

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.

기본 정보

가상자산 카테고리	유틸리티
거래지원 네트워크	Ethereum
홈페이지	https://boundless.network/
참고문헌 (백서, Docs 등)	https://read.boundless.network/

1. 프로젝트 정보

프로젝트 개요

바운드리스(Boundless)는 실행(Execution)과 합의(Consensus)를 분리하는 설계를 통해, 모든 블록체인에 대규모의 검증 가능한 연산(Verifiable Compute)을 제공하는 범용 제로 지식(Zero-Knowledge, ZK) 프로토콜입니다. 제가 설명드리면, 각 체인은 고유의 보안과 합의를 유지한 채 복잡한 연산을 오프체인으로 위임하고, 오프체인에서 생성된 ZK 증명만 온체인에서 저비용으로 검증합니다. 이렇게 함으로써 체인은 가스 한계와 재실행 병목에서 벗어나고, 네트워크 성능이 가장 느린 노드가 아닌 전체 프로버 집합의 총합 능력에 의해 결정되도록 만듭니다.

바운드리스의 진입점은 각 주요 체인에 네이티브로 배포된 Boundless Market 컨트랙트입니다. 애플리케이션 개발자는 자신이 활동하는 체인을 떠날 필요 없이, 로컬 컨트랙트 주소와 상호작용하고 해당 체인의 네이티브 자산(예: 이더리움의 ETH, 솔라나의 SOL, 스테이블코인 등)으로 비용을 지불한 뒤, 즉시 온체인에서 검증 가능한 증명을 받아 활용할 수 있습니다. 이 구조 덕분에 별도 브리징이 필요 없고, 지갑·RPC·개발 툴 체인이 그대로 유지되어 채택 장벽이 현저히 낮아집니다.

마켓 동작은 역더치경매(reverse Dutch auction)를 중심으로 이뤄집니다. 요청자는 실행할 zkVM 프로그램의 식별자(이미지 ID와 URL), 입력값(인라인 또는 URL), 공개 출력에 대한 요구조건(예: 예상 저널 해시), 그리고 가격·시간·담보 파라미터를 포함한 오퍼를 구성해 온체인(예: BoundlessMarket.submitRequest()) 또는 오프체인 주문 스트림으로 방송합니다. 경매는 최소가에서 시작해 램프업 기간 동안 선형적으로 최대가까지 상승하며, 프로버는 실제로 프로그램을 내려받아 게스트 실행을 돌려 사이클 수와 증명 난이도를 추정한 뒤 현재 가격이 비용을 상회하는지 판단해 입찰합니다. 가장 먼저 가격을 수락한 프로버가 요청을 락(lock)하여 독점 이행 권한을 확보하고, 이를 위해 락인 담보를 예치합니다. 이 담보는 기한 내 미이행 시 슬래시되며, 50%는 영구 소각, 50%는 온체인 바운티로 전환되어 다른 프로버가 작업을 이어받을 유인을 제공합니다. 한편 어떤 요청은 락 없이 곧바로 이행해도 되며, 이 경우 당시 경매가로 정산됩니다.

증명 생성은 집계와 배치를 통한 가스 절감에 초점을 둡니다. 프로버는 여러 개의 개별 요청을 병렬·연속 처리한 후, 각 요청의 실행 영수증(저널과 개별 증명)을 머클 트리의 리프로 구성하고, 배치 전체의 정합성에 대해 단일 Groth16 증명으로 루트를 보증합니다. 온체인에서는 이 루트만 한 번 검증하면 되고, 각 요청은 자신의 머클 포함 증명만 제시하면 되므로, 검증 가스가 요청 수에 비해 거의 증가하지 않습니다. 이 덕분에 바운드리스는 “요청이 많을수록 단가가 떨어지는” 규모의 경제를 만들고, 실사용 환경에서 DEX 스왑보다 낮은 수준의 가스 발자국으로 많은 요청을 정산할 수 있게 설계되었습니다.

