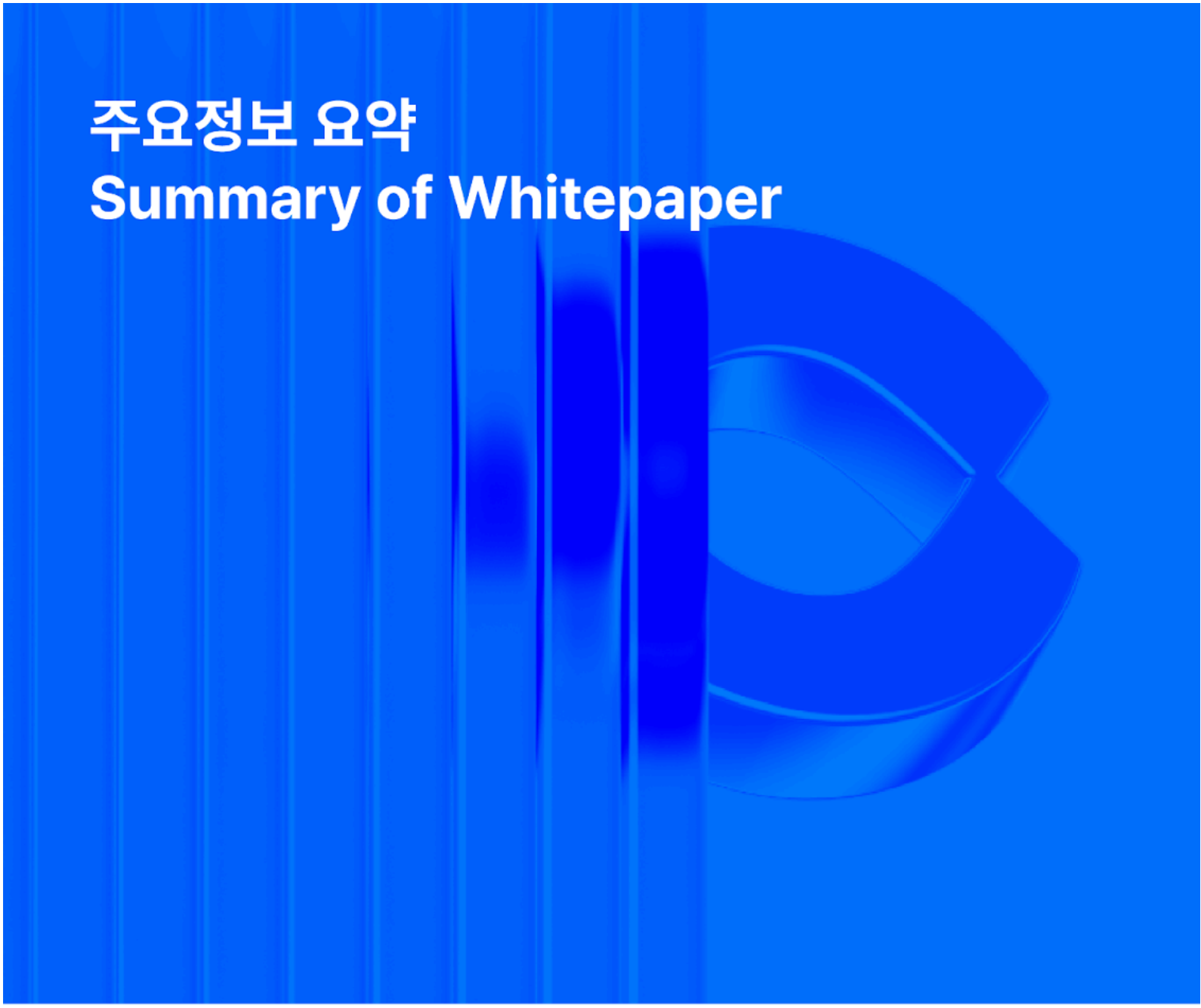
주요정보 요약
Summary of Whitepaper



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

기본 정보

가상자산 카테고리	유틸리티
거래지원 네트워크	Babylon Genesis
홈페이지	https://babylonlabs.io
참고문헌 (백서, Docs 등)	https://docs.babylonlabs.io/papers/btc_staking_litepaper(EN).pdf https://docs.babylonlabs.io/guides/overview/

1. 프로젝트 정보

바빌론 소개

지분증명(PoS) 방식의 블록체인은 자본에 의해 보안이 유지되지만, 그 자본을 확보하는 데에는 높은 비용이 듭니다. 반면 비트코인은 작업증명(PoW) 기반의 블록체인이지만, 약 6천억 달러 규모의 거대한 자산이 존재하며, 이 중 대부분은 활용되지 않은 채 유휴 상태로 남아 있습니다.

