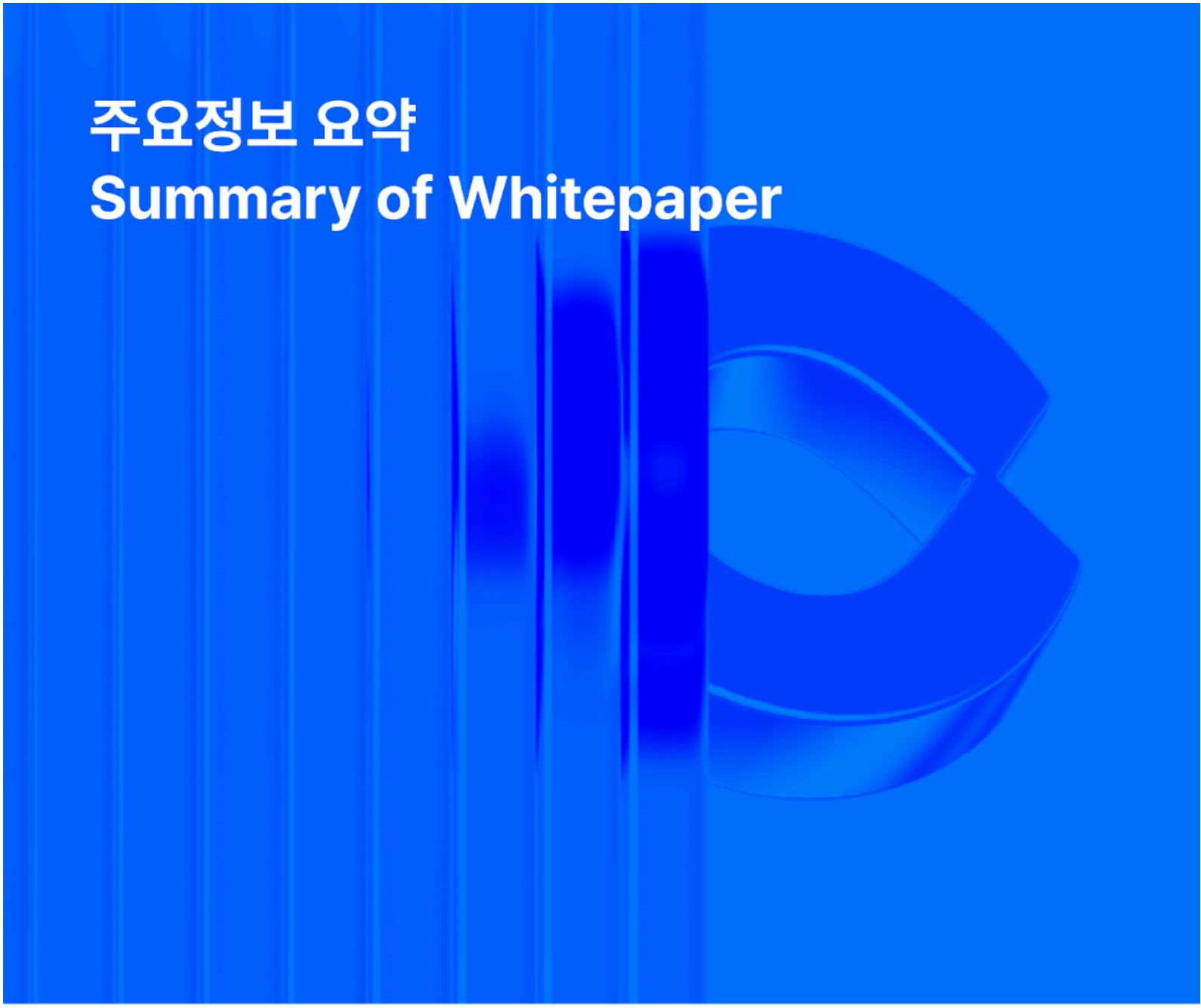
주요정보 요약
Summary of Whitepaper



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	Ethereum
홈페이지	https://www.polyhedra.network/
참고문헌 (백서, Docs 등)	https://docs.zkbridge.com/ https://docs.polyhedra.network/expander/ https://docs.polyhedra.network/expchain/ https://polyhedra.foundation/tokenomics

1. 프로젝트 정보

폴리헤데라 네트워크란?

