오로치네트워크(ON)

주요내용설명서(국문백서)

Korean White Paper

2026년 11월 24일

Disclaimer

본 번역본은 2026년 11월 24일 기준의 오로치네트워크(Orochi Network) Docs 및 X(구 트위터)의 관련 내용 위주로 번역됐습니다.

빗썸은 발행주체 또는 운영주체가 제공하는 가상자산의 총발행량, 유통량 계획, 사업 계획 등이 포함된 정보를 이용자들의 편의를 위해 참고용으로 제공하고 있습니다.

본 번역본은 그 내용이 정확하지 않을 수 있으며 원문의 내용이 일부 누락될 수 있으므로, 정확한 정보 습득을 위해서는 원문을 참고하시거나 원문 작성 측에 문의하시기를 바랍니다. 또한 본 번역본은 오픈 커뮤니티의 검토에 따라 내용이 변경될 수 있습니다.

빗썸

프로젝트 소개

오로치네트워크(Orochi Network)는 검증 가능한 데이터 인프라로서 디지털 시대의 데이터 처리 방법을 재정립합니다. 보안과 신뢰 최소화를 설계 원칙으로 두는 오로치네트워크는 영지식 증명[1]과 완전 동형 암호[2], 신뢰 실행 환경[3]을 활용하여 데이터 무결성과 프라이버시를 보장합니다. 오로치네트워크는 데이터의 안전한 처리 및 검증을 통해 기밀성과 투명성이 동시에 확보되는 플랫폼을 제시합니다.

오로치네트워크의 핵심은 검증 가능 데이터 파이프라인(Verifiable Data Pipeline)과 ZK 데이터 롤업(ZK-Data-Rollup)으로, 이 핵심 구성 요소 두 가지를 통해 데이터 무결성이 강화됩니다. 검증 가능 데이터 파이프라인은 데이터 처리의 전 과정을 투명하게 이행하고 위·변조를 방지하며, ZK 데이터 롤업은 데이터 연산을 오프체인에서 일괄 처리하고 민감한 세부 정보는 공개하지 않으면서도 연산이 정확히 실행되었음에 대한 간결한 증명 데이터를 생성합니다. 두 요소가 함께 작용하여 안전하고 확장 가능하며 프라이버시 보호까지 가능한 데이터 관리 시스템의 토대를 형성합니다.

오로치네트워크는 최초의 검증 가능한 데이터 인프라로서 안전하고 검증 가능한 데이터 처리를 위해 영지식 증명을 채택했다는 점이 특징이라 할 수 있습니다. 영지식 증명을 활용하는 덕분에 높은 수준의 프라이버시와 보안, 탈중앙화가 요구되는 애플리케이션 및 플랫폼의 필요를 충족하는 것이 가능합니다. 오로치네트워크의 핵심 특징과 영지식 증명 기반의 데이터 처리 방식이 가진 잠재력은 살펴보도록 하겠습니다.

- ZK 데이터 롤업 직접 지원: 다른 데이터 가용성[4] 레이어와 다르게 오로치네트워크는 자체적으로 영지식 증명을 지원하고 데이터에 롤업 작업을 실행합니다. 그렇기 때문에 간결한 증명 하나로 데이터를 온체인에서 효율적으로 검증할 수 있어 디앱[5]의 확장성과 프라이버시가 강화됩니다.
- 검증 가능 데이터 파이프라인: 오로치네트워크는 데이터 가용성에만 국한되지 않습니다. 샘플링부터 저장, 조회까지 모든 데이터 처리 과정에 암호화 증명을 제공합니다. 암호화 프로토콜만을 활용하기 때문에

[1] Zero-knowledge (zk) proof
[2] Fully homomorphic encryption (FHE)
[3] Trusted execution environment (TEE)
[4] Data availability (DA)
[5] DApp (decentralized application)

제3자를 신뢰해야 하는 필요가 사라지며, 실제 세계 데이터를 스마트 컨트랙트[6]가 읽고 검증할 수 있는 증명 가능한 데이터로 전환하는 것 또한 가능합니다.