Babylon은 이러한 유휴 비트코인을 활용해 PoS 체인의 보안을 강화하고, 동시에 비트코인 보유자가 수익을 창출할 수 있도록 하는 비트코인 스테이킹 개념을 제안합니다. 제안하는 프로토콜은 비트코인을 PoS 체인으로 직접 브리징하지 않고도, 무신뢰 스테이킹(Trustless Staking)이 가능하며, 체인 측에서는 슬래시가 가능한 완전한 보안을 제공받을 수 있습니다.

또한, 스테이킹된 비트코인을 빠르게 언본딩(Unbonding)할 수 있도록 설계되어, 보유자에게 높은 유동성을 제공합니다. 구조적으로는 다양한 PoS 합의 알고리즘 위에 모듈형 플러그인 방식으로 적용될 수 있으며, 이를 기반으로 리스테이킹(Restaking) 같은 새로운 프로토콜도 구축할 수 있습니다.

Babylon은 비트코인 확장성을 위해 Babylon Chain이라는 비트코인 스테이킹 기반의 블록체인을 컨트롤 플레인(Control Plane)으로 사용하여, 여러 스테이커들과 다양한 PoS 체인을 연결하고 동기화하는 시스템 아키텍처를 제안합니다. Babylon 프로토콜을 기반으로 한 비트코인 스테이킹은 비트코인의 새로운 활용 가능성을 제시하며, 비트코인과 지분증명(PoS) 블록체인 생태계 간의 본격적인 연결을 촉진하는 중요한 전환점이 될 수 있습니다.

PoS 보안의 한계와 비트코인의 새로운 역할

PoS 보안에는 자본이 필요하다

2022년 9월 이더리움이 PoW에서 PoS 합의 방식으로 전환한 '머지(The Merge)'를 시작으로, 최근 몇 년 동안 많은 프로토콜이 작업증명(PoW)에서 지분증명(PoS)으로 서서히 전환하고 있습니다. PoW 체인은 채굴자들이 복잡한 수학 문제를 푸는 작업으로 체인을 보호하지만, PoS 체인은 검증인이 일정량의 자산(지분)을 보유하고 있는 것으로 보안을 확보합니다. 이 지분은 담보 역할을 하며, 만약 검증인이 규칙을 어기면 해당 지분은 슬래시 될 수 있습니다. 이러한 슬래시 가능성은 PoW 체인에는 없는 기능이며, 이더리움이 PoS로 전환한 주된 이유 중 하나이기도 합니다. PoS 체인을 공격하려면

스테이킹된 자산의 시가총액만큼의 자본이 필요하므로, 스테이킹된 자산의 규모가 클수록 보안이 강화됩니다. 즉, PoW 체인은 '작업'으로, PoS 체인은 '자본'으로 보안을 유지하는 셈입니다. 하지만 이러한 자본을 유치하는 것은 특히 초기 단계의 체인이나 소규모 체인에게는 매우 어려운 과제입니다. 많은 체인들은 높은 수익률로 자본을 유치하기 위해 초기 인플레이션율을 높게 설정해야 합니다. 예를 들어 Cosmos 생태계의 60개 이상의 앱체인 중 상당수는 연간 20%에서 100%에 이르는 인플레이션율을 설정합니다. 이처럼 높은 인플레이션은 체인의 장기적 성장 가능성에 부담을 줄 수 있습니다.

