

지케이싱크(ZKsync)

해당 번역본은 이용자가 디지털자산 관련 정보를 편리하게 확인할 수 있도록
단순 참고용으로 번역된 것이며, 투자 권유를 목적으로 하지 않습니다.
그 내용이 정확하지 않을 수 있으므로 정확한 정보 습득을 위해서는
원문을 참고하시거나 원문 작성 주체 측에 문의하시기 바랍니다.
두나무는 해당 번역본 내용의 진실성 및 정확성을 보장하지 않고,
제공된 정보에 의한 투자 결과에 대하여 어떠한 책임도 지지 않으며,
투자 손실은 투자자에게 귀속됩니다

ZKsync 프로토콜 개요

ZK 롤업(Rollup)에 대해 알아보기

ZKsync는 ZK Stack을 기반으로 구축된 상호 운용 가능한 영지식(Zero-Knowledge, ZK) L2 롤업과
밸리디움(Validium) 네트워크를 생성할 수 있도록 설계된 프로토콜이다.

이 문서는 프로토콜의 아키텍처 개요를 제공하며, 모듈형 설계가 어떻게 여러 상호 연결된 체인의 개발을 지
원하는지를 중점적으로 다룬다.

이러한 체인들은 함께 이더리움의 확장성, 보안성, 그리고 사용성을 강화하면서도 탈중앙화를 훼손하지 않는
다.

롤업(Rollup)이란 무엇인가?

롤업은 트랜잭션 데이터를 오프체인(off-chain)에서 처리 및 저장하면서도, 그 데이터의 무결성과 가용성
을 메인체인에 보장하는 블록체인 확장성 솔루션이다.

이 방식을 통해 롤업은 보안을 유지하면서도 트랜잭션 처리량을 크게 향상시킨다.

롤업에는 주로 두 가지 유형이 있다: 옵티미스틱 롤업(Optimistic Rollup)과 영지식(ZK) 롤업이다.

ZKsync 체인은 후자를 사용하며, 암호학적 증명(cryptographic proof)을 통해 보안성과 효율성을 확
보한다.

작동 방식과 그 이유

이더리움의 탈중앙화 네트워크는 검증자(validator) 수가 늘어나더라도 처리 용량이 비례하여 증가하지 않기 때문에 트랜잭션 처리량이 제한적이다.

즉, 각 검증자가 동일한 트랜잭션을 모두 검증해야 하므로 병목 현상이 발생한다.

반면, Web2에서는 서버 수가 증가함에 따라 네트워크의 요청 처리 능력이 선형적으로 증가하여 확장성이 향상된다.

롤업의 개념은 이러한 블록체인 확장성 문제를 해결하기 위해 연산을 오프체인에서 수행하고, 그 결과만 이더리움으로 전송하는 방식으로 접근한다.

특히 ZK 롤업은 실행 결과와 함께 유효성 증명(Validity proof)을 제출하여, 각 트랜잭션을 다시 실행하는 것보다 훨씬 저렴한 비용으로 검증을 가능하게 한다.

데이터 가용성(Data Availability, DA) 문제

롤업의 무결성과 보안을 보장하기 위해 가장 중요한 요소 중 하나는 데이터 가용성(DA) 문제를 해결하는 것이다.

만약 이더리움의 관찰자들이 롤업의 상태를 알 수 없다면, 검증자(증앙화 혹은 탈중앙화)가 처리를 중단한 상황에서 신뢰할 수 있는 검증자에 의존하지 않고는 상태 전이를 수행할 수 없게 된다.

그러나 데이터가 항상 관찰자에게 공개되어 있다면, 신뢰된 검증자가 작동을 멈추더라도 네트워크 상태를 복원하고 처리를 계속할 수 있다.

데이터 가용성 문제에 대한 자세한 내용은 다음 링크를 참고하라: [Ethereum Data Availability](#).

ZK 증명(ZK proof)

영지식 증명(Zero-Knowledge Proof, ZKP)은 검증 가능한 프로그램을 실행할 수 있는 방법을 제공하며, 온체인에서 zk 증명을 검증하는 비용이 매우 낮다.