- 머클[7] DAG(방향성 비순환 그래프)[8] 활용: 오로치네트워크는 머클 DAG 기술을 활용하여 확장성 및 성능 측면에서 기존 블록체인 구조보다 이점을 제공할 수 있는 잠재력을 갖고 있습니다.
- 간결한 하이브리드형 aBFT(비동기 비잔틴 장애 허용)[9] 합의 메커니즘: 상태 확정을 비동기 방식으로 처리하는 것이 가능해 동기 처리 방식을 활용하는 타 프로토콜에 비해 효율성을 개선할 수 있습니다.
- 시스템 호환 증명: 오로치네트워크는 플롱키3[10], 헤일로2[11], 노바[12], 피클[13] 등 다양한 영지식 증명 시스템과 함께 작동할 수 있어, 개발자는 자신에게 가장 필요하고 적합한 증명 시스템을 유연하게 선택할 수 있습니다.
- 체인 호환: 블록체인 호환을 염두에 두고 설계된 오로치네트워크는 영지식 증명을 활용해 각기 다른 블록체인 간 상호 운용성을 개선하여 다양한 블록체인 플랫폼과의 통합을 진행할 수 있습니다.

비즈니스 모델

zk데이터베이스(zkDatabase)

zk데이터베이스는 오로치네트워크의 혁신적인 솔루션으로 최신 noSQL[14] 데이터베이스 아키텍처와 고도화된 암호화 기술을 결합하여 증명 가능한 데이터 무결성과 프라이버시를 보장합니다. zk데이터베이스의 핵심은 영지식 증명을 활용해 기초 데이터를 노출시키지 않고도 데이터 쿼리 및 트랜잭션[15]을 검증할 수 있다는 점입니다.

---

[6] Smart contract
[7] Merkle
[8] Directed acyclic graph
[9] Asynchronous Byzantine fault tolerance
[10] Plonky3
[11] Halo2
[12] Nova
[13] Pickles
[14] Not only structured query language
[15] Transaction

zk데이터베이스의 엔진 역할을 하는 영지식 증명자[16]는 모든 데이터 트랜잭션의 암호학적 검증 가능성을 책임집니다. 증명자는 그로스16[17] 영지식 스나크[18] 기술을 활용해 검증 시 연산 효율이 높은 간단한 증명 데이터를 생성합니다. 이렇듯 효율적이고 효과적인 증명 생성 및 검증 방식을 통해 데이터베이스 내 영지식 증명을 원활하게 통합할 수 있습니다.

zk데이터베이스는 모듈형 아키텍처로 설계되어 여러 증명 시스템과의 통합이 가능합니다.

아키텍처

- 최신 noSQL: zk데이터베이스는 noSQL 프레임워크를 기반으로 구축되어 유연성과 확장성, 성능이 담보됩니다. 키/값[19], 문서, 그래프 기반 구조 등 다양한 데이터 모델을 지원합니다.
- 암호화 모듈: zk데이터베이스에는 영지식 증명의 생성 및 검증에 특화된 암호화 모듈이 포함되어 있습니다. 암호화 모듈은 최고의 성능을 낼 수 있도록 최적화되어 있어 증명 생성 및 검증 과정의 비용이 최소화됩니다.

사용 사례

- 웹3.0 통합: zk데이터베이스는 증명 가능한 데이터 무결성을 갖춘 안전한 프라이버시 데이터 레이어로서 디앱과 완벽한 호환이 가능합니다.
- 기업용 애플리케이션: 기존 산업에서는 zk데이터베이스를 활용해 데이터를 안전하고 검증 가능한 방식으로 관리할 수 있습니다. 사용 사례로는 금융 서비스(고객 확인[20]/자금 세탁 방지[21]), 의료(환자 데이터 보호), 공급망(제품 진위 확인) 등이 있습니다.
- 데이터 프라이버시 및 보안: zk데이터베이스는 영지식 증명 기반의 효과적인 데이터 검증 방식을 통해 데이터의 기밀을 유지하면서도 검증할 수 있습니다. 따라서 높은 수준의 데이터 무결성과 프라이버시가 요구되는 애플리케이션에 활용하기 적합합니다.