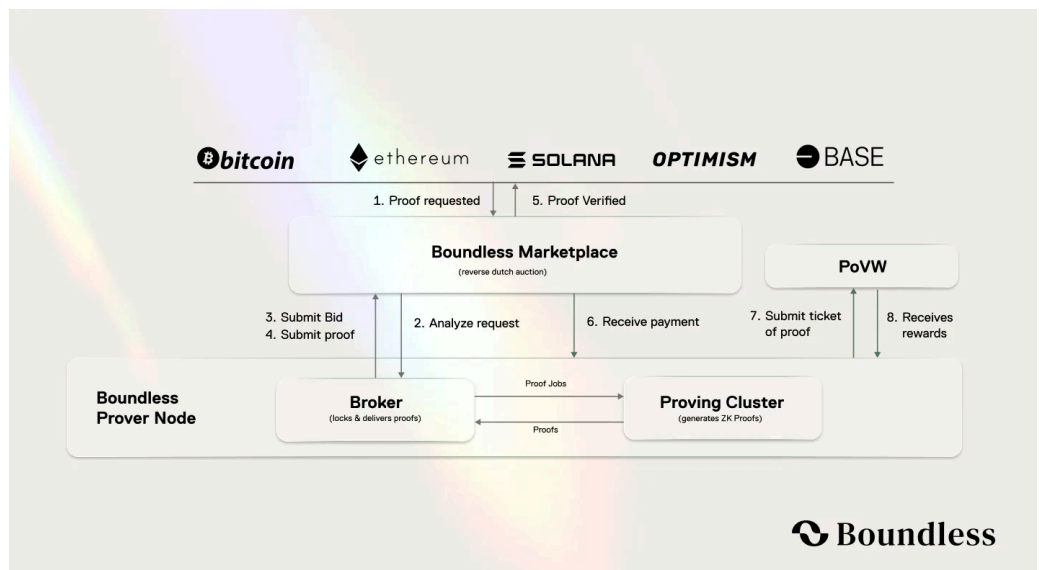
Boundless market participants

Role	What they do	What they receive
Proof Requestors - apps, rollups, bridges, exchanges	Proof request that includes what they want proven, how much they are willing to pay and when they need it by	A proof on their preferred settlement layer
Boundless Prover Nodes - independent operators, GPU farms, datacenters	Hardware plus a refundable stake; they claim requests at or below the posted price	Immediate onchain payment from the requestor, plus a protocol-level PoVW reward

 Boundless

출처 : 바운드리스 블로그

정산 단계에서 마켓 컨트랙트는 제출된 Groth16 루트를 검증하고, 각 요청에 대한 머클 포함 증명이 사전 요구조건(이미지 ID 일치, 저널 제약 충족 등)을 만족하는지 확인합니다. 모든 조건을 충족하면 컨트랙트는 요청자가 사전에 예치해 둔 네이티브 자산(또는 락된 자금)에서 프로버에게 대가를 지급하고, 락인 담보를 반환합니다. 동시에 “요청 이행” 이벤트를 방출해 요청자에게 머클 포함 증명을 제공하고, 요청자는 이를 애플리케이션 컨트랙트의 검증 루틴(예: 라우팅형 검증 컨트랙트)으로 전달해 상태를 안전하게 업데이트합니다. 필요 시 컨트랙트 콜백을 등록해 증명 납품 즉시 온체인 로직을 트리거할 수도 있습니다.



출처 : 바운드리스 블로그

토크노믹스 관점에서 ZKC는 담보, 스테이킹, 인센티브, 거버넌스를 아우르는 핵심 실행 자산으로 작동합니다. 프로버는 증명 요청을 수락하기 전 일반적으로 요청 최대 수수료의 약 10배에 해당하는 ZKC를 담보로 예치해야 하며, 미이행 시 절반 소각·절반 바운티의 슬래싱이 적용됩니다. 이 담보 체계는 납기 준수를 경제적으로 강제하고, 요청량이 늘수록 약 10배 스케일의 담보가 동반 잠기기 때문에 유통량을 구조적으로 조이는 효과가 발생합니다. 모든 참여의 출발점은 스테이킹이며, ZKC를 스테이킹하면 프로버 운영 자격과 함께 프로토콜 거버넌스 권한이 부여되고, 에폭 보상의 최소 25%가 스테이커에게 분배됩니다. 일부 설계에서는 스테이킹된 ZKC를 기준으로 sZKC 같은 파생 토큰을 발행해 온체인 검증성과 경제적 안전성을 더합니다.