ZKsync의 맥락에서 ZKP는 트랜잭션을 다시 실행하지 않고도 그 실행의 정확성을 검증할 수 있도록 한다.

ZKsync 구성 요소

ZKsync 프로토콜은 다음과 같은 핵심 구성 요소로 이루어진다:

- **노드 구현(Node Implementation):**

이 구성 요소는 사용자로부터 트랜잭션을 수신하고 처리하는 역할을 담당한다.

오프체인 상태를 유지하며 트랜잭션을 배치(batch)로 집계하고, 밀봉된 배치를 온체인으로 전송한다.

- **ZK 회로(ZK Circuits):**

이는 검증 가능한 연산 논리를 수학적으로 표현한 복잡한 구조물이다.

어떤 것이 유효한 증명으로 검증될 수 있는지를 결정하며,

특히 ZKsync에서는 트랜잭션이 어떻게 실행되는지를 정의하는 연산 규칙을 포함한다.

- **프루버(Prover):**

프루버는 오프체인에서 처리된 트랜잭션의 정확성을 입증하는 암호학적 증명(cryptographic

proof)을 생성한다.

이 증명은 이후 이더리움 상에서 검증되며, 이를 통해 오직 유효한 트랜잭션만이 승인되도록 보장한다.

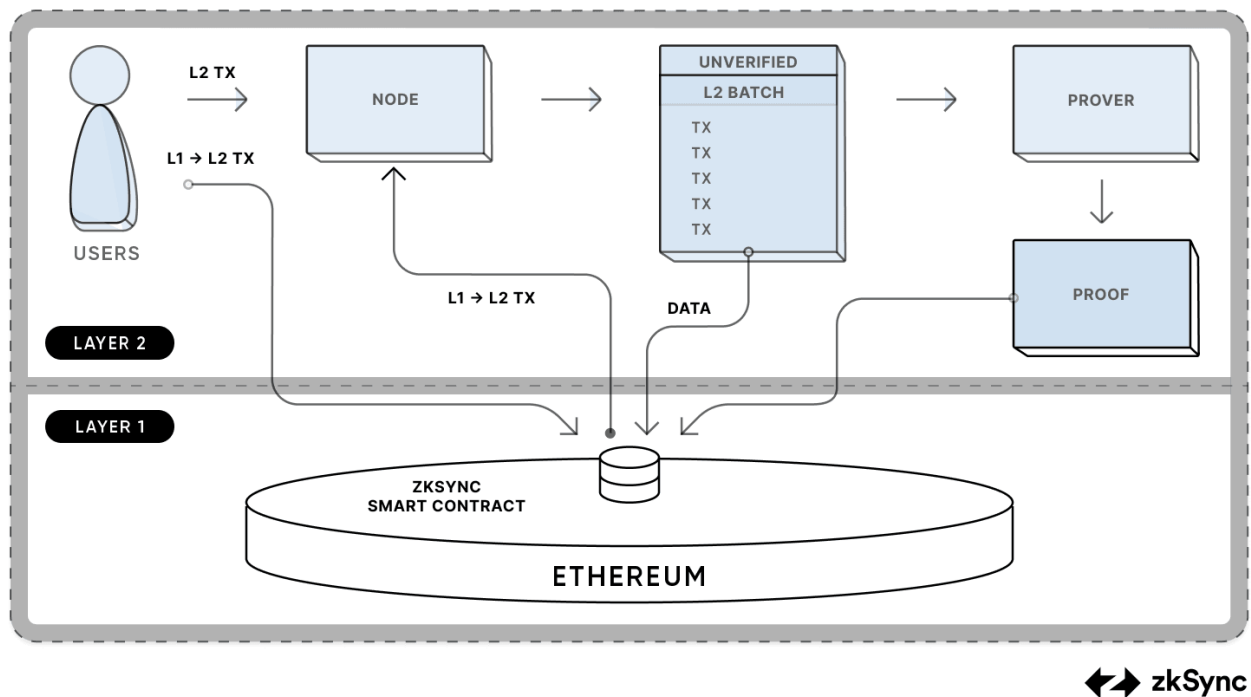
- **스마트 컨트랙트(Smart Contracts):**

이는 zkRollup의 온체인 구성 요소이다.

