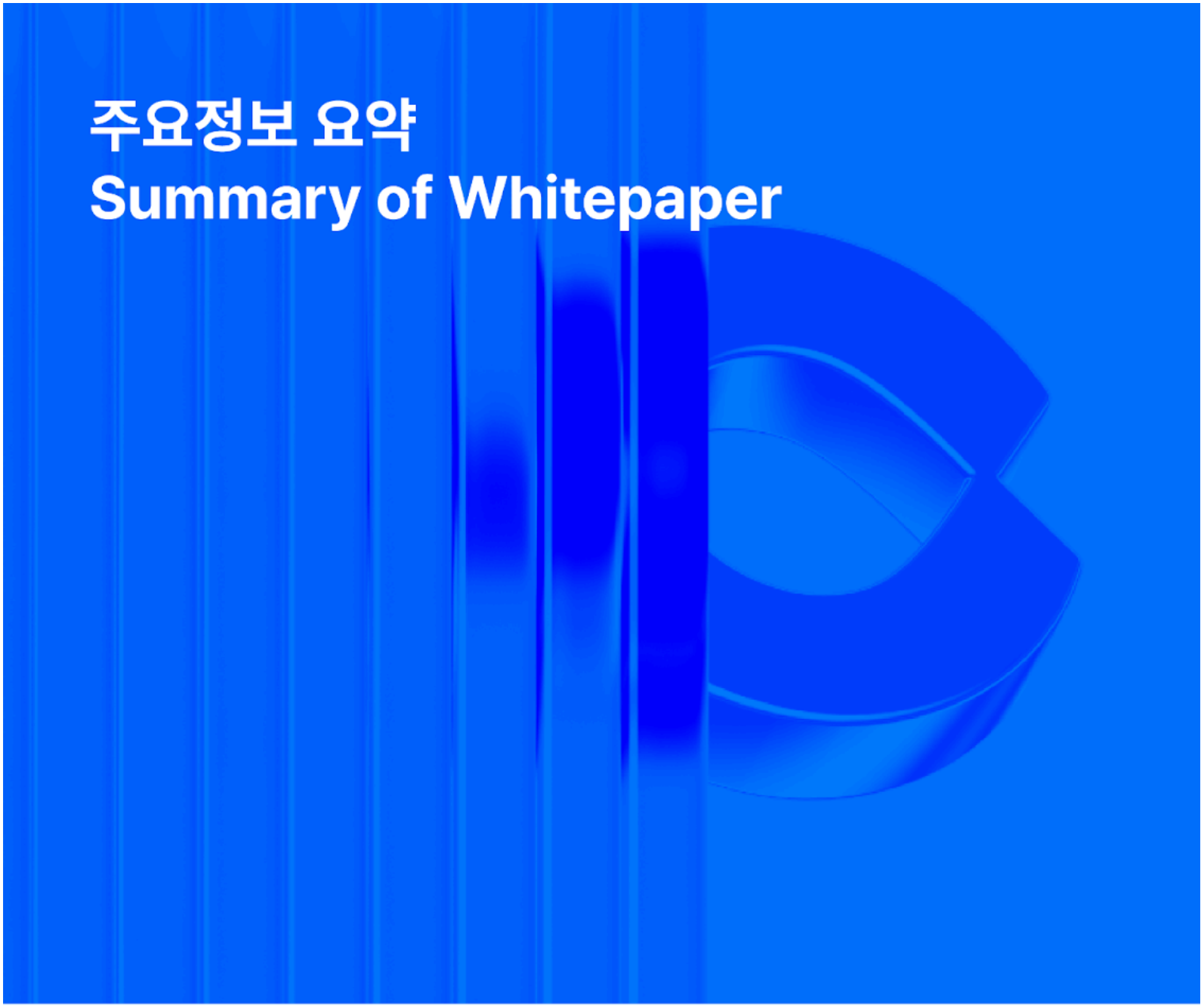
주요정보 요약
Summary of Whitepaper



본 문서는 거래지원 가상자산 백서의 주요 내용을 한글로 설명한 주요정보 요약입니다.
코인원은 거래지원 가상자산의 주요정보 요약을 주기적으로 점검하여 가능한 한 최신 정보를 제공할 예정입니다.

coinone

비트레이어(BTR)

2025.08.25

기본 정보

가상자산 카테고리	유틸리티
거래지원 네트워크	Ethereum
홈페이지	https://www.bitlayer.org/
참고문헌 (백서, Docs 등)	https://docs.bitlayer.org/docs/Learn/Introduction https://static.bitlayer.org/Bitlayer-Technical-Whitepaper.pdf

1. 프로젝트 정보

개요

Bitlayer는 비트코인의 강력한 보안성과 탈중앙화를 유지하면서도 확장성과 프로그래머빌리티를 제공하기 위해 개발된 최초의 비트코인 롤업 솔루션입니다. 비트코인의 기본 레이어를 기반으로 신뢰성과 회복력을 그대로 계승하면서, BitVM 패러다임을 통해 스마트 컨트랙트 기능을 도입하였고, EVM과의 호환성을 통해 이더리움 생태계의 애플리케이션을 쉽게 이전할 수 있도록 설계되었습니다. 이를 통해 단순한 확장 솔루션을 넘어, 비트코인의 활용 범위를 DeFi, 신뢰 없는 시스템, 확장 인프라까지 넓히고 있습니다.