인센티브는 PoVW(Proof of Verifiable Work) 메커니즘으로 집행됩니다. 각 증명에는 “증명된 사이클 수”와 재사용 방지용 난스가 포함된 변경 불가능한 태그가 기록되며, 이는 증명의 공개 주장(public claim)의 일부라 요청자나 프로버가 임의로 조작할 수 없습니다. 에폭이 끝나면 해당 기간 동안 최종 확정된 증명의 사이클 태그를 합산하고, 미리 정의된 양의 ZKC가 새로 발행돼 사이클 점유율에 정확히 비례해 분배됩니다. 따라서 전체 사이클의 2%를 제공한 프로버는 해당 에폭 발행량의 2%를 받습니다. 이 구조는 “10 사이클 증명과 1,000만 사이클 증명을 동일하게 취급”하는 불공정성을 제거하고, 지연·담보 요건을 충족하는 누구에게나 열린 경쟁을 제공하며, 모든 정산이 온체인에서 감사 가능한 투명성을 갖추게 합니다. 에폭 발행분 중 75%가 프로버에게, 25%가 프로토콜 스테이커에게 돌아가므로, 유용한 작업에 직접 연결된 발행과 장기 안정성을 위한 기본 보상이 균형을 이룹니다.

수수료 라이프사이클을 정리하면, 요청자는 자신의 홈 체인의 네이티브 자산으로 Boundless Market에 수수료를 예치하고, 역더치경매를 통해 선정된 프로버가 기한 내 유효한 배치 증명을 제출하면 컨트랙트가 이를 검증한 뒤 프로버에게 예치금을 지급합니다. 프로버의 ZKC 담보는 이행 시 반환되지만, 미이행 시 50% 소각·50% 바운티로 전환되어 다른 프로버가 이어받을 인센티브가 됩니다. 이 과정과 별개로 에폭 단위의 PoVW 발행이 사이클 점유율에 따라 분배되어, 프로버는 “요청자 수수료 + PoVW 보상”의 이중 수익 구조를 갖게 됩니다. 요약하면 결제 자산은 체인별 네이티브 토큰이지만, 네트워크의 안전성과 서비스 품질은 전적으로 ZKC 스테이킹·슬래싱 규율과 PoVW에 의해 담보됩니다.

아키텍처적 장점도 분명합니다. 검증과 정산은 항상 애플리케이션이 정착하는 L1/L2에서 직접 수행되므로 보안·검열저항성이 호스트 체인과 동일하게 유지됩니다. 입찰·순서 민감 연산은 체인의 기본 시퀀서가 결정해 공정성과 MEV 최소화를 달성하고, 펀드 브리징이 필요 없어 추가적 신뢰 가정과 UX 마찰을 건어냅니다. 핵심 로직은 zkVM으로 오프로드되고, 온체인 저장·실행을 최소화하며, 배치·집계로 가스를 크게 절감합니다. 블록 타임이 빠른 체인에 마켓을 배치하면 “다음 블록 제출” 수준의 저지연 증명 전달도 현실적인 목표가 됩니다.

실제 적용 사례로는, 이더리움 정합성을 유지하면서 멀티 프로버 구성으로 유효성 증명을 위임하는 ZK 롤업(Taiko), 비트코인 블록스페이스에 EVM 스타일의 프로그래머빌리티를 더하는 Citrea, 솔라나 툴체인 성능을 유지하되 임의 체인으로 결산하는 SVM 롤업 스택(SOON), 비트코인 파이널리티를 앵커로 1시간대 파이널리티를 구현하는 하이브리드 롤업(BOB), 고빈도 매칭을 오프체인에서 수행하고 거래·지급능력을 동시에 증명하는 검증가능 거래소(Hibachi), 멀티체인 유동성을 하나의 풀처럼 취급하면서 대규모 상태 조화·금리 계산을 오프체인에서 처리하는 대출 프로토콜(Mendi) 등이 있습니다. 초기 채택자들은 가장 무거운 로직을 바운드리스로 밀어내면서 가스 한계를 벗어나고, 보안 가정을 강화하는 효과를 이미 확인하고 있습니다.