프루버가 제출한 증명을 검증하고, 그 결과에 따라 이더리움 블록체인의 상태를 업데이트한다.

또한 이더리움과 ZKsync 간의 예치(Deposit), 출금(Withdrawal), 계층 간 메시징(Cross-layer messaging) 같은 상호작용을 처리한다.

LAYER 2 COMPONENTS



추가적인 맥락이나 이해를 위해 다음 자료를 참고하라:

- **노드 구현(Node Implementation):** <https://github.com/matter-labs/zksync-os-server>
- **ZK 회로(ZK Circuits):** <https://github.com/matter-labs/zksync-protocol>
- **프루버(Prover):** <https://github.com/matter-labs/zksync-airbender>

ZKsync 체인(Chain)

ZKsync 체인은 이더리움의 롤업 중심 로드맵(rollup-centric roadmap)을 이어가는 구성 요소이다. 이더리움은 데이터 가용성(DA)과 증명 검증을 통해 보안을 제공하지만, 실행(execution) 책임은 롤업에 위임된다.

최적의 사용자 경험(UX)을 제공하기 위해서는 체인 간 상호 운용성과 자산의 자유로운 이동을 해결해야 한

다.
이를 위해 L1(이더리움 메인체인)에 존재하는 **공유 브리지 컨트랙트(Shared Bridge Contract)**를 사용하며,
이 컨트랙트는 모든 ZKsync 체인을 위한 이더(Ether)와 ERC20 토큰을 보관한다(사용자 정의 브리지 구현도 여전히 가능하다).

공유 브리지를 통해 각 체인은 동일한 체인 유형 관리자(Chain Type Manager, CTM) 컨트랙트에 의해 관리되며,
동일한 가상머신(VM)과 증명 시스템을 사용하기 때문에 상호 신뢰가 가능하다.

자세한 내용은 ZKsync Chains 페이지를 참조하라.

ZKsync OS 개요

ZKsync OS 소개

실행 환경(Running Environments)

앞서 언급했듯이, ZKsync OS에는 두 가지 실행 타겟(target)이 존재한다.
그러나 이는 단순한 컴파일 타겟일 뿐만 아니라, 시스템의 일부 기본 요소(primitives)가 어떻게 처리되는지를 결정하는 개념이기도 하다.

두 가지 실행 환경은 다음과 같다:

- 순방향 실행 모드(Forward Running Mode):**
이 모드는 시퀀서(sequencer)에서 사용된다.
이 모드에서는 코드가 일반적인 OS 환경에서 실행된다고 가정하므로,
기본 메모리 할당자(default memory allocator)를 그대로 사용할 수 있다(이는 OS의 일부이기 때문이다).
비결정성(non-determinism)의 소스로는 Oracle의 Rust 구현체를 부트로더(bootloader) 입력으로 전달할 수 있다.
또한, 이 모드에서는 일부 코드(예: 스토리지 읽기를 위한 머클 증명 검증)는 생략될 수도 있다.
- 증명 실행 모드(Proving Running Mode):**
이 모드는 증명(proof) 생성 과정에서 사용된다.
코드가 OS가 없는 순수 RISC-V 플랫폼에서 실행되므로, 메모리 관리는 수동으로 처리되어야 한다.
또한 표준적인 비결정성 소스가 존재하지 않기 때문에, 외부 데이터를 RISC-V 머신에 전달할 때 특별한 주의가 필요하다.
모든 동작은 완전히 결정적(deterministic)이고, 검증 가능(provable)해야 한다.

시스템 자원(System Resources)

ZKsync OS에서는 연산(특히 증명 생성) 및 데이터 사용량 모두를 제한하고 이에 대해 비용을 부과하기 위해

“리소스(resources)” 개념을 도입한다.

이는 단순해 보이지만 실제로는 훨씬 복잡한 문제다.

ZKsync OS는 EVM 가스 모델과 동등(EVM gas-equivalent)하도록 설계되어 있으며, 즉 EVM 코드 실행이 이더리움의 가스 스케줄과 동일한 규칙을 따라야 한다.