Polyhedra Network는 차세대 Web3 인프라스트럭처를 위한 상호운용성(interoperability), 확장성(scalability), 프라이버시 보호를 목표로, 고도화된 영지식 증명(Zero-Knowledge Proof, ZKP) 기술을 바탕으로 개발되고 있는 프로젝트입니다. Polyhedra Network는 Web2 및 Web3 시스템 간의 자산 이전, 메시지 전달, 데이터 공유를 위한 신뢰 최소화(trust-minimized) 및 고성능 상호운용 솔루션을 제공합니다.

폴리헤데라 팀은 UC Berkeley, 칭화대학교(Tsinghua University), 스탠퍼드 대학교 출신의 최고 수준의 엔지니어, 개발자, 연구원으로 구성되어 있으며, 상호운용성, 확장성, 프라이버시를 중심으로 한 ZKP 기반 Web3 풀스택 솔루션 개발에 집중하고 있습니다. 현재까지 우리는 여러 차세대 zkSNARK 프로토콜과 다양한 혁신적 ZKP 기반 솔루션들을 개발 및 배포하였습니다. 여기에는 다양한 블록체인 시스템 간 자산 및 데이터 상호운용을 가능케 하는 zkBridge, 사용자 프라이버시를 침해하지 않으면서도 자격 증명을 검증할 수 있는 zkDID (탈중앙화 신원) 솔루션, 대규모 ZKP 시스템을 가속화하기 위한 paraPlonk 기반 확장 솔루션 등이 포함됩니다.

상호운용성: 중요하지만 도전적인 과제

Web3 생태계가 지속적으로 확장됨에 따라, 상호운용성(interoperability)은 점차 더 중요한 요소가 되고 있습니다. 상호운용성이란 서로 다른 블록체인, 프로토콜, 시스템들이 원활히 통신하고 함께 작동할 수 있는 능력을 의미합니다. 우리는 Web3의 미래는 상호운용성에 기반한 연결성에 있다고 믿습니다. 즉, 블록체인, 메타버스, 인터넷이 하나로 연결된 세계입니다.

그러나, 블록체인 네트워크 간 보안이 보장된 크로스체인 브리지 구축조차도 상당히 도전적입니다. 현재 존재하는 대부분의 크로스체인 솔루션은 과도한 신뢰 가정에 의존하고 있으며, 이는 다양한 보안 위협에 노출될 수 있습니다. 실제로, 지난 수년간 이러한 크로스체인 브리지를 겨냥한 공격으로 인해 사용자 피해액이 18억 달러 이상에

이르렀습니다.

zkBridge

Polyhedra Network의 zkBridge는 L1 및 L2 간 상호운용성을 위한 신뢰 없는(trustless) 고성능 크로스체인 인프라스트럭처로 설계되었습니다. zkBridge는 영지식 증명(Zero-Knowledge Proof)을 활용하여 두 블록체인 간 합의의 유효성을 검증합니다. 이를 통해 외부 신뢰에 의존하지 않으면서도 높은 보안성과 낮은 온체인 검증 비용을 동시에 달성할 수 있습니다.

우리는 deVirgo라는 새로운 분산형 증명 시스템을 도입하여 증명 생성을 가속화하였으며, 재귀 증명(recursive proof) 기술을 활용해 온체인 검증 비용을 더욱 절감하였습니다. zkBridge는 현재 BNB Chain, Ethereum, Polygon, Cosmos 등 여러 블록체인 네트워크 간의 상호운용을 지원하는 테스트넷을 운영 중입니다. 라이트 클라이언트(light client) 프로토콜이 존재하는 체인에 대해서는 해당 프로토콜을 zk-SNARK 회로로 컴파일한 후, 실행의 정당성을 증명합니다. 수신 측 체인은 소량의 연산만으로 이 증명을 검증할 수 있습니다. 모듈형 아키텍처를 채택한 zkBridge는 토큰 브리징/스와핑, 메시지 전달, 멀티체인 상태변화 기반 연산 로직 처리 등 다양한 애플리케이션에 활용될 수 있습니다.

EXPchain

EXPchain은 Polyhedra Network가 개발한 혁신적인 블록체인으로, 인공지능(AI)과 탈중앙화 기술의 접점을 새롭게 정의하기 위해 설계되었습니다. Polyhedra가 지향하는 신뢰 가능한 AI 생태계의 기반이 되는 EXPchain은, 고급 영지식 기반 머신러닝(zkML) 기술과 혁신적인 지능 증명 프레임워크(Proof of Intelligence, PoI)를 통합함으로써 구축되었습니다. 이 독창적인 결합을 통해, EXPchain 위에 구축되는 AI 애플리케이션은 확장성과 효율성을 갖추는 동시에, 프라이버시 보호와 결과 검증 가능성을 보장합니다. 글로벌 AI 및 블록체인 시장은 빠르게 확장되고 있으며, 2030년까지 수조 달러 규모의 경제적 기여가 예상됩니다. 그러나 이러한 성장에도 불구하고 신뢰, 투명성, 보안에 대한 문제는 여전히 해결되지 않은 과제로 남아 있습니다. EXPchain은 개발자들이 규제 준수, 프라이버시, 책임성을 우선시하는 윤리적인 AI 시스템을 성능 저하 없이 구축할 수 있도록 설계되어, 이러한 문제들을 효과적으로 해결합니다.