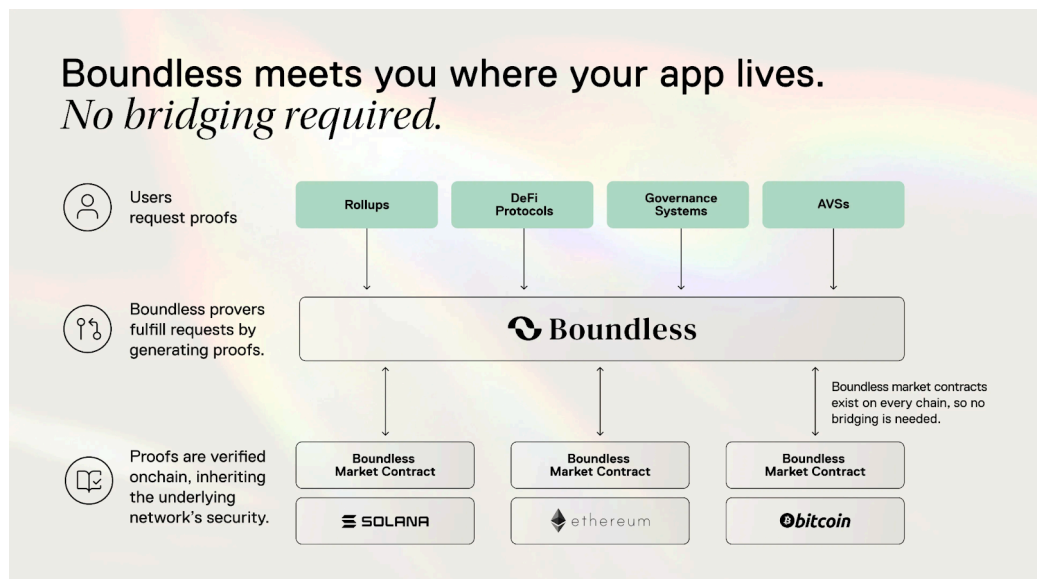
바운드리스 네트워크의 아키텍처

Boundless는 개발자들이 필요로 하는 다양한 조건들을 충족시키기 위해 여러 가지 접근 방식을 검토하면서 탄생한 프로젝트입니다. 비용 효율성과 개발자 경험, 검열 저항성, 그리고 안정성 같은 요소들을 모두 고려한 끝에, Boundless는 결국 ZK 증명이 필요한 프로토콜과 같은 위치에서 동작하는 스마트 컨트랙트가 가장 튼튼한 기반이라는 결론에 도달했습니다. 이 구조를 통해 Boundless는 증명 노드와 시장 요청과 같은 핵심 구성 요소들을 오프체인에서 처리하면서도, 사용자가 요구하는 높은 수준의 안정성과 보안성을 충족시킬 수 있습니다. 결과적으로 사용자는 DEX를 사용하는 것과 같은 매끄러운 경험을 얻을 수 있고, 동시에 ZK 기술이 보장하는 강력한 보안성과 신뢰성을 누릴 수 있습니다. Boundless는 이미 주요 L1과 L2 체인 위에서 배포되어 있으며, 애플리케이션은 자신이 속한 네이티브 체인에서 Boundless를 자연스럽게 통합할 수 있습니다.

Boundless의 시장 아키텍처는 특히 높은 안정성과 검열 저항성을 요구하는 프로토콜을 위해 설계되었습니다. 예를 들어 롤업, 탈중앙화 거래소, 리스테이킹 프로토콜, 온체인 거버넌스 시스템 같은 사례들이 여기에 해당합니다. 이러한 애플리케이션들은 메이저 L1 수준의 보안과 신뢰성을 반드시 필요로 하는데, Boundless는 이 요구를 충족시키기 위해 온체인 검증을 제공하고, 호스트 체인과 동일한 수준의 검열 저항성을 보장하며, 자금을 브리징할 필요성을 제거합니다. 중요한 점은 애플리케이션이 어느 체인을 선택하든 Boundless가 해당 체인에서 직접 동작한다는 점입니다.