비트코인의 한계와 Bitlayer의 해결 방향

- 낮은 처리량과 높은 수수료: 보안과 탈중앙화를 우선한 구조로 인해 트랜잭션 속도와 비용에서 제약이 큼
- 스마트 컨트랙트 부재: 복잡한 애플리케이션을 직접 구현하기 어려움
- 신뢰 없는 브리지 부재: 타 블록체인과 안전하게 연동할 수 있는 네이티브 수단이 없음

Bitlayer는 이를 해결하기 위해 비트코인 수준의 보안 계승, 탈중앙화된 BTC 브리지, 튜링 완전한 프로그래머빌리티, 확장 가능한 높은 처리량을 목표로 합니다.

현재 진행 상황

- Bitlayer PoS(Mainnet-V1): 2024년 4월 초 정식 런칭되어 운영 중이며, 개발자와 사용자가 기능을 시험할 수 있는 테스트넷도 제공됨.
- Bitlayer Rollup(Mainnet-V2): 차세대 업그레이드가 개발 중으로, BTC 자산을 안전하게 연결하는 BitVM Bridge 테스트넷이 공개됨. 곧 롤업 아키텍처를 지원하는 방향으로 확장될 예정.

Bitlayer의 비전

Bitlayer는 단순한 확장성을 넘어, 비트코인 기반 금융 애플리케이션(BTCFi)을 위한 최고의 인프라를 제공하는 것을 핵심 목표로 삼고 있습니다. 궁극적으로 비트코인을 안전하면서도 확장 가능한 플랫폼으로 발전시켜 새로운 탈중앙화 금융과 애플리케이션 생태계를 열고자 합니다.

Bitlayer Network Architecture

Bitlayer는 이중 레벨 구조를 기반으로 합니다.

- PoS 합의 레이어: 검증인(Validator)이 빠른 블록 생성과 트랜잭션 시퀀싱을 담당, 고속·EVM 호환 환경을 제공
- 롤업 레이어: L2 체인의 상태를 주기적으로 비트코인 블록체인에 정산·앵커링하여 보안과 데이터 가용성을 확보

즉, Bitlayer는 계산과 확장을 담당하는 L2로 작동하고, 비트코인은 보안과 최종 정산을 담당하는 L1로 작동합니다.

네트워크 참여자와 역할

- 검증인(Validators): PoS 합의의 핵심으로, L2 블록을 생산·검증합니다. BTR 토큰을 스테이킹해야 하며, 위임받은 지분 포함 총 스테이크 규모에 따라 영향력이 결정됩니다.
- 롤업 오퍼레이터(Rollup Operator): 검증인 중 하나가 순환 방식으로 맡는 특수 역할입니다. L2 상태 전이를 묶어 배치(batch)로 만들고, 암호학적 증명을 생성해 비트코인 L1에 제출합니다. 이를 위해 상당량의 BTC를 L1에 담보로 예치해야 하며, 주기적 순환으로 검열·중앙화를 방지합니다.
- 풀 노드(Full Nodes): Bitlayer 블록체인의 전체 사본을 유지하며 독립적으로 모든 거래와 상태 전이를 검증합니다. 검증인을 신뢰하지 않고도 네트워크 규칙 준수와 투명성을 보장합니다.

이중 레벨의 거래 최종성

- 소프트 파이널리티 (Soft Finality): 트랜잭션은 Bitlayer PoS 합의에서 블록이 확정되면 1초 미만에 빠른 확정성을 가집니다. 검증인 지분 경제적 담보가 보안 근거입니다.
- 하드 파이널리티 (Hard Finality): L2 상태가 비트코인 블록체인에 정산·최종 확정되면 최고 수준의 보안이 보장됩니다. 낙관적 롤업의 챌린지 기간 때문에 약 7일이 소요됩니다. 단 1명의 정직한 참여자가 도전을 제기하면 보안이 유지되므로 비트코인 자체 보안에 준합니다.

만약 챌린지 성공으로 L2 상태와 L1 정산 상태가 불일치하게 되면, 프로토콜은 작동을 멈추며, 이후 복구는 사용자 자산의 안전성을 위해 '사회적 합의(social consensus)'에 의해 진행됩니다.