그러나 EVM의 가스 스케줄은 ZK 증명 생성의 실제 비용을 정확히 반영하지 못한다.

이 불일치를 해결하기 위해 ZKsync OS는 이중 회계(double accounting)을 도입한다.

이를 통해 실행 환경(Execution Environment, EE)에서 EVM 가스에 상응하는 가스 추적과, 증명 생성 비용을 모델링하는 “네이티브(native)” 계산 자원을 동시에 추적한다.

L1 통합(L1 Integration)

ZKsync OS는 상태 전이(state transition)의 정확성을 정산 레이어(settlement layer, 여기서는 간단히 L1이라 부른다)에서 검증해야 하는 ZK 롤업(ZK rollup) 및 밸리디움(validium) 환경에서 사용하도록 설계되었다.

구체적으로, 상태 커밋먼트(state commitment)는 L1에 저장된다.

각 블록(block) 또는 배치(batch)에 대해, 주어진 입력 집합에 따라 알려진 L1 상태 커밋먼트에서 새로운 커밋먼트로 올바른 상태 전이가 발생했음을 검증하기 위한 증명이 생성된다.

따라서 상태 전이 이전(pre)과 이후(post)의 상태는 ZK 증명의 공개 입력(public input, 또는 preimage)에 포함되어야 한다.

또한 공개 입력(public input)에는 다음과 같은 구성 요소들이 포함된다:

- 메시징(Messaging)
- 데이터 가용성(Data Availability, DA) 검증
- 입력(Input) 검증

ZKsync OS는 또한 L1과 L2 간 신뢰 없는(trustless) 통신을 가능하게 하는 메시징 메커니즘을 포함한다.

이는 [EraVM](#)과 완전히 호환되며, $L1 \rightarrow L2$ 트랜잭션 및 $L2 \rightarrow L1$ 메시지를 모두 지원한다.

ZKsync OS 개요

ZKsync OS 소개

실행 환경

앞서 언급했듯이, ZKsync OS에는 두 가지 타깃이 있다. 그러나 이는 단지 컴파일 타깃만을 의미하는 것이 아니라, 일부 시스템 프리미티브가 어떻게 처리되는지도 포함한다.

두 가지 실행 환경은 다음과 같다:

1. **순방향 실행 모드(Forward Running Mode):** 시퀀서에서 사용하도록 설계되었다. 이 모드에서는 코드가 일반적인 OS가 있는 플랫폼에서 실행된다고 가정하므로, 기본 메모리 할당자를 사용할 수 있다(이는 OS의 일부이기 때문이다). 비결정성의 소스로는 Oracle의 Rust 구현체를 부트로더 입력으로 전달하면 된다. 또한 이 모드에서는 일부 코드를 생략할 수 있다(예: 스토리지 읽기를 위한 머클 증명 검증).
2. **증명 실행 모드(Proving Running Mode):** 증명 생성 중에 사용하도록 설계되었다. 코드는 OS가 없는 순수 RISC-V 플랫폼에서 실행되므로, 메모리 관리를 수동으로 처리해야 한다. 또한 표준적인 비결정성 소스가 없으므로, 외부 데이터를 RISC-V 머신에 전달할 때 특별한 주의가 필요하다. 모든 동작은 완전히 결정적이며 증명 가능해야 한다.

시스템 자원

ZKsync OS에서는 연산(주로 증명)과 데이터 사용 모두를 제한하고 과금하기 위해 “리소스” 개념이 필요하다. 이는 처음 보기에 비해 더 복잡한 문제다. ZKsync OS는 EVM 가스와 동등하도록 설계되었으며, 이는 EVM 코드 실행이 이더리움과 동일한 가스 스케줄을 따라야 함을 의미한다.

그러나 EVM 가스 스케줄은 ZK 증명 생성 비용을 정확히 반영하지 못한다. 이 불일치를 해결하기 위해, ZKsync OS는 이중 회계(double accounting)를 도입하여 EVM 가스에 상응하는 실행 환경(EE) 가스와, 증명 비용을 모델링하는 “네이티브” 계산 자원을 모두 추적한다.