Boundless의 검증 방식은 신뢰성을 크게 강화합니다. 다른 체인에서 검증하거나 브리징을 거치게 되면 새로운 밸리데이터 집합이나 브리지에 대한 신뢰 의존성이 발생합니다. 하지만 Boundless는 애플리케이션이 위치한 체인에서 증명이 제출되고 검증이 완료되어야만 지급이 이루어지도록 설계되어 있습니다. 이를 통해 애플리케이션은 중간 매개체를 거치지 않고 Boundless의 마켓 컨트랙트와 직접 상호작용할 수 있습니다.

검열 저항성 역시 Boundless의 핵심 장점 중 하나입니다. 롤업이나 거버넌스 시스템 같은 경우에는 어떤 상황에서도 증명이 꾸준히 제출되어야 하는데, Boundless는 애플리케이션 체인의 트랜잭션 보장에 의존해 이를 실현합니다. 따라서 애플리케이션 체인과 단 하나의 증명자만 살아 있다면 Boundless는 증명을 전달할 수 있습니다. 시장의 대부분의 상호작용은 스마트 컨트랙트를 통해 이루어지며, 오프체인 주문 제출은 단순히 선택 가능한 빠른 경로일 뿐 필수적이지 않습니다. 심지어 모든 웹 서비스가 오프라인이 되더라도 Boundless는 여전히 애플리케이션 체인의 검열 저항성에 기대어 정상적으로 동작할 수 있습니다.



출처 : 바운드리스 블로그

입찰 순서 역시 중요한 요소인데, Boundless는 이를 애플리케이션 체인의 네이티브 시퀀싱에 맞춰 처리합니다. 입찰이나 순서 결정이 중요한 연산은 모두 해당 체인의 스마트 컨트랙트 상에서 이루어지며, 이는 체인의 시퀀싱 레이어와 동일한 수준의 공정성과 최소한의 가치 추출 보장을 제공합니다. 결국 Boundless의 보장은 애플리케이션 체인 자체의 보장과 완전히 동일해집니다.

자금 브리징 문제 또한 Boundless가 해결하는 부분입니다. 다른 체인으로 자금을 이동시켜야 한다는 조건은 사용자에게 불필요한 불편과 신뢰 부담을 안깁니다. Boundless는 사용자가 속한 체인에서 직접 동작하기 때문에 새로운 가스 토큰을 사용할 필요가 없고, 요청을 위해 자금을 브리징할 필요도 없습니다. 또한 기존 지갑과 RPC

제공자와도 매끄럽게 호환되기 때문에, 사용자 입장에서는 Boundless와의 상호작용이 기존의 스마트 컨트랙트와 다르지 않습니다.

흥미로운 점은 Boundless 팀이 초기에는 커스텀 L1이나 L2 롤업을 구축하는 방안도 고려했다는 것입니다. 당시에는 지연 시간 단축, 가격 발견 효율성, 운영 비용 절감 측면에서 독자적인 장점이 있을 것이라고 판단했습니다. 그러나 최종적으로는 커스텀 체인 없이도 동일한 효과를 낼 수 있다는 결론에 도달했습니다. 예를 들어 증명 제출 속도와 관련해 Boundless는 “다음 블록 증명 제출”을 목표로 설계되어, 애플리케이션의 블록 타임이 곧 증명 제출 속도가 됩니다. 또한 역더치 경매를 활용한 가격 발견 방식을 채택하여 탈중앙 환경에서도 효율적인 시장 운영을 가능하게 했습니다. 다만 경매 방식이 지연을 초래할 수 있어, 블록 타임이 짧은 여러 체인에 시장을 배치하는 방식으로 이를 완화합니다.