---

16 Prover

17 Groth16

18 SNARK (succinct non-interactive arguments of knowledge)

19 Key/value

20 Know your customer (KYC)

21 Anti-money laundering (AML)

데이터베이스 기술의 상당한 진일보를 상징하는 오로치네트워크의 zk데이터베이스는 데이터 무결성과 프라이버시를 동시에 유지하는 안전한 암호학적 선택지를 제공합니다. 모듈형 설계와 미래에도 지속적으로 사용 가능한 아키텍처로 인해 웹3.0과 기존 기업 애플리케이션에 두루 활용될 수 있습니다.

zk메모리(zkMemory)

zk메모리는 오로치네트워크가 개발한 혁신적인 모듈로서 설정 자유도가 높은 zkVM[22]을 개발할 수 있도록 지원합니다. 근본적으로 zk메모리는 범용 메모리 증명자 역할을 하면서 메모리 일관성 증명[23]을 생성하는 필수 인프라로 기능합니다. 메모리 일관성 증명은 안전하고 효율적이며 검증 가능한 zkVM을 구축하는 데 핵심적인 구성 요소입니다. 유연성, 효율성, 커뮤니티 주도의 혁신 등 오로치네트워크의 지향점이 구체화된 것이 바로 zk메모리라 할 수 있습니다.

zk메모리의 목적은 zkVM 개발을 간소화하면서도 맞춤 설정 측면에서 높은 유연성을 제공하는 것입니다. RAM[24]과 같은 프로그램에서 정확성을 위해 근본적으로 필요한 메모리 일관성을 해결함으로써 zk메모리는 개발자가 메모리 증명을 블록체인, 프라이버시 보호 애플리케이션 등 암호화 및 검증 가능한 환경에 원활하게 통합할 수 있도록 돕습니다. zk메모리는 완전한 오픈 소스 프로젝트이므로, 커뮤니티에서 자발적으로 협업하고 기여하여 성능을 강화하고 혁신을 촉진하는 것이 장려됩니다.

zk메모리는 zkVM 개발 및 통합을 원하는 개발자에게 획기적인 도구가 되어 줍니다. 사전 설정되어 있으나 유연한 조정이 가능한 모듈을 활용해 메모리 증명을 처리함으로써 개발 시간 및 공수를 크게 줄이고 중요한 기능 부분에 더욱 집중할 수 있습니다.

zk메모리의 이점은 아래와 같습니다.

- 편의성: zk메모리는 복잡한 메모리 증명 생성 및 검증을 처리하여 zkVM 구축 과정을 간소화합니다.
- 유연성: VM 아키텍처, 메모리 크기, 구성 요소(스택, 메모리, 레지스터), 명령어 집합, 증명 엔진 등 모든 것을 맞춤 설정할 수 있습니다.

---

[22] Zero-knowledge virtual machine

[23] Memory consistency proof

[24] Random access machine

- 즉시성 및 용이성: 메모리 일관성 증명을 생성하는 데 필요한 도구를 종합적으로 제공받아 다양한 zkVM 사용 사례에 따라 빠르고 간편하게 활용할 수 있습니다.
- 효율성: 비용은 최소화하고 성능은 최대화할 수 있도록 설계되어 있어 기존 시스템과의 원활한 통합이 가능합니다.

zk메모리를 활용해 개발자는 zkVM 설계 시 필요한 기능을 맞춤 설정하고 자체 도구를 통해 메모리 일관성을 유지하고 증명을 생성할 수 있습니다.

오로클(Orocle)

오로클은 블록체인 스마트 컨트랙트에서 사용될 오프체인 데이터를 가져오고 검증하는 오라클[25] 서비스입니다. 기존의 중앙화된 오라클과는 다르게 오로클은 증명 가능한 모델을 토대로 작동하여 단일 장애점[26]과 관련된 위험성을 완화하고 분산형 노드[27] 네트워크를 활용해 신뢰도를 향상시킵니다. 오로클은 웹3.0 생태계 내 동적 애플리케이션에 실시간으로 정확한 데이터를 전달할 수 있도록 설계되었습니다.