Bitlayer Rollup(V2)

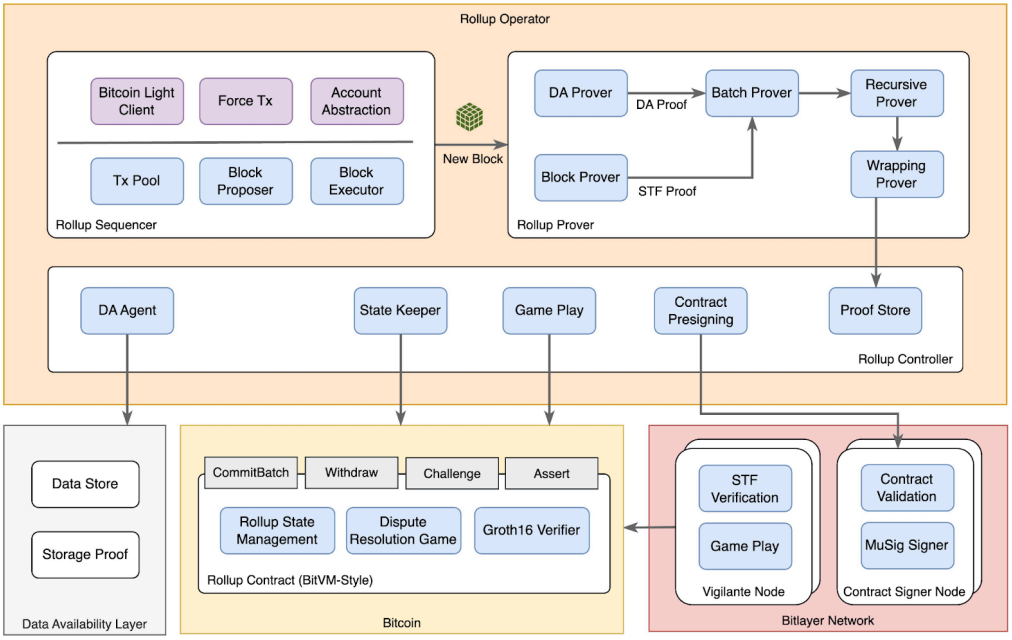
Bitlayer V2는 비트코인 생태계에서 최초의 비트코인 네이티브 롤업을 지향하는 차세대 레이어 2 업그레이드입니다. 기존 사이드체인 방식을 대체하며, 비트코인의 강력한 보안을 그대로 계승하면서 높은 처리량·낮은 수수료·스마트 컨트랙트 기능을 제공해 비트코인의 활용 범위를 크게 확장합니다.

기술적 특징과 차별점

Bitlayer V2는 이더리움 롤업처럼 레이어 2 트랜잭션을 모아 상태 변화를 처리한 뒤, 이를 비트코인 레이어 1에 증명과 함께 제출합니다. 다만 비트코인의 스크립트 언어가 제한적이어서 영지식 밸리데이터를 직접 실행하기 어렵다는 한계가 있습니다. 이를 해결하기 위해 BitVM2 기반의 하이브리드 증명 방식을 도입했습니다. 즉, 기본적으로 증명을 유효하다고 간주하되, 문제 제기가 있으면 7일간의 챌린지 윈도우에서 분쟁을 통해 검증이 이뤄집니다. 이 과정에서 잘못된 증명을 한 운영자는 보증금을 잃게 되고, 정직한 참여자가 보상을 받는 구조로 신뢰성을 확보합니다.

핵심 기능

- EVM 호환성: 기존 이더리움 애플리케이션을 수정 없이 실행 가능
- 신뢰 최소화된 BTC 브리지: BitVM Bridge를 통한 안전한 비트코인 크로스체인 전송
- 비트코인 수준의 보안: 사기 증명 메커니즘으로 레이어 1에서 상태 전이를 검증
- 유연한 데이터 가용성: 비트코인 네이티브 또는 외부 솔루션 선택 가능



출처 : Bitlayer Docs

Bitlayer 롤업은 크게 네 가지 구성 요소로 이루어져 있습니다.