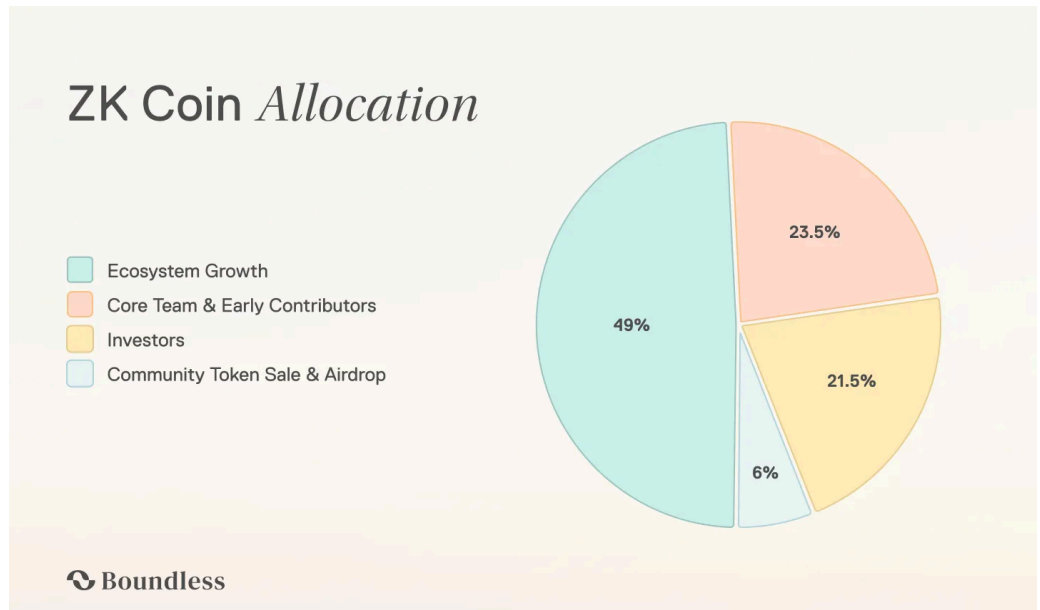
가스 비용 문제 또한 중요한 고려사항이었는데, Boundless는 핵심 로직을 zkVM에 오프로딩하고, 온체인 저장 및 실행을 최소화하며, 증명을 집계하는 방식으로 이 문제를 해결했습니다. 그 결과 온체인에서의 비용 부담은 크게 줄어들었고, 요청 하나당 약 35,000 EVM 가스 수준으로 처리할 수 있어 일반적인 DEX 스왑보다도 저렴합니다. 이는 메이저 L1의 보안성을 그대로 유지하면서도 비용 효율성을 보장합니다.

2. 토큰 이코노미

가상자산 소개

Boundless의 인센티브 설계의 중심에는 PoVW(Proof of Verifiable Work)가 있습니다. PoVW는 허가 없는(permissionless) 채굴 메커니즘으로, 고유한 제로지식 증명을 생산하는 프로버에게 ZKC 보상을 지급합니다. 프로버는 에폭 단위로 자신이 수행하는 총증명 작업량에 비례해 일정 규모의 ZKC를 스테이킹해야 보상 자격이 생기며, 스테이킹 규모가 작업 총량과 함께 스케일합니다. 이 구조는 Boundless 마켓 안팎을 막론하고 다양한 네트워크·마켓에서 ZKC 스테이킹과 PoVW 보상 청구가 가능하도록 확장성을 제공합니다. 그 결과, 더 많은 증명 수요는 더 많은 ZKC 스테이킹으로 이어지고, 프로버 운영자들은 더 큰 PoVW 점유율을 얻기 위해 성능을 지속적으로 개선하게 되는 선순환이 만들어집니다.