오로클 기능

- 다양한 데이터 수집: 금융 시장부터 날씨 현황, 소셜 미디어 여론, 사물 인터넷 데이터까지 다양한 정보 풀에 접근할 수 있습니다. 무궁무진한 데이터를 바탕으로 디앱은 필요한 관련 데이터를 실시간으로 받아볼 수 있습니다.
- 탈중앙화 및 신뢰 가능: 데이터 무결성을 검증 및 유지하는 분산형 노드 네트워크를 통해 데이터 조작 위험이 제거됩니다. 단일 주체가 정보 흐름을 관리하는 일이 없기 때문에 신뢰도와 투명성이 강화됩니다.
- 높은 확장성 및 효율성: 대규모 데이터 요청을 효율적으로 처리할 수 있어 디앱에 복잡한 데이터를 통합하여도 원활한 작동이 보장됩니다.
- 체인 호환: 다양한 블록체인 플랫폼과의 통합을 수월하게 진행할 수 있어 유연성을 확보하고 더 폭넓은 디앱 생태계에 접근할 수 있습니다.

---

[25] Oracle

[26] Single point of failure

[27] Node

오랜드(Orand)

오랜드 프로젝트는 타원 곡선[28] VRF(검증 가능 무작위 함수)[29]를 기반으로 구축되었습니다. 결정론적[30]이고 검증 가능하며 타원 곡선을 활용한 수학적 가정을 토대로 안전하게 작동합니다. 오로치네트워크 운영진이라 해도 결과를 조작하는 것은 불가능합니다.

오랜드는 운영비 최적화와 보안 강화에 도움이 되는 아래와 같은 기능들을 갖추고 있습니다.

- 검증 가능: 오랜드의 에포크[31]는 오로치 시스템 외부에서 개별적으로 검증 가능하며, 스마트 컨트랙트로도 검증할 수 있습니다.
- 직접 제출 및 위임 제출: 오랜드 프로젝트는 증명 제출에 있어 여러 선택지를 제공합니다. 오랜드에서 타원 곡선 VRF 증명을 생성하면 사용자는 제출 방식을 택하기만 하면 됩니다.
    - 직접 제출: 백엔드에서 오랜드로 요청을 보내 스마트 컨트랙트로 무작위 함수를 제출할 수 있습니다.
    - 위임 제출: 토큰을 오로치네트워크 운영자에게 전송하여 제출 과정을 오로치네트워크에 위임함으로써 무작위 함수를 자동으로 제출할 수 있습니다.
    - 요청 제출: 오랜드 서비스 대신 오라클 컨트랙트를 통해 무작위 함수를 요청할 수도 있습니다.
- 일괄 처리: 에포크당 일괄 처리 한도를 설정할 수 있습니다. 예를 들어 한 에포크에 요청 가능한 무작위 함수를 100개로 설정하여 비용을 대폭 절감할 수 있습니다.

---

[28] Elliptic curve

[29] Verifiable random function

[30] Deterministic

[31] Epoch

토크노믹스

네이티브 토큰[32] 오로치네트워크(ON)는 검증 가능한 데이터 인프라의 기반으로서 생태계가 안전하고 효율적으로 작동할 수 있도록 합니다. ON은 아래와 같은 여러 주요 유틸리티를 갖추고 있습니다.

검증인 인센티브

합의 과정 참여 시 검증인은 ON을 스테이킹하여 네트워크의 보안과 무결성을 보장합니다. 검증인은 기여도에 따라 ON을 보상으로 제공받으면서 안정적이고 탈중앙화된 시스템을 함께 형성해 나갑니다.

분산형 스토리지[33]

사용자는 ON을 사용해 오로치의 분산형 스토리지 네트워크 내 저장 공간을 대여할 수 있으며, 사용료는 데이터를 효율적이고 검증 가능한 방식으로 관리하는 데 활용됩니다. 인프라를 유지 및 관리하는 스토리지 제공자는 보상으로 수수료를 제공받습니다.

영지식 시퀀서[34] 보상

트랜잭션 처리 및 프라이버시 보호를 담당하는 영지식 시퀀서는 연산 작업을 수행해 네트워크 확장성을 향상시킨 것에 대한 보상으로 ON을 제공받습니다.

트랜잭션 수수료

ON은 트랜잭션 및 네트워크 상호 작용에 대한 수수료로 사용됩니다. ON은 네트워크 운영의 지속 가능성을 뒷받침함과 동시에 사용자에게는 오로치의 고급 기능을 이용할 수 있는 수단이 되어줍니다.