1. 롤업 오퍼레이터(Rollup Operator)
   오퍼레이터는 L2 트랜잭션을 처리하고, L2 블록과 배치를 제안·증명한 뒤 이를 비트코인에 제출합니다. 현재는 단일 오퍼레이터만 지원됩니다.
2. 데이터 가용성(DA) 레이어
   오퍼레이터는 L2 배치를 DA 레이어에 제출해 트랜잭션 데이터가 항상 이용 가능하도록 합니다. 만약 검열이 발생하면 사용자는 강제 트랜잭션을 DA 레이어로 직접 전송해 이를 우회할 수 있습니다.
3. 비트코인 컨트랙트
   비트코인 위에 BitVM 방식의 재귀 스마트 컨트랙트 형태로 배포되며, 제출된 증명을 통해 L2 상태 전이의 유효성을 검증합니다.
4. 롤업 네트워크
   네트워크는 여러 노드로 구성됩니다.
   - 오퍼레이터 노드: 활성 오퍼레이터 1개와 예비 오퍼레이터 여러 개로 구성
   - 어테스터 노드: 롤업 컨트랙트 배포 및 상호작용 담당
   - 워처 노드: 네트워크를 모니터링하며 악의적인 오퍼레이터가 잘못된 상태 전이를 제출하면 이를 감지해 도전

롤업 오퍼레이터의 세 가지 역할

오퍼레이터는 다시 세 가지 역할로 구분됩니다.

- 롤업 시퀀서(Sequencer)
  L2 트랜잭션을 수신해 블록을 제안·실행하고, 블록의 유효성을 증명합니다. 이후 블록과 증명을 모아 L2 배치와 배치 증명을 생성합니다.
- 롤업 프로버(Prover)
  개별 블록의 유효성을 증명하고, 블록 증명과 DA 증명을 통합해 하나의 배치 증명을 만듭니다. 이를 다시 Groth16과 같은 방식으로 압축해 효율적으로 검증할 수 있게 합니다.
- 롤업 컨트롤러(Controller)
  전체 롤업 파이프라인을 관리하며, L1 컨트랙트와 상호작용해 L2 상태 전이를 검증하고 최종 확정을 달성합니다.

Technologies - Overview

Bitlayer 리서치 팀은 비트코인의 한계를 뛰어넘고, 더 다양한 활용을 가능하게 하기 위한 기술 개발에 집중하고 있습니다. 목표는 비트코인을 보다 다재다능하고 확장 가능하며 효율적인 플랫폼으로 발전시키는 것입니다.

현재 연구 중인 핵심 분야

1. 비트코인 위 스마트 컨트랙트
   비트코인은 기본적으로 복잡한 스마트 컨트랙트를 지원하지 않지만, Bitlayer는 이 문제를 해결하고자 합니다.
   - 탈중앙 브리지: 비트코인과 다른 블록체인을 연결해 상호운용성을 확보
   - 확장 가능한 롤업: 오프체인으로 트랜잭션을 처리해 처리량은 높이고 수수료는 낮추면서 보안성은 유지
   - DeFi, 에스크로 등 다양한 신뢰 없는 애플리케이션 구현
2. 제로지식 증명(ZKP) 검증
   ZKP는 정보 자체를 공개하지 않고도 사실을 증명할 수 있는 암호학적 기법입니다. 이를 비트코인 스크립트에 통합하면 레이어 2 확장과 프라이버시 강화에 혁신적 전환점을 마련할 수 있습니다.
3. L1 검증 프로토콜
   비트코인 기본 레이어(L1) 위에서 직접 동작하는 새로운 프로토콜을 개발 중입니다. 이를 통해 오프체인 연산을 안전하게 검증하여 더 복잡한 애플리케이션과 확장 솔루션이 가능해집니다.
4. 고성능 L2 트랜잭션 실행
   비트코인 기반 레이어 2 위에서 초고속 트랜잭션 처리를 가능하게 하는 기술을 연구하고 있습니다.

주요 연구 성과

- BitVM 스타일 스마트 컨트랙트
  - 비트코인에 적합한 스마트 컨트랙트 추상화
  - 신뢰 최소화 BTC 브리지 스마트 컨트랙트
  - 롤업용 재귀적 상태 전이 검증 스마트 컨트랙트
- 사기 증명(Fraud Proofs)
  - 비트코인에 특화된 사기 증명 모델링
  - BTC 브리지와 롤업용 프레임워크 구축
  - 실제 구현 가능한 사기 증명 방식 제안
- Bitlayer 증명 시스템
  - Groth16: 스크립트 최적화 및 BitVM 프로젝트에 기여
  - TapSTARK: STARK와 Taptree를 결합한 하이브리드 증명 시스템,

비트코인 스크립트의 머클 증명 한계를 보완
    - BF-STARK: 차세대 STARK 시스템, 향후 비트코인 업그레이드 전제
- 암호학
    - 원자적 스왑을 위한 Threshold Adapter Signatures 연구

Technologies - BitVM Smart Contract

BitVM 개요

비트코인은 기본적으로 스마트 컨트랙트를 지원하지 않지만, BitVM은 이를 모방해 구현할 수 있는 혁신적인 방식을 제시합니다. Robin Linus가 제안한 BitVM은 비트코인 생태계에 범용 연산과 스마트 컨트랙트 개념을 도입한 시도이며, 현재는 BitVM2로 발전해 보다 탈중앙적이고 개방적인 구조를 제공합니다. Bitlayer 역시 BitVM 연합의 핵심 멤버로, 지속적인 기여를 하고 있습니다.