비트코인 : 6천억 달러 규모의 자산

PoS 방식이 대세로 자리 잡아가고 있지만, 여전히 가장 규모가 큰 가상자산은 비트코인입니다. 전체 시장 시가총액의 절반 이상을 차지하며, PoW 기반으로 운영되고 있습니다. 비트코인은 PoS 자산과 달리 체인의 보안에 직접 사용되지 않고, 대부분 유휴 상태로 존재합니다. 이 때 수익을 내려면 브리징이나 중앙화 수탁을 거쳐야 하며, 이는 많은 사용자에게 리스크로 인식됩니다. 실제로 wBTC와 같은 래핑 비트코인의 비중은 전체 비트코인 공급량의 극히 일부에 불과합니다. 또한 비트코인은 초기부터 다양한 참여자들에게 폭넓게 분산되어 있어 중앙화 우려가 적고, PoS 자산보다 가격 변동성이 낮아 보안 자산으로서도 안정적인 특성을 갖추고 있습니다.

비트코인 스테이킹

이러한 비트코인의 특성을 고려할 때, 비트코인을 PoS 체인의 보안을 위해 스테이킹 자산으로 활용한다는 것이 Babylon의 핵심 아이디어입니다. 비트코인 스테이킹은 양면 시장(Two-sided Marketplace) 구조를 가지고 있습니다.
한쪽에는 보안이 필요하고 그에 대한 보상을 지불할 의향이 있는 PoS 체인들,
다른 한쪽에는 자본을 보유하고 있고 수익을 얻고자 하는 비트코인 보유자들이 존재합니다. 비트코인 스테이킹 프로토콜은 이 두 집단을 연결해주는 보안 공유(Security-sharing) 메커니즘입니다. PoS 체인에는 충분한 보안성을, 비트코인 보유자에게는 안전하고 무신뢰의 수익 창출 수단을 제공해야 합니다.

바빌론 프로토콜의 핵심 구조

바빌론 비트코인 스테이킹 프로토콜: 보안 특성

Babylon의 비트코인 스테이킹 프로토콜은 PoS 체인의 보안성과 비트코인 보유자의 유동성을 동시에 보장하는 것을 목표로 합니다. 이 프로토콜은 세 가지 핵심 보안 특성을 중심으로 설계되었습니다.

첫째, 슬래시가 가능한 완전한 보안을 제공합니다. 즉, PoS 체인에서 검증인이 안전 규칙을 위반할 경우, 해당 검증인이 비트코인 체인에 스테이킹해둔 자산은 실제로 슬래시될 수 있습니다.

둘째, 비트코인을 다른 체인으로 옮기지 않고도 스테이킹이 가능한 무신뢰 스테이킹(trustless staking)을 구현합니다. 이로써 사용자는 자산을 제3자에게 맡기거나 중앙화된 브리지에 의존하지 않고도 PoS 체인에 참여할 수 있습니다.

셋째, 비트코인 보유자들은 빠르고 안전하게 스테이킹 자산을 언본딩할 수 있어, 기존 PoS 체인에 비해 훨씬 높은 유동성을 확보할 수 있습니다. 이러한 보안 특성을 충족시키기 위해 Babylon은 암호학 기술, 합의 프로토콜 설계의 혁신, 그리고 비트코인 스크립트 언어의 정교한 활용을 결합하여 신뢰성 높은 비트코인 기반 스테이킹 솔루션을 만들어냈습니다.

도전 과제

비트코인을 PoS 체인의 보안 자산으로 활용하는 데에는 두 가지 주요 접근 방식이 존재하며, 각각 고유한 한계를 가지고 있습니다.

첫 번째 방식은 비트코인을 PoS 체인으로 브리징하는 것입니다. 즉, 비트코인을 기존 체인에서 PoS 체인으로 옮기고, 그 체인 내에서 슬래시 규칙을 적용하는 방식입니다. 이 방식은 PoS 체인이 슬래시 가능한 보안을 확보할 수 있다는 점에서 효과적이지만, 브리지 자체의 신뢰성과 보안성에 의존해야 한다는 근본적인 문제가 있습니다. 대부분의 비트코인 브리지는 중앙화된 커스터디(예: BitGo)나 다중 서명 방식을 기반으로 하고 있으며, 이는 보안 취약점이 될 수 있습니다. 궁극적으로 브리지를 통해서는 진정한 신뢰 없는 스테이킹을 달성하기 어렵습니다.