위와 같은 유틸리티를 보유한 ON은 검증인과 스토리지 제공자, 시퀀서, 사용자가 탄탄한 경제 시스템 안에서 공동의 목표를 향해 나아가게 함으로써 참여를 촉진하고 오로치네트워크를 지속시키는 데 기여합니다.

---

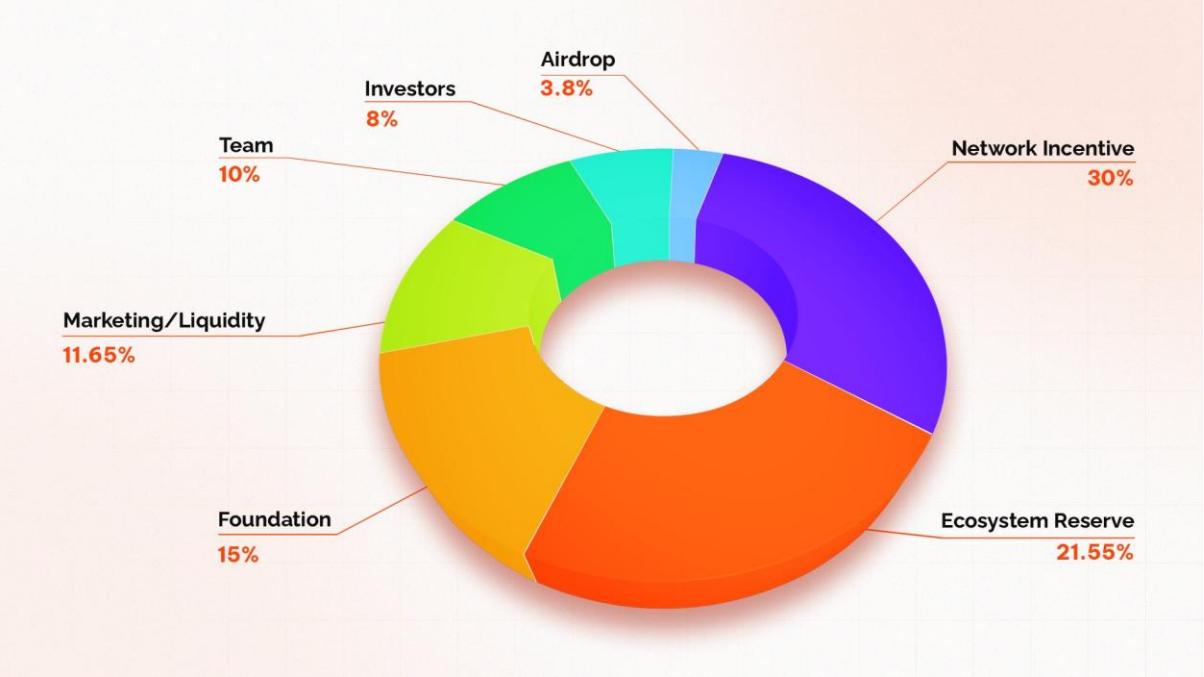
[32] Native token

[33] Storage

[34] Sequencer

토큰 분배

총발행량: 1,000,000,000 ON



[ON 토큰 분배]

네트워크 인센티브: 300,000,000 ON(총발행량의 30%)

암호화 증명을 통해 안전하게 합의를 이루고 프라이버시를 보호하며 네트워크를 확장하는 검증인 및 영지식 시퀀서를 위한 인센티브로 활용됩니다.

생태계 예비분: 215,500,000 ON(총발행량의 21.55%)

오로치 제품을 사용하는 개발자와 파트너사, 프로젝트를 유치하기 위한 보조금 프로그램, 육성 프로그램, 해커톤을 진행하는 데 활용되어 생태계 성장을 촉진합니다. 또한 연구 및 증명자/검증인 보상 풀의 자금으로도 활용됩니다.

재단: 150,000,000 ON(총발행량의 15%)

독립 조직인 오로치 재단에 의해 관리되며 프로토콜의 장기적인 대응력을 강화하기 위한 연구, 정형 검증[35], 유동성 안전 장치, 비상 자금 등으로 사용됩니다.