BitVM 스마트 컨트랙트의 개념

BitVM 스마트 컨트랙트는 비트코인에서 이미 쓰이는 '해시 시간 잠금 계약(HTLC)'에서 영감을 얻었지만, 훨씬 복잡한 형태로 발전했습니다.

- 계약은 '사전에 서명된 거래 그래프(transaction graph)'로 표현되며, 이 그래프가 스마트 컨트랙트의 '소스 코드' 역할을 합니다.
- 모든 참여자가 해당 그래프를 사전 검토·서명하면, 이후에는 수정 불가능한 불변 계약이 됩니다.
- 이 과정에서 '검증 위원회(attesting committee)'가 멀티시그(multisig)를 이용해 그래프의 무결성을 보장하며, 서명 후 개인키를 삭제해 추가 변조 가능성을 원천 차단합니다.

핵심 설계 요소

1. 상태 전이 관리 (Finite State Machine)
   비트코인에는 상태 관리 기능이 없기 때문에, BitVM은 '커넥터 출력(connector outputs)'이라는 특수 UTXO를 활용해 상태 전이를 제어합니다. 이를 통해 특정 경로가 사용되면 다른 경로는 자동 무효화되며, 타임락을 활용해 실행 순서를 제어할 수 있습니다.
2. 동적 요소 처리 (Unknown Data & Addresses)
    - Commit-and-Reveal: 미리 알 수 없는 서명 데이터(witness data)는 암호학적 커밋과 공개(reveal) 방식을 통해 처리합니다.
    - SIGHASH 플래그: 수신 주소가 미리 확정되지 않은 경우, 일부 트랜잭션만 서명하고 나머지는 나중에 지정할 수 있도록 유연성을 제공합니다.

BitVM 스마트 컨트랙트 생성 과정

1. 거래 그래프 설계: 스마트 컨트랙트의 동작을 나타내는 트랜잭션 네트워크를 설계
2. 사전 서명: 위원회가 멀티시그로 그래프를 검토·승인
3. 공개 배포: 모든 참여자가 동일하고 변조 불가능한 계약을 공유

보안 모델과 신뢰 스펙트럼

BitVM은 신뢰 수준에 따라 다양한 모델을 구현할 수 있습니다.

- Trustless: 비트코인·이더리움처럼 완전히 암호학과 네트워크 탈중앙성에만 의존
- Trusted: 소수 중앙 주체에 의존
- Hybrid:
    - Honest Majority: 다수의 정직한 참여자 가정
    - Honest Minority: 소수만 정직해도 유지 가능
    - Honest One: 단 한 명의 정직한 참여자만 있어도 시스템이 안전

BitVM은 이 스펙트럼 어디에도 적용될 수 있으며, 브리지는 '정직한 다수' 모델, 롤업은 '정직한 한 명' 모델을 활용할 수 있습니다.

재귀적 증명

비트코인 재귀적 정산 프로토콜을 롤업에 적용했습니다. 우리는 BitVM 기반의 재귀적 프레임워크를 활용하여 레이어 2 상태 전이의 연속적인 클레임 체인을 비트코인에서 정산할 수 있는 최초의 롤업 프로토콜을 설계하고 공식화했습니다. 이 프로토콜은 L2의 유효성을 L1에 직접 연결함으로써 보안을 제공합니다.