두 번째 방식은 비트코인을 체인에 그대로 둔 채 스테이킹하는 원격 스테이킹(remote staking) 방식입니다. 이 방식은 비트코인을 비트코인 체인 상의 특정 컨트렉트에 락업하고, PoS 체인에서 안정성을 해치는 행위가 발생할 경우 이를 슬래시하는 구조입니다. Ethereum의 Eigenlayer나 Cosmos의 Mesh Security 같은 기존 솔루션에서는 이를 스마트 컨트랙트를 활용하여 구현하지만, 비트코인은 튜링 완전한 스마트 컨트랙트를 지원하지 않기 때문에 이러한 구현이 매우 제한적입니다. 따라서 자산은 비트코인 체인에 그대로 있으면서도, 슬래시 가능한 보안을 제공하는 것은 큰 기술적 과제입니다.

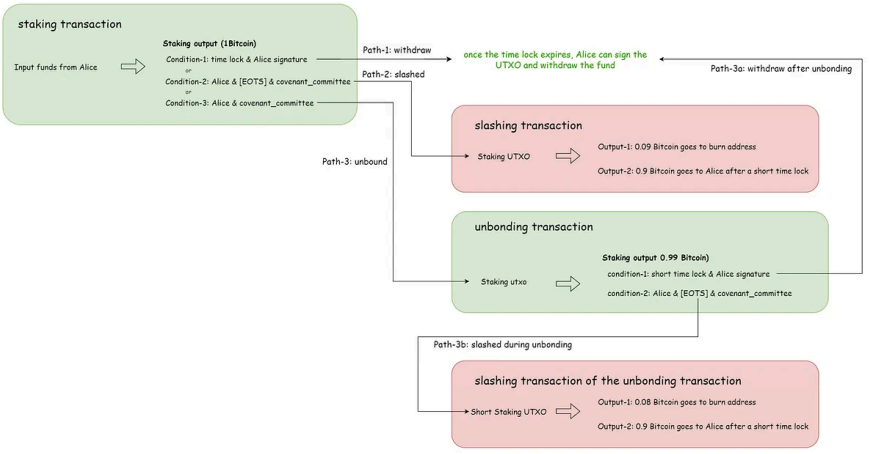
스테이커의 여정

Alice라는 사용자가 1 BTC를 PoS 체인의 보안에 활용하고자 할 때 다음과 같은 여정을 거치게 됩니다. 우선 Alice는 비트코인 체인에 스테이킹 거래를 전송하여, 자신의 비트코인을 셀프 커스터디 형태의 Vault에 락업시킵니다. 이 비트코인은 두 가지 경우에만 언락이 가능합니다. 첫 번째는 Alice가 언본딩 거래(Unbonding Transaction)를 제출하여, 3일 후 비트코인이 그녀에게 반환되는 경우입니다. 두 번째는 Alice가 슬래시 거래(Slash Transaction)를 제출하거나, 그 외의 누군가가 제출하여 비트코인을 소각 주소로 전송하는 경우입니다.

스테이킹 거래가 비트코인 체인에 반영되면, Alice는 PoS 체인에서 검증인으로 활동하며 블록에 서명할 수 있게 됩니다. 이때 두 가지 시나리오가 존재합니다. 첫 번째는 정상 경로(Happy Path) 로, Alice가 정직하게 검증인 역할을 수행한 뒤 스테이킹을 종료하고 싶을 때 언본딩 거래를 제출하는 경우입니다. 해당 거래가 비트코인 체인에 반영되면, 그녀의 검증인 역할은 종료되고 3일 후 비트코인이 반환되며, PoS 체인에서 검증인으로서의 보상도 함께 수령하게 됩니다. 두 번째는 비정상 경로(Unhappy Path)로, Alice가 PoS 체인에서 이중 서명(Double Signing) 같은 안전 위반 행위를 저지를 경우입니다. 이때 프로토콜은 Alice의 개인키를 공개하도록 설계되어 있어, 누구든지 슬래시 거래를 제출해 Alice의 1 BTC를 영구 소각할 수 있게 됩니다. 이 메커니즘은 PoS 체인의 보안을 유지하고, 검증인에게 강력한 억지력을 부여합니다.