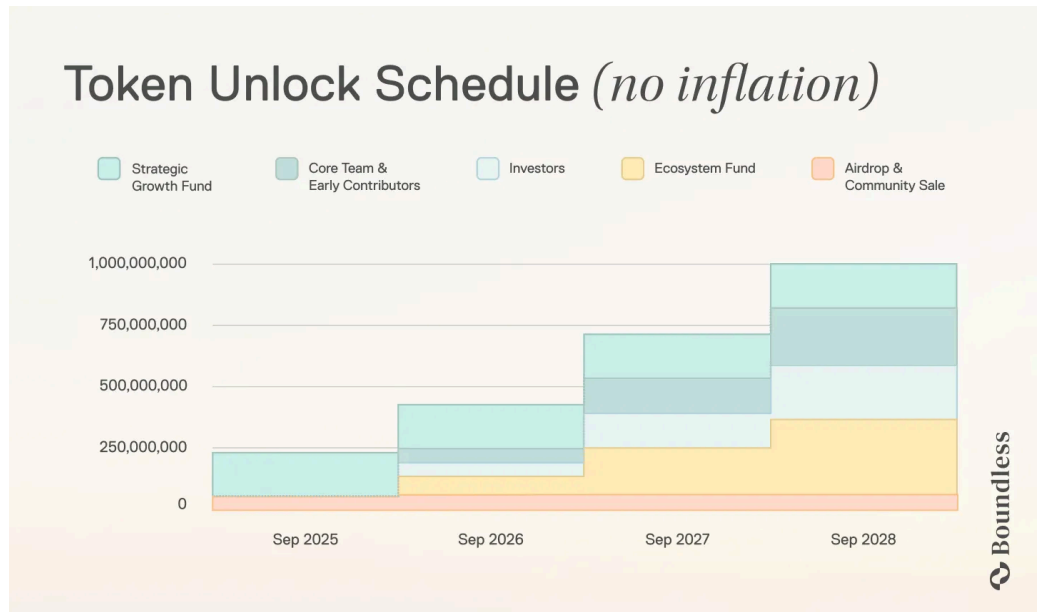
ZKC가 프로토콜을 구동하는 방법을 경제적 안전성과 거버넌스 관점에서 살펴보면 구조가 더 분명해집니다. 먼저 담보 관점에서, 프로버는 증명 요청을 수락하기 전에 해당 요청의 최대 수수료 상한의 최소 10배에 해당하는 ZKC를 담보로 스테이킹해야 합니다. 만약 프로버가 기한 내에 증명을 제출하지 못하면 담보가 즉시 슬래시되는데, 50%는 영구 소각되고 나머지 50%는 온체인 현상금으로 재지정되어 다른 프로버가 작업을 이어받아 증명을 완수할 수 있도록 설계되어 있습니다. 이 담보 메커니즘은 증명 전달의 경제적 확실성을 크게 끌어올립니다. 동시에 요청 규모가 커질수록 약 10배 스케일의 ZKC가 잠기므로 유통량이 구조적으로 조여지는 효과가 발생합니다.



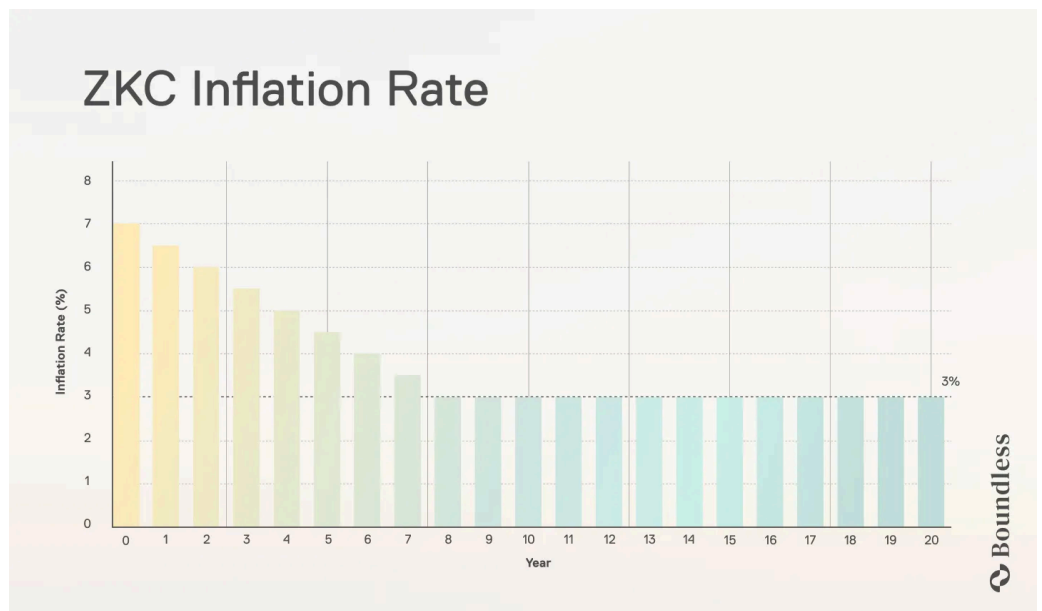
초기 토큰 배분은 총 10억 ZKC를 기준으로 설계되어 생태계 확장과 핵심 기여자 보상, 커뮤니티 분산, 투자 파트너 인센티브를 균형 있게 반영합니다. 생태계 성장에 49%가 할당되며, 이 중 31%는 Boundless 재단이 보유하는 에코시스템 펀드로, 1년 클리프 이후 25%가 해제되고 남은 75%는 24개월 동안 균등 분할로 베스팅되어 3년 차 말에 완료됩니다. 에코시스템 펀드는 검증 가능한 애플리케이션 온보딩과 수수료 보조, 실전 빌드를 돕는 핸즈온 지원, 타 프로토콜과의 통합 및 개발자 도구·교육 리소스 제작, 그리고 프로버와 협력한 용량 변동성 완화 및 인프라 고도화 등 세 갈래 트랙을 중점 지원합니다. 별도로 18%는 전략적 성장 펀드로 배정되어 엔터프라이즈 통합, 비즈니스 개발, 기관급 프로버 온보딩에 쓰이며, 토큰은 12개월에 걸쳐 점진적으로 해제되며 실제 파트너십 체결과 신규 프로버 클러스터 가동 같은 가시적 마일스톤에 연동됩니다. 이 두 풀은 초기 혁신과 기업 채택을 동시에 촉진해, 프로토콜 전반에서 증명 수요를 넓고 깊게 키우는 역할을 합니다.