EXPchain의 주요 특징은 다음과 같습니다.

영지식 머신러닝 (zkML)

AI 모델과 프로세스에 대한 암호학적 검증을 가능하게 하여, 민감한 데이터를 노출하지 않고도 결과에 대한 신뢰성을 확보할 수 있습니다. 이는 AI 시스템의 투명성과 보안성을 동시에 충족시킵니다.

Expander Proof System
세계에서 가장 빠른 영지식 증명 시스템으로, 복잡한 AI 연산에 대한 실시간 검증을 가능하게 합니다. 기존의 영지식 증명 시스템 대비 최대 1000배 빠른 성능을 자랑하며, 성능의 새로운 기준을 제시합니다.

확장형 지분 증명 (Expanded Proof of Stake, ExPoS)
영지식 증명을 기반으로 하는 통합형 합의 모델로, 다양한 블록체인 간에 확장 가능하고 투명한 스테이킹을 지원합니다.

zkPyTorch
영지식 머신러닝(zkML)을 대표적인 AI 프레임워크인 PyTorch와 원활하게 통합할 수 있는 기능을 제공하여, 개발 복잡도와 시간을 크게 줄여줍니다.

zkNative 블록체인 인프라
AI 사용 사례를 위해 전용 설계된 블록체인 인프라로서, 탁월한 확장성, 빠른 확정성(Finality), 비용 효율성을 제공합니다.

EXPchain은 헬스케어, 스마트 시티, 로보틱스, 금융 등 다양한 분야에 걸쳐 활용될 수 있으며, 책임 있는 혁신을 위한 신뢰성 높은 탈중앙 플랫폼으로 기능합니다. 이는 AI가 더욱 지능적으로 진화하는 것에 그치지 않고, 본질적으로 안전하고 윤리적이며 인간 중심적인 가치에 부합하는 방향으로 나아가기 위한 핵심적인 전환점이 됩니다. EXPchain은 단순한 블록체인을 넘어, “AI를 위한 만능 체인(Everything Chain for AI)”으로서, 인간의 신뢰와 디지털 혁신 사이의 간극을 연결하는 역할을 수행합니다.

2. 토큰 이코노미

가상자산 소개

네이티브 토큰 ZKJ는 보안성과 탈중앙성을 갖춘 생태계 조성에 핵심적인 역할을 수행합니다. EXPchain의 가스비, 트랜잭션 수수료, 스테이킹, 거버넌스의 기반으로 기능하는 ZKJ는, 개발자와 사용자 모두가 신뢰 가능한 탈중앙화 프레임워크 내에서 인공지능(AI)이 발전할 수 있도록 하는 인프라 구축에 주체적으로 참여할 수 있도록 합니다.

Polyhedra Network는 ZKJ 토큰을 통해 커뮤니티 구성원 중심의 거버넌스 구조를 실현합니다. ZKJ는 Polyhedra Network의 네이티브 토큰으로, 다음과 같은 다양한 용도로 사용됩니다.

EXPchain 트랜잭션 수수료(Gas fees)
개발자 및 애플리케이션은 EXPchain 위에 구축된 dApp 및 AI 시스템에서 원활한 운영을 위해 ZKJ로 트랜잭션 수수료를 지불할 수 있습니다.

영지식 증명 서비스 이용료
개발자 및 애플리케이션은 Polyhedra의 영지식 증명(ZK Proof) 서비스 이용 시 ZKJ를 수수료로 지불할 수 있습니다.

zkBridge 트랜잭션 수수료
프로토콜과 사용자는 zkBridge를 통한 크로스체인 트랜잭션 수수료를 ZKJ로 지불할 수 있습니다.
예를 들어, LayerZero 개발자 및 옴니체인 애플리케이션(OApps)은 LayerZero zkBridge Oracle 또는 DVN 트랜잭션 수수료를 ZKJ로 결제할 수 있습니다.