기술 구성 요소

Babylon은 스마트 컨트랙트를 지원하지 않는 비트코인 체인의 한계를 극복하기 위해, 여러 기술을 결합해 슬래시 가능한 스테이킹을 구현합니다. 먼저, 비트코인 스크립트를 활용해 자산이 언본딩되거나 슬래시될 수 있도록 설계된 트랜잭션 구조를 사용합니다. 이를 통해 사용자는 자신의 비트코인을 조건부로 락업하고, 특정 상황에서만 회수하거나 소각할 수 있게 됩니다. 슬래시는 EOTS(Extractable One-Time Signature)라는 서명 방식을 이용해 구현됩니다. 검증인이 이중 서명을 할 경우 개인키가 공개되며, 누구든지 해당 비트코인을 소각할 수 있게 됩니다. 이 방식은 기존 합의 프로토콜을 변경하지 않고도 모듈 형태로 쉽게 통합될 수 있습니다. 또한, Babylon은 비트코인 블록체인에 PoS 체인의 블록 정보와 스테이커 정보를 기록함으로써 빠른 언본딩을 가능하게 하고, PoS 체인과의 데이터 동기화를 유지합니다. 이 구조는 Babylon뿐 아니라 다른 PoS 체인에서도 외부 보안 기준으로 활용될 수 있는 가능성을 제시합니다.



시스템 아키텍처

Babylon 비트코인 스테이킹 프로토콜의 전체 인프라는, 비트코인과 PoS 체인들 사이에서 정보를 중재하고 조율하는 '컨트롤 플레인(Control Plane)' 개념을 기반으로 설계되었습니다. 이 컨트롤 플레인은 다양한 기능을 수행합니다. 예를 들어, PoS 체인의 블록 해시와 스테이커 정보를 비트코인에 타임스탬핑하는 서비스를 제공함으로써 두 체인

간의 시간적 동기화를 유지하며, 스테이킹 자산과 PoS 체인을 매칭하고 검증인 키 정보나 파이널리티 서명을 기록 및 추적하는 역할도 수행합니다.

PoS 체인의 검증인들은 일반적인 블록 생성 및 검증 작업 외에도, 파이널리티 가젯에 대한 추가 서명을 수행합니다. 이들은 전체 아키텍처에서 '데이터 플레인(data plane)'을 구성하며, 컨트롤 플레인과 함께 시스템 전반을 운용하게 됩니다. 이 컨트롤 플레인은 자체 블록체인으로 구현되어 있으며, 분산성·보안성·검열 저항성·확장성을 갖춘 구조로 운영됩니다. 기존 비트코인 네트워크의 블록 크기 제한과 비용 문제로 인해, 모든 PoS 체인이 개별적으로 비트코인에 타임스탬핑을 수행하는 것은 비효율적이며, 이를 해결하기 위해 Babylon 팀은 Cosmos SDK를 기반으로 한 Babylon 체인을 설계했습니다. 이 체인은 IBC(Inter-Blockchain Communication)를 활용하여 여러 Cosmos 기반 체인들과 효율적으로 연결되며, 타임스탬프 집계를 담당합니다.

Babylon 체인은 2023년 2월에 테스트넷을 시작했으며, 현재까지 30개 이상의 Cosmos SDK 체인과 통합되어 다양한 분야에서 활용되고 있습니다. 전체 아키텍처는 비트코인을 중심으로, Babylon 체인이 중간에서 조율을 담당하고, 다수의 PoS 체인이 참여하는 3계층 구조로 구성됩니다. 이러한 구조는 네트워크 효과와 상호운용성(Interoperability)의 가능성을 열어주며, 장기적으로는 PoS 체인 간 거래를 Babylon 체인을 통해 정산하는 등의 확장도 가능하게 합니다.