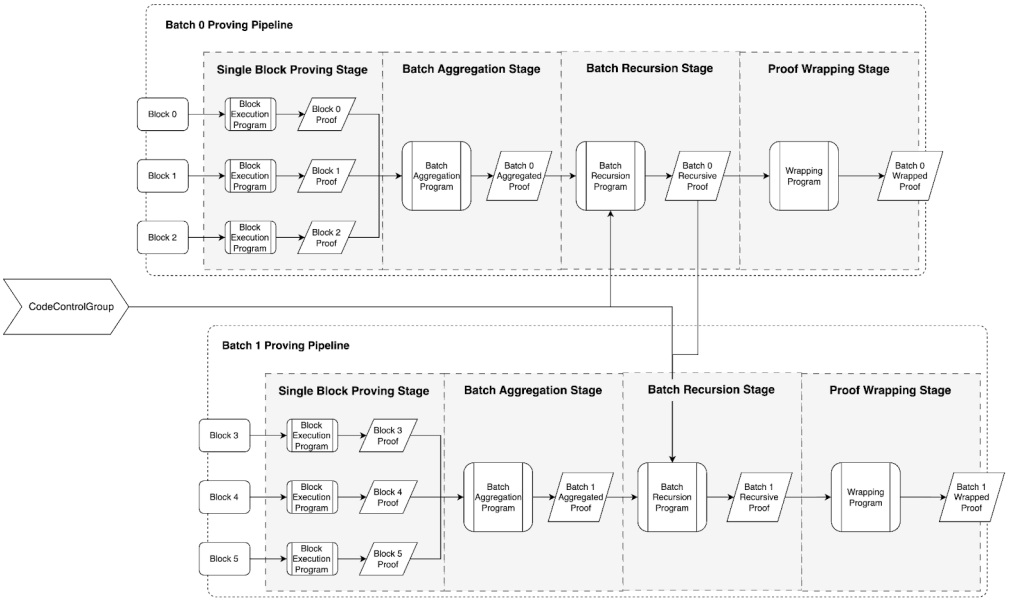
또한, 브리지와 롤업의 시너지적 통합을 구현했습니다. BitVM 브리지 아키텍처에서 영감을 얻어 안전한 자산 브리지를 설계했으며, 이를 롤업 프로토콜과 깊이 통합함으로써 자산 보안과 롤업의 유효성이 단일 신뢰 모델에 의해 관리되도록 했습니다. 이로써 원활하고 안전한 자산 전송이 가능합니다.

정산 프로토콜은 단일하고 거대한 컨트랙트가 아니라, 사전 서명된 비트코인 트랜잭션들의 복잡한 그래프 형태로 구현된 BitVM 스타일 스마트 컨트랙트로 구성됩니다. 참여자들은 이 트랜잭션 그래프를 공동으로 사전 서명해야 하며, 미리 정의된 경로에 따라서만 상호작용할 수 있습니다. 기존의 BitVM 프로토콜이 외부 체인과 비트코인 사이의 사건을 정산하는 브리징 목적에 초점을 맞췄다면, Bitlayer의 프로토콜은 훨씬 더 정교합니다. Bitlayer는 레이어 2 상태 변화 하나하나를 불연속적이지 않고 연속적으로 연결된 클레임으로 정산해야 하며, 이 체인이 끊기지 않고 이어지도록 보장해야 합니다.

이 프로토콜은 재귀적 구조로 이해할 수 있습니다. 먼저 단일 상태 클레임을 정산하는 서브 프로토콜을 정의하고, 그 후 이 단일 클레임 검증 메커니즘을 재귀적으로 확장하여 연속된 상태 클레임의 체인 전체를 정산합니다. 이 두 가지를 결합함으로써, 우리는 Bitlayer 네트워크의 상태를 비트코인 위에서 정산할 수 있는 완전한 롤업 프로토콜을 구축합니다.

또한, 이 프로토콜의 증명 파이프라인은 네 단계로 구성된 순차적 구조입니다. 각 블록에는 고유한 번호가 부여되며, 이는 코드 컨트롤 그룹 내에서 검증을 위한 인덱스 역할을 합니다. 블록들은 배치(batch) 단위로 묶여 집계되며, 배치 기준은 블록 개수나 시간 등 시스템 파라미터로 정의됩니다. 전체 타임라인은 에포크(Epoch) 단위로 조직되어 시스템 전체 재구성을 관리합니다.

이 네 단계는 '단일 블록 증명, 배치 집계, 배치 재귀, 증명 압축(wrapping)'으로 이루어집니다. 이 구조는 중첩된 파이프라인처럼 작동합니다. 각 배치 내에서는 증명이 단계적으로 이어지며, 더 상위 레벨 파이프라인은 재귀 단계를 통해 연속된 배치들을 서로 연결합니다. 각 단계는 특정 입력을 받아 zkVM 내에서 계산을 수행하고, 산출물을 다음 단계에 전달하거나 최종 압축 증명에 기여합니다. 이러한 재귀적 아키텍처 덕분에 증명을 효율적으로 집계하고 압축할 수 있어, 시스템의 확장성을 크게 향상시킬 수 있습니다.