코어 팀과 초기 기여자에게는 23.5%가 배정됩니다. 총 공급의 20%는 아이디어 단계에서 메인넷까지 프로토콜을 끌고 온 핵심 개발팀과 초기 공헌자에게 돌아가며, 3.5%는 Boundless를 초기 인큐베이션한 RISC Zero에 할당되어 zkVM 성능 향상을 위한 채용 및 연구 гран트에 사용됩니다. 베스팅 일정은 1년 클리프 후 25% 해제, 이후 24개월 균등 베스팅으로 3년 차 말 완료라는 동일한 구조를 따릅니다. 커뮤니티 토큰 세일과 에어드롭에는 약 6%가 할당되며, 세일 물량은 TGE(토큰 생성 이벤트) 시점에 50%가, 6개월 후 나머지 50%가 해제됩니다. 에어드롭은 프로버와 초기 기여자(예: kaito yappers 등)를 대상으로 하며 TGE 시점에 100% 해제됩니다. 투자자 몫은 21.5%로, 자본과 피드백, 기술적 지원, 네트워크 확장을 제공한 전략 파트너에게 돌아갑니다. 이 물량 역시 1년 클리프 후 25% 해제, 이후 24개월 균등 베스팅으로 3년 차에 완료됩니다. 이렇게 설계된 초기 배분은 생태계 구축과 장기적 기여에 인센티브를 조화시키고, 단기 유통량 급증을 방지하는 한편 실사용을 촉진합니다.

토큰 인플레이션은 알고리즘적으로 점진 완화되는 스케줄을 따릅니다. 1년 차 연간 7%에서 시작해 8년 차 이후에는 3%로 테이퍼링되며, 스테이커는 네트워크 보안을 강화한 대가로 예측 가능한 에폭 보상을 받고, 프로버는 운영 비용을 충당하기 위해 일부 보상을 시장에서 판매할 수 있습니다. 중요한 점은 ZKC가 모든 증명 요청의 담보로 필수 스테이킹되어야 한다는 사실입니다. 증명 수요가 증가할수록 담보로 잠기는 ZKC가 늘어 유통량이 효과적으로 조여지고, 여기에 슬래시된 담보의 소각이 결합되어, 공급 동학이 네트워크의 실제 사용량과 직접적으로 연결됩니다.



출처 : 바운드리스 공식 블로그



출처 : 바운드리스 공식 블로그

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.