L1 통합

ZKsync OS는 상태 전이의 정확성이 결제 레이어(간단히 L1이라 지칭함)에서 검증되어야 하는 ZK 롤업과 밸리디움에서 사용되도록 설계되었다.

구체적으로, 상태 커밋먼트는 L1에 저장된다. 각 블록 또는 배치에 대해, 알려진 L1 상태 커밋먼트에서 특정 입력 집합에 기반하여 새로운 커밋먼트로 유효한 상태 전이가 발생했음을 검증하는 증명이 생성된다. 이는 전이 전과 전이 후의 상태가 ZK 증명의 공개 입력(또는 프리이미지)에 포함되어야 함을 의미한다.

추가로, 공개 입력에는 다음에 필요한 다른 구성 요소가 포함된다:

- 메시징
- 데이터 가용성(DA) 검증
- 입력 검증

ZKsync OS에는 L1과 L2 간 신뢰 없는 통신을 가능하게 하는 메시징 메커니즘도 포함되어 있으며, 이는 EraVM과 완전히 호환된다. 여기에는 L1에서 L2로의 트랜잭션과 L2에서 L1로의 메시지가 포함된다.

ZK Nation에 오신 것을 환영한다

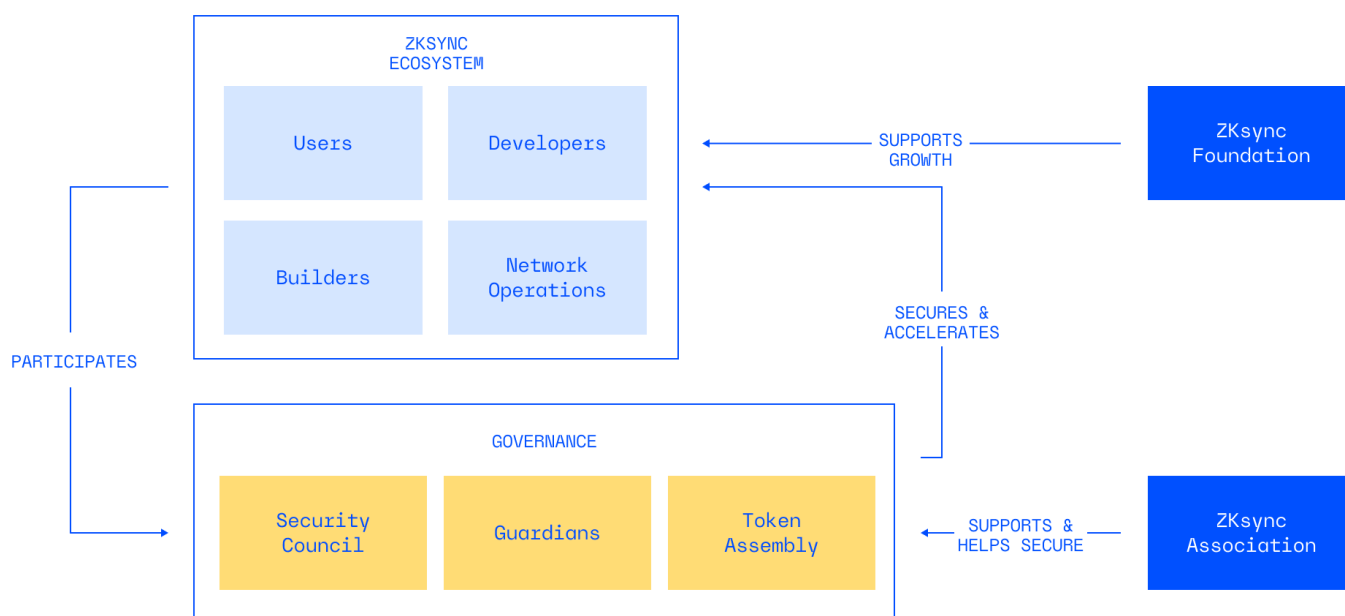
ZK Nation은 퍼블릭과 프라이빗 원장을 하나의 확장 가능한 신뢰 네트워크로 연결하여 ZKsync 프로토콜을 거버넌스하고 성장시키기 위해 체인, 빌더, 운영자를 결집한다.