---

[35] Formal verification

마케팅/유동성: 116,500,000 ON(총발행량의 11.65%)

앰배서더, 교육, 이벤트, 마케팅 캠페인, 번역, 사용자 인센티브를 통해 커뮤니티 참여를 활성화하고 인지도를 제고하는 데 활용됩니다.

팀: 100,000,000 ON(총발행량의 10%)

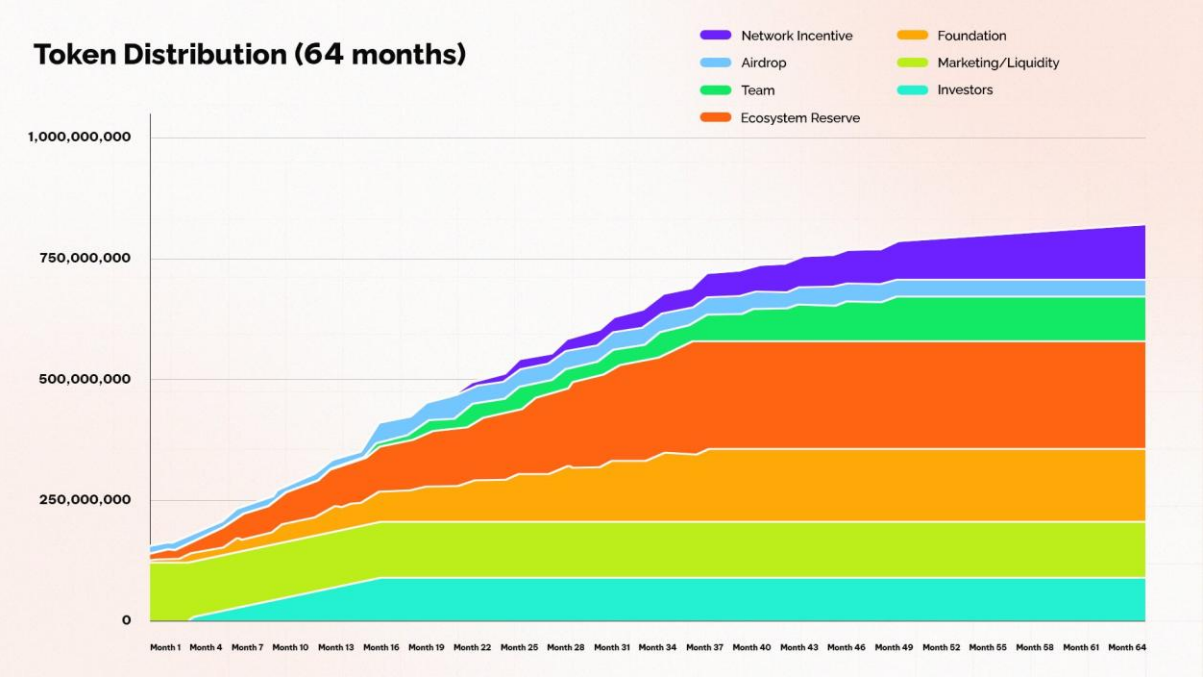
오로치의 핵심 기여자에게 보상으로 제공되어 검증 가능 데이터 인프라를 고도화하기 위한 우수 인재를 확보하는 데 활용됩니다.

투자자: 80,000,000 ON(총발행량의 8%)

신속한 연구 개발 및 배포를 지원하는 전략적 파트너에게 분배되어 네트워크의 성공을 위한 장기적인 협력을 유도하는 데 활용됩니다.

에어드랍[36]: 38,000,000 ON(총발행량의 3.8%)

초기 증명자, 앰배서더, 커뮤니티 지지자에게 거버넌스 영향력과 네트워크 참여 권리를 제공하는 데 활용됩니다.



[ON 토큰 유통 일정]

---

[36] Airdrop

로드맵

오로치네트워크는 별도 로드맵을 공지하고 있지 않으나, 공식 홈페이지, 블로그 및 X(구 트위터)를 통해 사업 현황에 대한 공지를 상시로 진행하고 있습니다.

- 홈페이지: https://orochi.network/
- 블로그: https://orochi.network/blog
- X(구 트위터): https://x.com/OrochiNetwork

*상기 링크는 작성일 기준으로 유효한 링크이며 변경될 가능성이 있습니다.