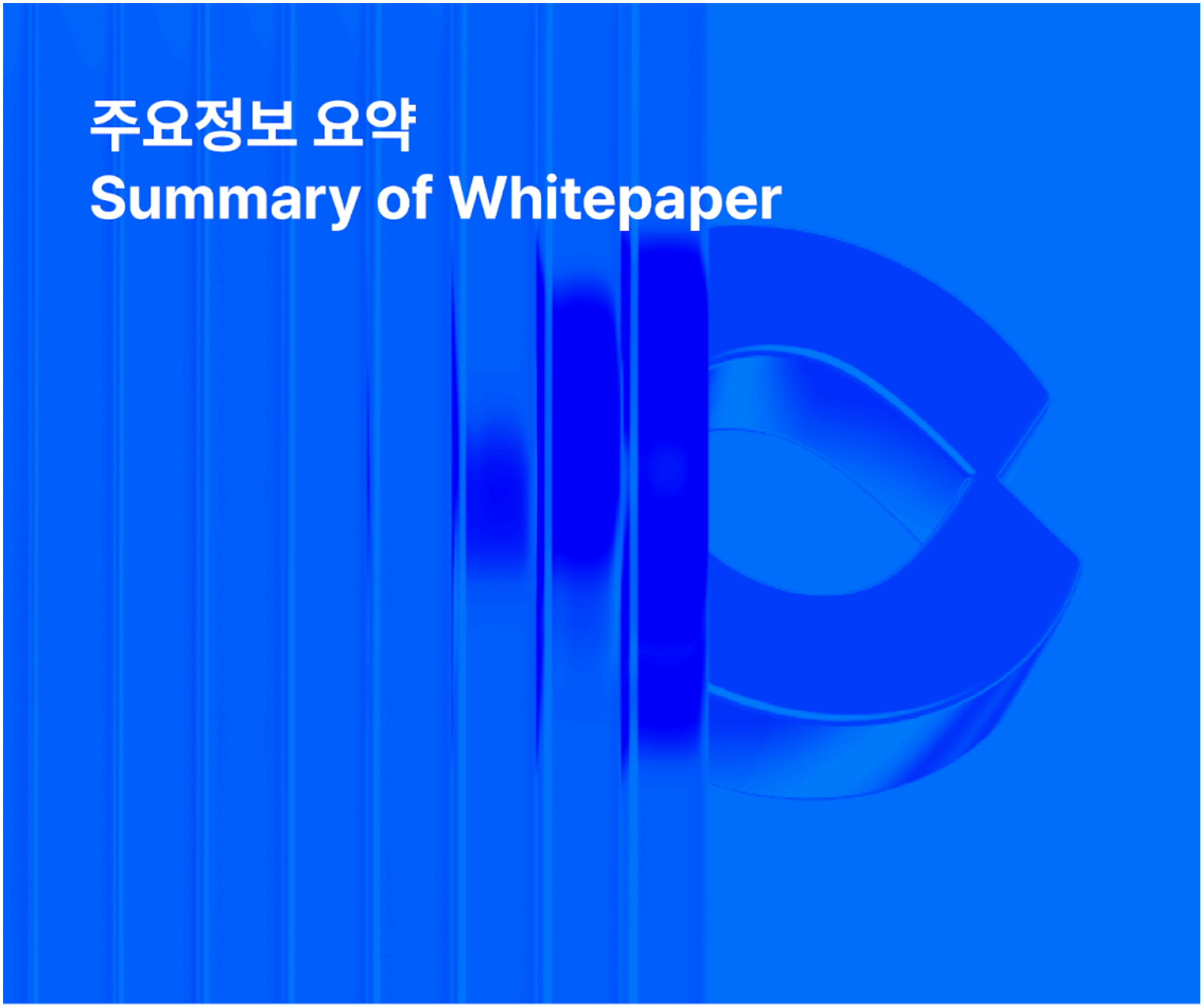
주요정보 요약
Summary of Whitepaper



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.lagrange.dev/
참고문헌 (백서, Docs 등)	https://docs.lagrange.dev/