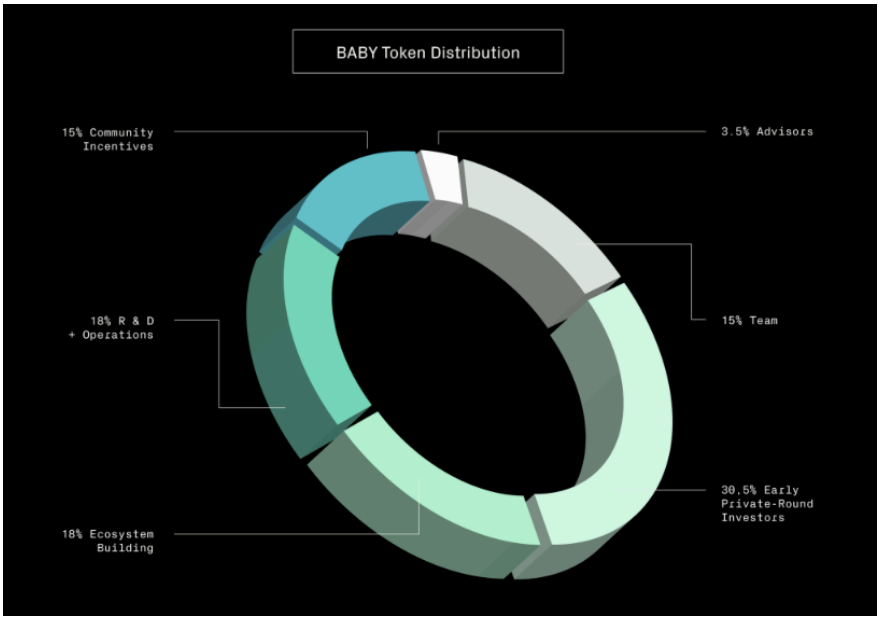
2. 토큰 이코노미

가상자산 소개

BABY는 Babylon 생태계의 네이티브 유틸리티 토큰으로, Babylon 체인의 트랜잭션 수수료, 거버넌스 참여, 네트워크 보안을 검증하기 위한 스테이킹 참여와 이에 대한 보상으로 사용됩니다.

발행량 및 유통량계획

BABY의 발행량은 100억 개이며, 분배율 및 유통량 계획은 아래와 같습니다.



BABY Token Distribution / 출처 : Babylon Foundation 공식 홈페이지

커뮤니티 인센티브 (15%)

Babylon 생태계의 참여를 장려하기 위해, 총 15억 BABY 토큰이 커뮤니티 인센티브 항목으로 배정되어 있습니다. 해당 토큰은 Babylon 재단에 의해 관리되며, 락업이 적용되지 않아 언제든지 배포가 가능합니다. 이 중 최대 4억 BABY 토큰까지 스테이킹이 허용되며, 발생하는 모든 스테이킹 보상은 동일 항목으로 귀속됩니다.

생태계 구축 (18%)

Babylon 생태계의 성장을 촉진하기 위해, 총 18억 BABY 토큰(전체의 18%)이 그랜트, 버그 바운티, 투자, 마케팅, 인수합병 등의 용도로 배정되어 있습니다. 해당 토큰은 총 3년에 걸쳐 언락되며, 네트워크 론칭 시점에 25%가 우선 언락되고, 이후 1주년부터 선형적으로 잔여 물량이 해제됩니다. 이 항목 중 최대 8억 BABY 토큰까지 스테이킹할 수 있으며, 발생하는 스테이킹 보상은 전부 본 항목으로 귀속됩니다.

연구 및 개발 + 운영 (18%)

재단의 운영 자금과, 프로토콜 및 인프라 개발, 비트코인 기반 네이티브 사용 사례 확대를 위한 연구·개발(R&D)을 지원하기 위해, 총 18억 BABY 토큰이 배정되어 있습니다. 이 토큰 역시 3년에 걸쳐 언락되며, 네트워크 론칭 시 25%가 먼저 해제되고, 이후 1주년부터 선형적으로 잔여 물량이 언락됩니다.

Babylon 재단은 필요 시 이 항목에서 언락된 토큰 일부를 커뮤니티 인센티브나 생태계 구축 항목으로 재배정할 수 있는 유연성을 가집니다. 이 중 최대 8억 BABY 토큰까지 스테이킹이 가능하며, 이에 따른 보상은 해당 항목에 귀속됩니다.