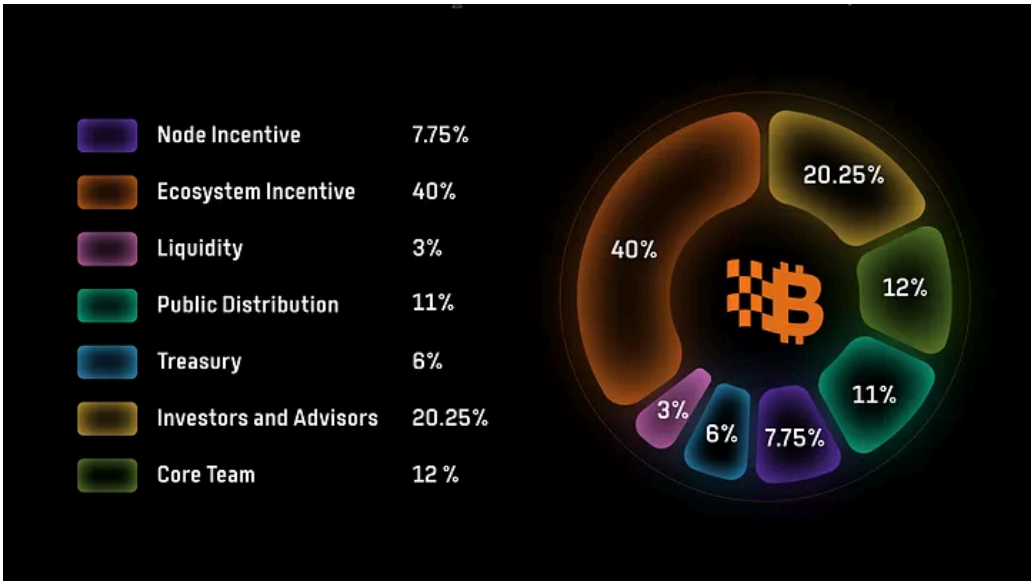
출처 : Bitlayer Docs

2. 토큰 이코노미

가상자산 소개

BTR은 비트레이어 생태계의 유틸리티 토큰으로, 비트레이어의 거버넌스 참여, 블록 생성 및 검증에 참여하기 위한 스테이킹 참여와 이에 대한 보상으로 사용됩니다.

발행량 및 유통량계획



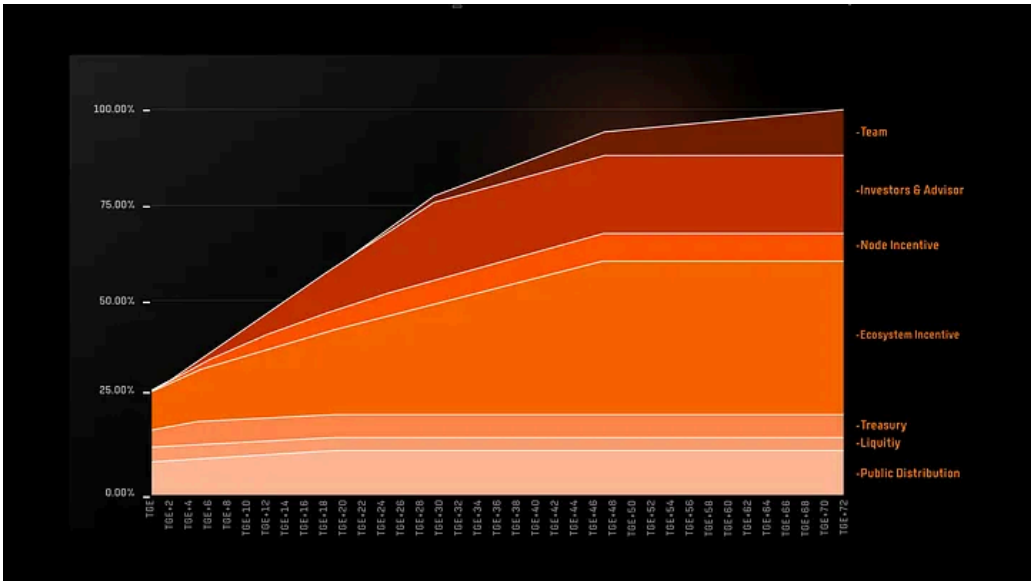
출처 : Bitlayer Medium

BTR은 초기에 10억 개가 발행됩니다.

Ecosystem Incentive가 전체의 40%를 차지하며, 이는 TGE 시점에 25%가 유통된 뒤

나머지는 48개월에 걸쳐 점진적으로 베스팅됩니다. Investors & Advisor 몫은 20.25%로, 6개월의 클리프 기간 이후 24개월 동안 분배됩니다. Team 할당분은 12%이며, 24개월이라는 긴 클리프 기간 이후 48개월에 걸쳐 베스팅됩니다.