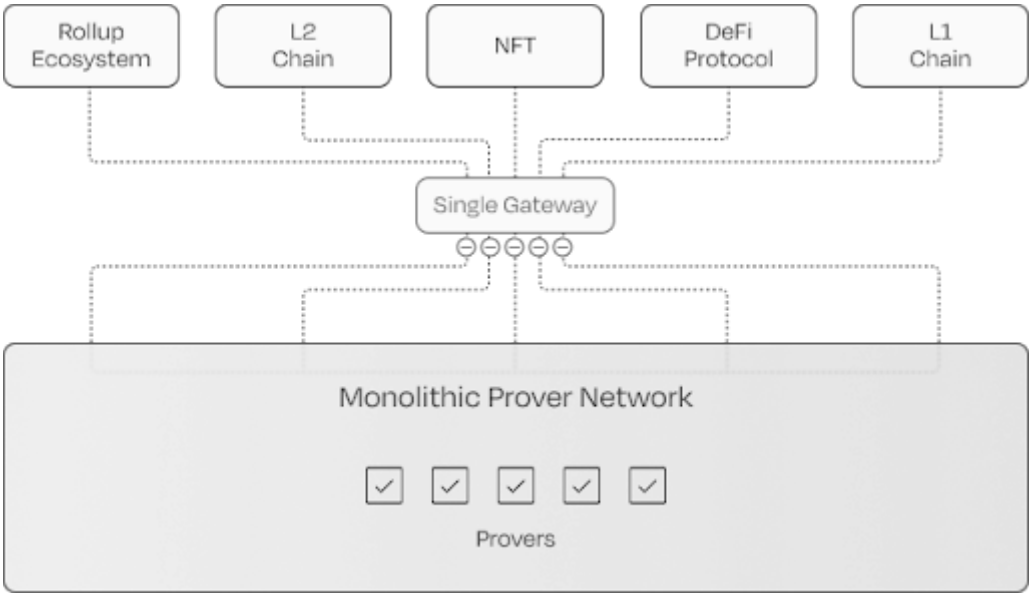
1. 프로젝트 정보

ZK Prover Network 개요

Lagrange의 ZK Prover Network는 롤업, ZK 코프로세싱, 체인 간 메시징과 같은 다양한 사용 사례에 대해 범용적인 증명 생성을 제공하는 기초적인 계층입니다. 이 네트워크는 EigenLayer에 배포되어 있으며, 각각 여러 개의 프로버(Prover)를 실행하는 85개 이상의 최고 수준의 기관급 오퍼레이터들의 지원을 받고 있습니다. Lagrange의 ZK Prover Network의 특정한 아키텍처 덕분에, 병목현상 없이 대량의 증명 요청을 처리할 수 있으며, 높은 생존성 보장과 함께 상호작용이 간단한 인터페이스를 제공합니다.

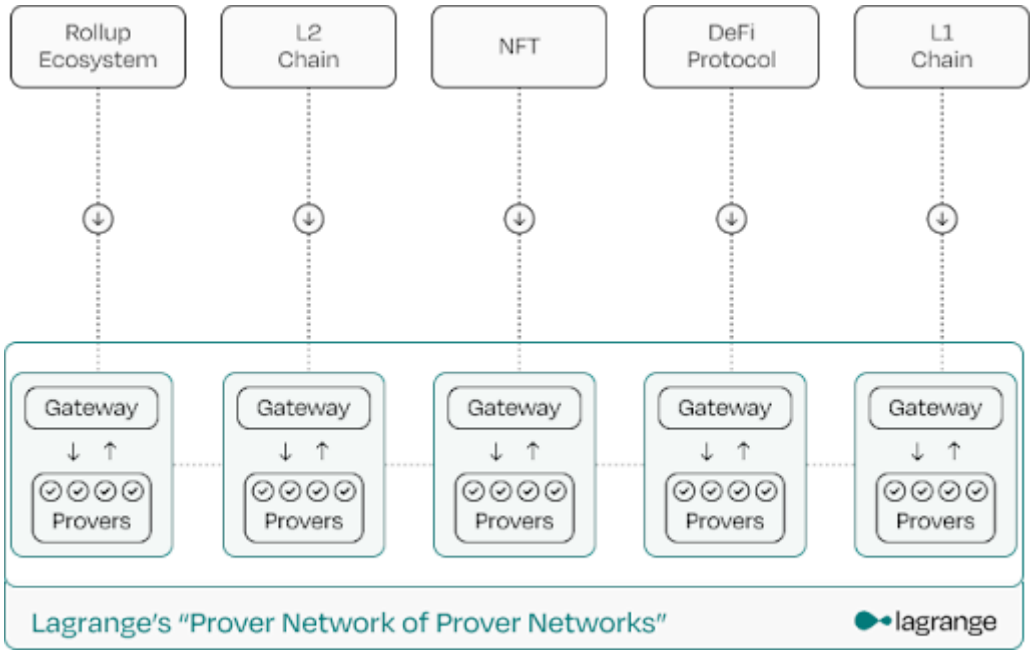
ZK Prover Network 아키텍처

전통적인 일체형(monolithic) ZK Prover 네트워크는 단일 게이트웨이 모델에 의존하며, 이는 본질적으로 확장성을 제한하게 되며 게이트웨이가 병목지점이 됩니다. 또한 시스템의 단일 장애 지점(single point of failure)으로 작용하게 됩니다.



