)’이란, 서로 다른 체인이 **하나의 동일한 체인처럼 상태(State)**를 읽고 쓸 수 있음을 의미한다.

이 기능을 구현하기 위해, Taiko Gwyneth는 **XCALLOPTIONS**라는 새로운 **프리컴파일(Precompile)**을 도입하여 **크로스 롤업 실행(Cross-Rollup Execution)**을 매끄럽게 수행할 수 있도록 한다.

XCALLOPTIONS 컨텍스트

```
XCALLOPTIONS(version: uint16, chainID: uint, sandbox: bool, txOrigin: address, msgSender: address, blockHash: bytes32, proof: bytes)
```

이 프리컴파일은 컨트랙트가 다음 호출(CALL)에서 **대상 체인(Target Chain)**을 지정할 수 있도록 하여, 롤업 간 **직접적인 상태 접근(Direct State Access)**을 가능하게 한다.

이는 해당 체인의 전체 실행 환경(Execution Environment)을 — basefee를 포함하여 — 완벽히 에뮬레이션한다.

증명(Proof)은 체인 간 상태를 수정할 때 **정확성을 보장**하기 위해 사용되며, 각 L2가 **자체적인 독립 실행 상태(Independent Execution State)**를 유지할 수 있도록 한다.

부스터 기능(Booster Functionality)

Taiko Gwyneth는 L1 확장을 가능하게 하기 위해 **부스터 롤업(Booster Rollup)** 개념의 일부를 채택하며, 이를 **부스터 기능(Booster Functionality)**이라 부른다.

부스터 기능은 **L1 상태(State)**를 **L2의 네이티브 상태와 동일한 비용으로 접근할 수 있도록** 하는 것을 의미한다.

이를 통해 Taiko Gwyneth는 **이더리움을 전역 상태(Global State)**로 활용하여 대부분의 dApp 데이터를 저장할 수 있다.

이더리움은 설계상 언제나 **체인 간 읽기(Cross-Chain Reading)**가 가능하기 때문이다.

따라서 L1에 존재하는 기존 스마트 컨트랙트에 직접 접근할 수 있으며, 모든 L2에 재배포(Redeployment)할 필요가 없다.

이는 **이더리움을 수평적으로 확장(Horizontal Scaling)**하는 효율적인 방법이며, 동시에 **유동성 및 상태의 분절(Fragmentation)**을 방지하는 추가적인 이점을 제공한다.

실시간 증명(Real-Time Proving)

고처리량(High Throughput)을 유지하기 위해, Taiko Gwyneth는 **다중 증명 유형(Multi-Proof Types)**을 사용한 **실시간 증명(Real-Time Proving)** 구조를 활용한다:

- **TEE 기반 증명자(TEE-Based Provers):**
Intel SGX, AMD SEV, Nitro Enclave 등을 활용한 **하드웨어 기반의 빠른 증명(Fast Hardware-Based Proofs)**
- **AVS 증명자(AVS Provers):**
경제적 인센티브를 통해 정확성을 보장하는 **분산형 증명 시스템(Distributed Attestation System)**
- **ZK 증명(ZK Proofs, 향후 통합 예정):**
현재 실시간 ZK 증명은 기술적으로 불가능하지만, **Taiko Gwyneth는 향후 통합을 위한 설계가** 되

어 있다.

당장은 ZK 증명을 사용해 **다른 증명자가 오류가 있음을 증명함**으로써 프로토콜의 보안을 간접적으로 강화한다.

기반 사전확인(Based Preconfirmations)

Taiko Gwyneth는 **기반 사전확인(Based Preconfirmations)** 기능도 지원한다.

이 기능은 트랜잭션이 L1에서 최종 확정되기 전에 **즉각적으로 실행 및 확인**될 수 있게 하여, 사용자 경험(UX)을 크게 향상시킨다.

요약(Summary)

Taiko Gwyneth는 **보안(Security)**, **탈중앙화(Decentralization)**, **사용자 경험(User Experience)**을 유지하면서 이더리움을 효율적으로 확장하기 위해 설계되었다.

부스터 롤업, 실시간 증명, 사전확인(preconfirmation)을 결합함으로써, 여러 L2 간의 **동기적 실행(Synchronous Execution)**을 가능하게 하고,

매끄럽고 확장 가능한 이더리움 네이티브 롤업 생태계(Ethereum-Native Rollup Ecosystem)를 구축한다.