이 문서에서는 ZK Nation, ZK 토큰, ZKsync 거버넌스 시스템, 그리고 자주 묻는 질문에 대한 정보를 확인할 수 있다.

생태계 개요

이 생태계 개요는 ZK Nation 내의 핵심 참여자들을 강조하고, 이들이 상호 작용하고 협업하여 서로를 어떻게 지원하는지를 보여준다.

거버넌스 기구, 지원 조직, 그리고 거버넌스 절차에 대해서는 **ZKsync Governance Procedures: Overview** 페이지를 참고하라.



ZK Nation 링크

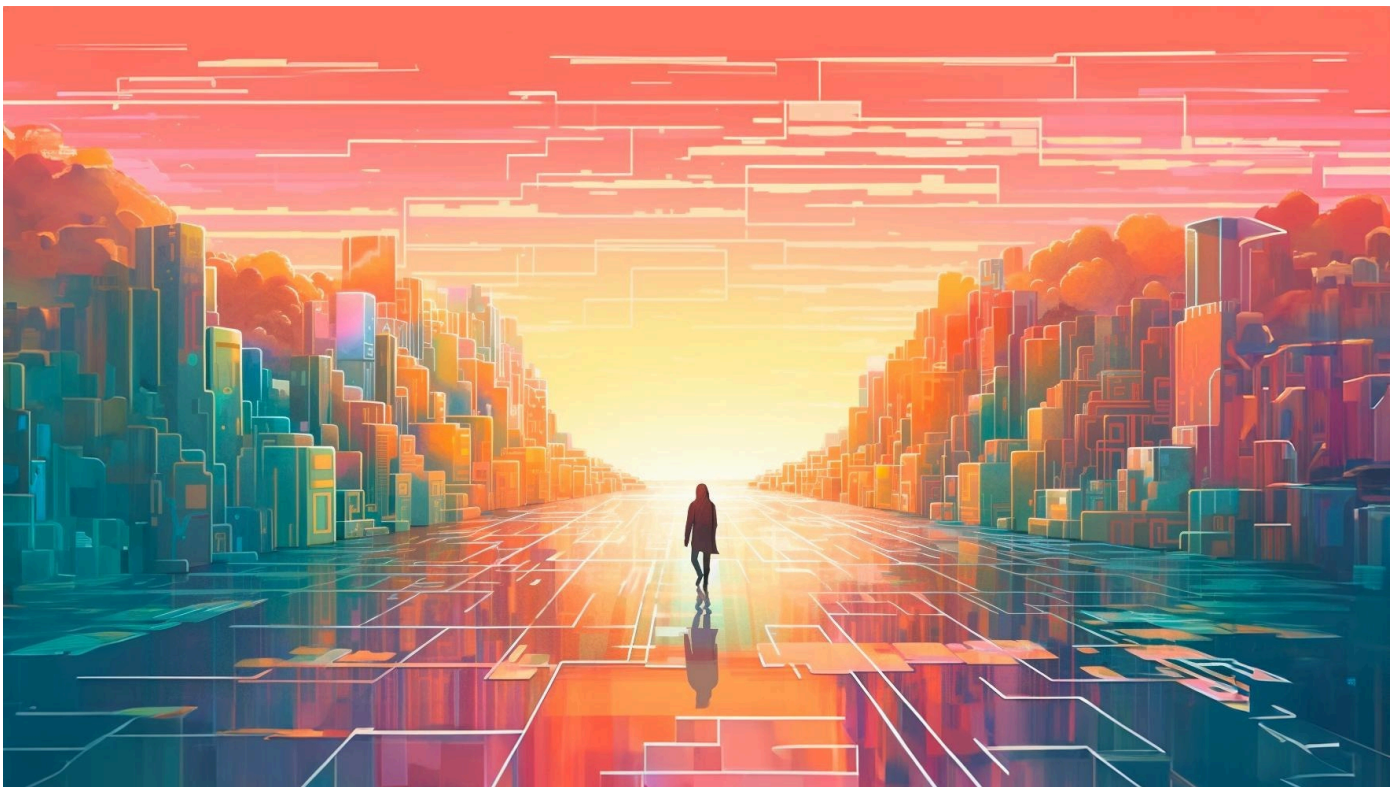
- [0x5A7d6b2F92C77FAD6CCaBd7EE0624E64907Eaf3E](https://explorer.zkscan.io/address/0x5A7d6b2F92C77FAD6CCaBd7EE0624E64907Eaf3E)에서 ZK 토큰 컨트랙트를 확인하라
- delegate.zknation.io에서 ZK 토큰 의결권을 위임하라
- <https://github.com/ZKsync-Association/zk-governance>에서 ZKsync 거버넌스 컨트랙트 코드를 살펴보라
- zknation.io에서 ZK Nation 홈페이지를 방문하라
- blog.zknation.io에서 ZK Nation 공지사항을 읽어보라