대조적으로, Lagrange의 설계는 모듈형(modular)으로 구성되어 있으며, 각각 전용 대역폭을 가진 다수의 독립적인 서브네트워크(subnetwork)를 지원하여, 이들이 집합적으로 “Prover 네트워크들의 Prover 네트워크”를 형성합니다. 이 접근 방식은 어떤 블록체인, 롤업, 또는 애플리케이션도 맞춤형 표준을 통해 연결할 수 있게 하며, 개발자가 병목현상이나 입출력(I/O) 제약 없이 확장할 수 있도록 해줍니다. 다시 말해, Lagrange의 ZK Prover Network는 대규모 롤업 생태계를 포함한 모든 것을 위해 동적으로 무한

확장이 가능한 증명을 가능하게 합니다.



Lagrange의 ZK Prover Network 아키텍처의 차이점

Lagrange의 ZK Prover Network는 "네트워크들의 네트워크(network of networks)" 아키텍처를 기반으로 하고 있어, 대규모 롤업 생태계가 요구하는 방대한 규모와 복잡도의 증명 생성을 유일하게 지원할 수 있습니다. 그 방식은 다음과 같습니다.

1. **모듈형 서브네트워크(Modular Subnetworks)**

Lagrange는 모듈형 서브네트워크들의 네트워크를 활용함으로써, 어떤 체인, 롤업, 애플리케이션이라도 필요한 증명 자원에 접근할 수 있도록 합니다—병목현상도 없고, 중앙의 접근 제한도 없습니다. 각 서브네트워크는 전용 대역폭을 할당받고 다양한 증명 수요를 지원할 수 있어, Lagrange는 가장 거대한 롤업 생태계를 유연하게 구동할 수 있습니다.

2. **범용 증명에 대한 맞춤형 지원(Customizable Support for Universal Proving)**

Lagrange ZK Prover Network는 전체 네트워크 및 각 서브네트워크 내에서 이질적이고 다양한 증명 수요를 지원합니다. 이는 Boojum, Plonky3, Plonky2와 같은 다양한 증명 시스템뿐 아니라, 고성능이며 표준화된 증명 생성을 포함합니다. 이러한 유연성 덕분에 시스템은 생태계의 요구에 따라 확장될 수 있으며, 동시에 각 프로버는 특화되어 효율성을 유지할 수 있습니다.

3. **증명 생존성 및 비용 효율성(Proof Liveness & Cost Efficiency)**

Lagrange ZK Prover Network는 현재 EigenLayer 상에서 85개 이상의 최고 수준의 기관급 오퍼레이터들로 구성되어 있으며, 이들은 각자 다수의 프로버를 운영하여 증명

생성을 지원합니다. 오퍼레이터들은 정해진 시간 내에 증명을 생성할 것을 약속하며, 이를 이행하지 못하면 슬래싱(slash) 또는 지급 거절의 위험이 있어, Lagrange 네트워크에서의 증명 생존성이 보장됩니다. 또한, 베어메탈 인스턴스의 활용, 규모의 경제(economies of scale), Lagrange의 혁신적인 DARA(Double Auction Resource Allocation) 메커니즘을 통해 비용 효율성 또한 보장됩니다.

4. **프로덕션 준비가 완료된 증명 시스템(Production-Ready Proving)**

ZK 작업의 핵심 요소 중 하나는 분산된 증명 시스템을 관리하는 다양한 세부사항을 처리하는 것입니다. Lagrange의 시스템은 이러한 복잡성을 모두 추상화하여, 증명 생성 요청을 위한 단순하고 통합된 인터페이스를 제공합니다. Lagrange의 ZK Prover Network와 통합함으로써, 파트너들은 애플리케이션에 필요한 증명 생성을 손쉽게 외주화할 수 있으며, 핵심 비즈니스에 더 많은 시간을 집중할 수 있습니다—나머지는 모두 Lagrange가 처리합니다.