초기 프라이빗 라운드 투자자 (30.5%)

Babylon 프로젝트의 초기 프라이빗 라운드 투자자들에게는 총 30억 5천만 BABY 토큰이 할당되며, 이는 4년에 걸쳐 언락되는 구조를 따릅니다. 첫 언락은 네트워크 론칭 1주년 시점에 발생하며, 이때 전체 할당량의 12.5%가 해제됩니다. 이후 잔여 물량은 3년에 걸쳐 선형적으로 언락됩니다. 투자자는 첫 해 동안 락업된 토큰을 스테이킹할 수 없으며, 1년 이후부터는 락업 상태의 토큰도 스테이킹이 가능합니다.

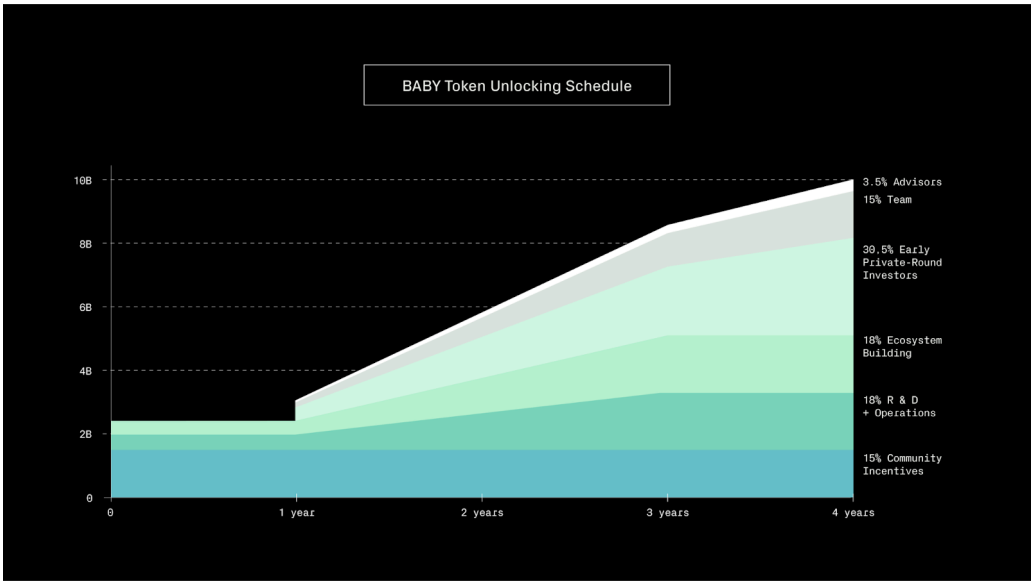
팀 (15%)

Babylon 핵심 팀에게는 총 15억 BABY 토큰이 할당됩니다. 이 토큰은 4년간의 베스팅 스케줄을 따르며, 1년 클리프(cliff) 이후 잔여 물량이 선형적으로 3년에 걸쳐 베스팅됩니다. 베스팅되지 않은 토큰은 스테이킹할 수 없으며, 베스팅이 완료된 토큰은 별도의 4년 언락 스케줄에 따라 해제됩니다.

언락은 네트워크 론칭 1주년 또는 구성원의 근속 1주년 중 더 늦은 시점을 기준으로 최초 12.5%가 언락되며, 이후 3년에 걸쳐 잔여 물량이 선형적으로 해제됩니다. 팀 구성원은 첫 해에는 락업된 토큰을 스테이킹할 수 없으며, 이후부터는 가능해집니다.

어드바이저 (3.5%)

총 3억 5천만 BABY 토큰이 어드바이저에게 배정되며, 이는 팀과 동일한 4년 언락 스케줄과 개인별 베스팅 스케줄을 따릅니다. 베스팅되지 않은 토큰은 스테이킹할 수 없으며, 첫 해에는 락업된 토큰의 스테이킹이 제한됩니다. 이후부터는 스테이킹이 허용됩니다.



BABY Token Unlocking Schedule / 출처 : Babylon Foundation 공식 홈페이지

참고로 1년에 총 8%의 인플레이션이 발생하며, 4%는 BABY 스테이킹에 대한 보상, 4%는 BTC 스테이킹에 대한 보상으로 지급됩니다. 인플레이션율은 거버넌스에 의해 변경될 수 있습니다.

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