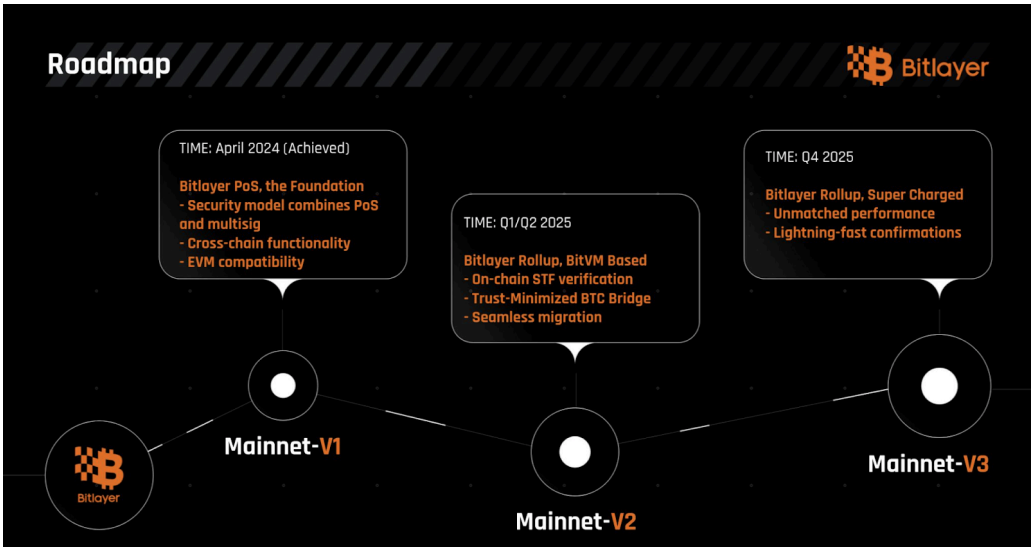
Public Distribution 항목은 11%로, TGE 시점에 해당 항목의 79% 유통, 이후 1개월의 클리프를 거친 뒤 18개월 동안 나머지가 분배됩니다. Node Incentive는 7.75%로, 첫 해에 총 공급량의 3.875%가 유통된 뒤 매년 절반씩 줄어드는 halving 방식으로 배분됩니다. 트레저리는 6%로, TGE 시점에 75%가 유통되고 나머지는 5개월에 걸쳐 베스팅됩니다. 마지막으로 유동성 공급 목적의 3%는 TGE 시점에 전량 유통됩니다.



출처 : Bitlayer Medium

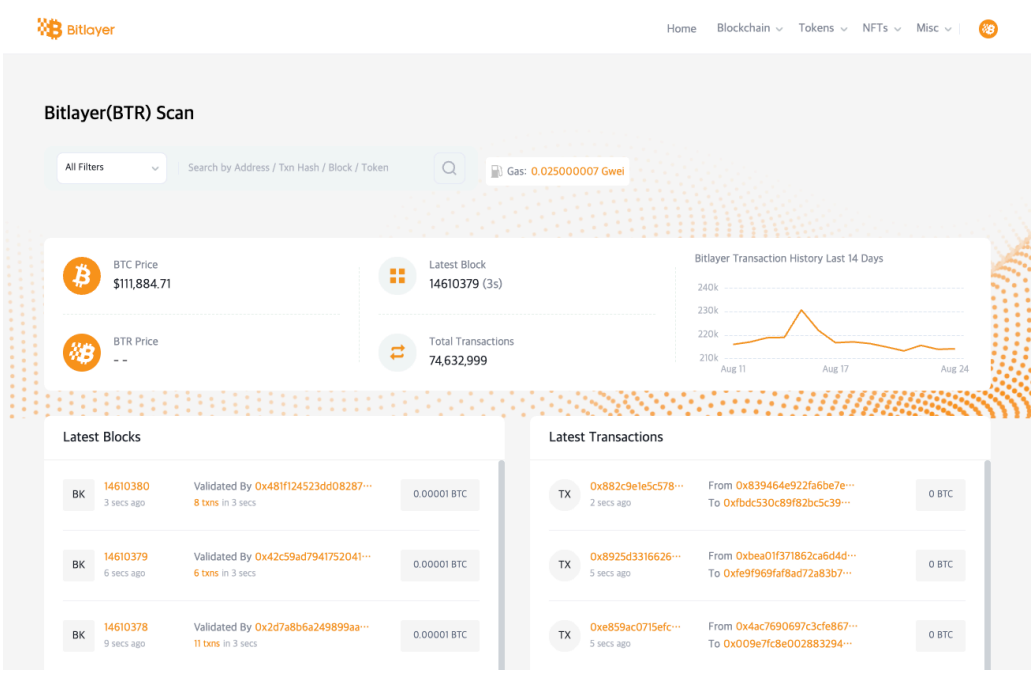
3. 참고자료

Roadmap



출처 : Bitlayer Docs

BTRScan



출처 : BTRScan

위험고지 안내
Disclaimer

본 문서에 기재된 정보는 당사(코인원)가 본 가상자산 심사 시점에 접근 가능한 정보 채널을 통하여 확인한 것으로, 정확하지 않거나 투자시점에는 변경 또는 유효하지 않을 수 있습니다.

가상자산 발행자가 공시한 내용 및 백서를 통해 정확한 정보를 확인하신 후 투자하시기 바랍니다.

가상자산은 법정화폐가 아니므로 특정 주체가 가치를 보장하지 않습니다.

coinone