ZK Coprocessor 및 Verifiable Database 개요

Lagrange의 ZK Coprocessor 및 Verifiable Database의 목표는 다음과 같이 간단히 표현할 수 있습니다.

원래 블록체인 데이터의 하위 집합을 포함하는 증명 가능한 데이터베이스를 생성하여, 이를 효율적으로 쿼리할 수 있도록 하는 것입니다. 이는 “코프로세서(coprocessor)” 개념과 매우 유사하며, 스마트 컨트랙트가 오프체인에서 집약적인 연산을 수행하고 이를 온체인에서 효율적으로 검증할 수 있도록 합니다. 이 목표를 달성하기 위해, Coprocessor는 다음 두 단계로 작동합니다.

1. 각 블록마다 스마트 컨트랙트의 스토리지를 전처리(preprocessing) 또는 인덱싱하고, 데이터를 Verifiable Database에 증명 가능한 방식으로 “삽입”합니다. 이 데이터베이스는 효율적인 증명 기반 쿼리를 지원합니다. 이 단계는 대부분의 블록체인 데이터 구조가 “증명 친화적(proof friendly)”이지 않기 때문에, 전체 과정 중 계산적으로 가장 집약적인 부분입니다.
2. 스마트 컨트랙트가 쿼리를 요청할 때, 이 새로운 데이터베이스에 대해 병렬적으로 증명 가능한 쿼리를 실행합니다. 이 계산은 대규모 데이터베이스 처리 도구에서 사용되는 MapReduce 방식의 정신을 따릅니다.

ZK Coprocessor는 임의의 스토리지 슬롯과 임의의 블록 범위에 대해 올바른 계산을 증명하는 **증명(proof)**을 생성할 수 있습니다. 예를 들어, 어떤 애플리케이션이 Ethereum 상에서 ETH / USDC 가격의 평균을 계산하고자 한다면, 개발자는 먼저 관심 있는 메모리 슬롯들과 블록 범위(약 50,400 블록)를 명시해야 합니다. 그 다음, 다양한 블록에 걸쳐 스토리지 슬롯을 대상으로 병렬적으로 실행할 계산 작업을 작성합니다. 증명이 생성되면, 이는 해당 데이터가 블록 헤더(스마트 컨트랙트 정보를 통해 유도된) 기준으로 유효한 스토리지 포함성과 집계 계산임을 입증하게 됩니다.

크로스체인

ZK Coprocessor는 EVM 기반의 모든 체인에서 스마트 컨트랙트의 스토리지를 처리할 수 있으며, 해당 쿼리의 결과를 다른 체인의 컨트랙트로 전달할 수 있습니다. 이 과정에서 브리지를 사용할 필요가 없습니다. 앞서 예시를 확장하면, Ethereum 상의 개발자가 여러 L2 체인에서 특정 페어의 평균값을 동시에 계산하고, 그 결과를 Ethereum 컨트랙트에서 받는 것이 가능합니다.

2. 토큰 이코노미

가상자산 소개

LA는 Lagrange의 암호학적 엔진을 구동하는 연료입니다. 이 토큰은 DeepProve와 같은 사용 사례에서 핵심이 되는 Lagrange Prover Network 내 탈중앙화된 증명 활동을 위해, 클라이언트, 프로버(Prover), 그리고 토큰 보유자 간의 이해관계를 조율하는 유틸리티 토큰입니다.

LA 토큰은 주로 클라이언트가 증명 생성 수수료를 지불하는 데 사용되지만, 동시에 프로버의 비용을 보조하고, 토큰 보유자가 스테이킹 및 위임을 통해 참여할 수 있는 구조를 가집니다. 이러한 구조가 어떻게 작동하는지를 이해하는 데는 토크노믹스를 살펴보는 것이 도움이 됩니다.

증명 수요 = 토큰 수요

ZK 롤업, 검증 가능한 AI 모델, 모듈형 실행 계층 등 어떠한 목적으로든 Lagrange Prover Network에서 증명이 생성될 때마다, 해당 활동은 작업 기반 모델을 통해 시스템 내에서 가치가 순환됩니다. 이처럼 토큰은 네트워크 내 활동으로부터 직접적으로 가치를 포착하게 됩니다.
토크노믹스 모델은 다음의 메커니즘을 통해, 증명 활동에서 발생한 가치를 네이티브 토큰(LA)으로 연결합니다

클라이언트 수수료(Client Fees)

클라이언트는 증명을 요청하고, 일반적으로 ETH, USDC 또는 LA와 같은 널리 통용되는 토큰으로, 요구되는 계산량에 비례한 수수료를 지불합니다. 이 수수료의 일부는 LA 보상으로 프로버에게 분배됩니다(모든 프로버는 항상 LA로 보상을 받음). 즉, 증명 수요가 LA 수요로 직접 연결됩니다. ETH나 USDC로 네트워크에 지급된 경우, 해당 자금으로 LA를 바이백하여 사용하는 구조입니다. 이 과정은 LA에 매수 압력을 부여하며, 토큰 보유자에게 긍정적인 피드백 루프를 형성합니다.