스테이킹(Staking)
사용자는 ZKJ 토큰을 스테이킹함으로써 네트워크 거버넌스, 트랜잭션 검증 등의 활동에 참여하고, 네트워크 및 생태계 인센티브를 받을 수 있습니다.
예를 들어, ZK 증명자(ZK Prover)는 ZKJ를 스테이킹하여 증명 네트워크에 참여하고, 자신이 제공한 증명에 대한 보상을 획득할 수 있습니다.

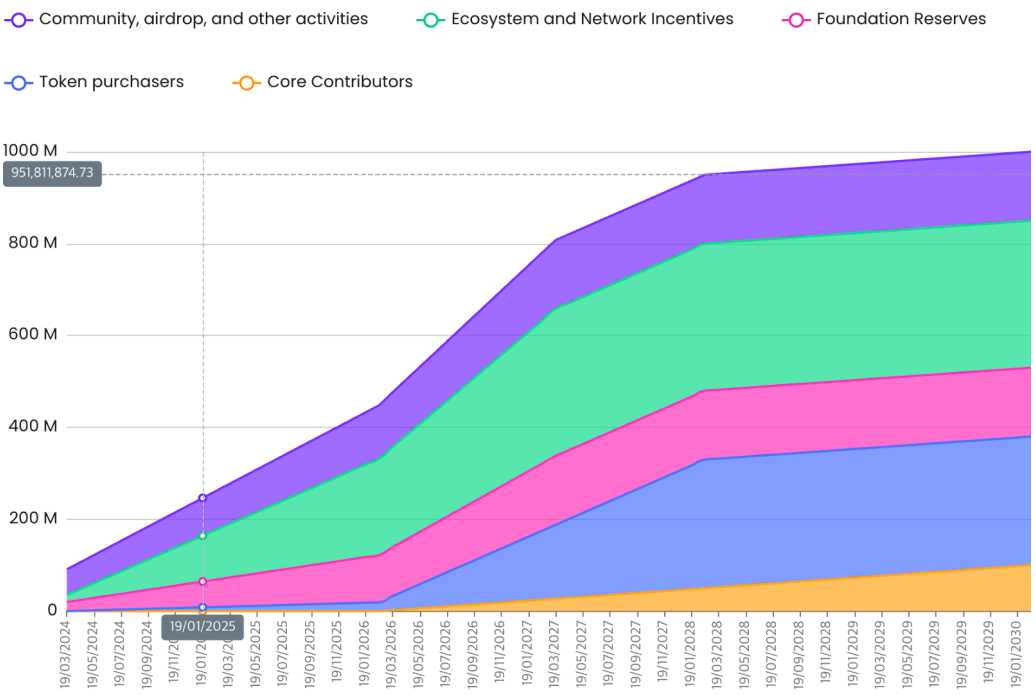
경제적 보안(Economic Security)
ZKJ 토큰은 EigenLayer 리스테이킹(restaking)과 함께 사용되어 암호경제적 보안을 제공합니다. 이중 스테이킹(dual staking) 메커니즘은 Ethereum에서 Bitcoin으로 이어지는 신뢰 최소화 브리지의 보안성을 확보하는 데 활용됩니다.

거버넌스(Governance)
ZKJ 토큰 보유자는 Polyhedra Network의 인프라 및 생태계에 대한 의사결정 과정에 투표권을 행사할 수 있으며, 네트워크 거버넌스 참여 권한을 가집니다.

발행량 및 유통량계획

최대 발행량은 1,000,000,000개 이며, 초기 유통량은 91,000,000개 입니다. Ethereum 체인과 BNB Smart Chain에 각각 900,000,000개, 100,000,000개씩 나뉘어 발행됩니다. ZKJ 토큰은 6년에 걸쳐 점진적으로 유통되며, 각 카테고리별로 다음과 같은 클리프(cliff) 및 언락(unlock) 일정을 따릅니다.

카테고리	총 할당량	클리프 기간	언락 일정
커뮤니티, 에어드롭 및 기타 활동	15%	없음	36개월 분할 해제
생태계 및 네트워크 인센티브	32%	없음	36개월 분할 해제
재단 준비금	15%	없음	36개월 분할 해제
토큰 구매자(TGE 이전 라운드)	2%	1개월	24개월 분할 해제
토큰 구매자 (프라이빗 세일 라운드)	26%	24개월	24개월 분할 해제
핵심 기여자	10%	24개월	48개월 분할 해제



3. 참고자료

https://blog.polyhedra.network/introducing-polyhedra-network/

https://docs.polyhedra.network/expander/

https://docs.polyhedra.network/expchain/

https://polyhedra.foundation/tokenomics

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