프로토콜 발행 및 보조금(Protocol Emissions and Subsidies)

동시에 네트워크는 연간 4%의 고정 $LA 발행량을 유지하며, 이는 클라이언트를 위한 증명을 생성한 프로버에게 분배됩니다. 이는 증명 비용을 보조하여, 클라이언트가 전체 비용 중 일부만 지불하고, 나머지는 토큰 발행분으로 충당되도록 합니다. 해당 보조금은 직접적으로 프로버에게 지급됩니다.

스테이킹 및 위임(Staking and Delegation)

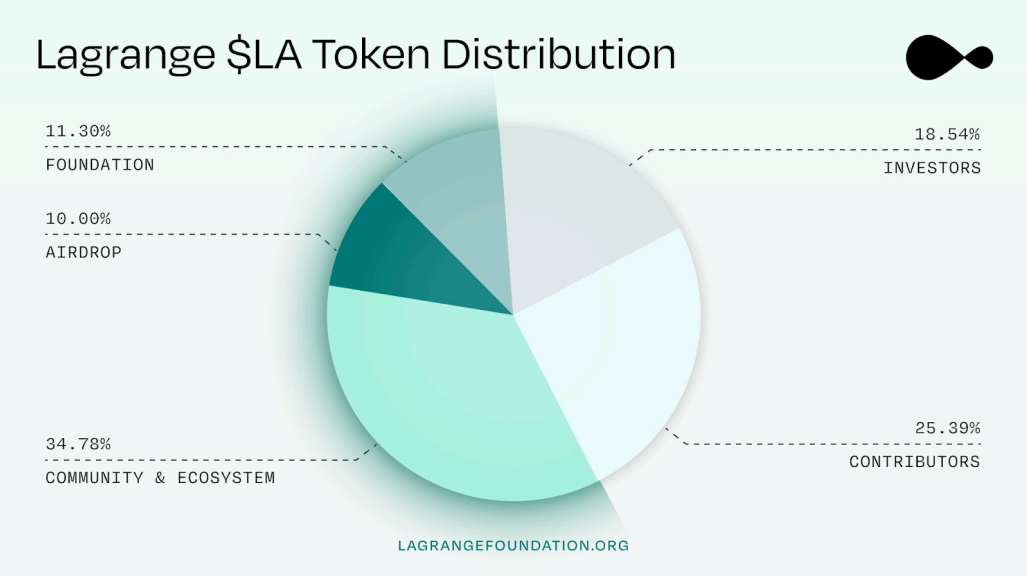
토큰 보유자는 특정 프로버에게 $LA를 스테이킹하거나 위임할 수 있으며, 이를 통해 해당 프로버가 받는 보조금(발행분)의 방향을 설정할 수 있습니다. 스테이킹은 토큰을 락업(lock)시키기 때문에 유통량을 줄이는 2차적인 공급 흡수 기제로 작동하며, 이는 토큰 가치 유지에 기여합니다. 이 메커니즘은 이해관계자가 네트워크의 경제적 우선순위에 영향을 미칠 수 있도록 하며, 증명 수요가 높은 영역과 인센티브가 정렬되도록 돕습니다.

발행량 및 유통량계획

LA 토큰은 총 공급량이 10억 개(1,000,000,000)이며, 연간 4%의 인플레이션율로 신규발행됩니다. 분배는 다음과 같이 이루어집니다.

- **초기 기여자 및 투자자**에게 할당된 토큰은 TGE(토큰 생성 이벤트) 후 1년간 락업되며, 이후 2년에 걸쳐 선형적으로 언락됩니다.

- **커뮤니티 및 생태계**에 할당된 LA는 2025년 5월 28일부터 TGE 등록을 통해 분배가 시작됩니다. 에어드롭 및 TGE에 대한 자세한 내용은 블로그에서 확인할 수 있습니다.



3. 참고자료

https://docs.lagrange.dev/
https://www.lagrangefoundation.org/blog/introducing-the-lagrange-token

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