주요 용어

- **ZK Nation:** ZK Nation은 ZKsync 프로토콜을 거버넌스하고 방어하며 성장시키려는 공동의 목적에 의해 움직이는 커뮤니티이다. 이는 [ZK Credo](#)를 실현하고 자유를 확장하며 의도적인 혁신을 가속하기 위해 참여하는 개인, 조직, 기술을 포괄적으로 지칭하는 용어이다.
- **ZKsync 체인:** [ZK Stack 프레임워크](#)를 사용해 구축된 완전한 커스터마이징이 가능한 자율 롤업, 밸리디움, 혹은 볼리션이다. 이들은 완전히 독립적으로 동작하면서도 ZK 게이트웨이와 L1 스마트 컨트랙트를 통해 상호 연결된다.
- **ZKsync 스택:** ZKsync 스택은 상호 운용 가능한 ZK 기반 블록체인을 커스터마이징하고 배포하기 위한 모듈형 개발자 친화적 프레임워크이다. 모든 ZKsync 체인은 ZK Stack 툴킷으로 구축되며 사용자와 유동성을 공유한다.
- **엘라스틱 네트워크(Elastic Network):** [ZK Stack 프레임워크](#) 위에 구축된 ZKsync 체인의 네트워크로, 단일 브리지허브(Bridgehub)를 통해 연결되고 프로토콜 수준에서 네이티브 상호 운용성을 갖추어 사용자와 자산의 매끄러운 이동이 가능한 구역을 형성한다.

미션 — ZK Credo

자유 → 진보 → 번영



역사는 기술이 개인의 자유를 확장하여 창의성과 혁신을 촉발하고, 그 결과 진보와 번영으로 이어졌음을 보여 준다.

초기 문명은 거래를 기록하기 위해 부기와 원장을 사용했으며, 이를 통해 개인과 공동체가 재정을 관리하고 협력할 수 있게 되었다. 인쇄술은 정보를 저렴하게 만들어 지식을 민주화했고, 비판적 사고와 과학 발전을 촉발했다.

증기기관과 기계화라는 기술적 돌파구로 구동된 산업혁명은 전례 없는 경제적·사회적 번영을 견인했다.

20세기에 암호학과 인터넷의 부상은 통신과 정보 접근을 변화시켰다. 이러한 개인의 자유 확장은 수십억 인구에게 경제적 기회를 창출했다.

오늘날 우리는 블록체인과 웹3와 함께 새로운 시대의 여명에 서 있다. 인터넷이 한때 정보의 지형을 바꿨듯이, 웹3는 디지털 소유권과 가치 교환의 판도를 바꾸고 있다. 이는 “네트워크 스테이트”와 같은 유망한 새로운 사회 조직 형태를 제시한다.

암호학 혁명의 물결은 현재진행형이다. 공개키 암호와 블록체인이 1·2차 물결을 이뤘다면, 이제 3차 물결인 ZK 혁명을 맞이하고 있다. 웹3와 결합된 ZK 혁명은 우리 공동의 미래를 재정의할 것이며, 개인의 자유를 여는 기술의 힘을 입증할 것이다.

ZK 혁명



“ZK”는 두 가지 의미를 가진 용어다. 처음에는 “Zero-Knowledge(Proofs)”를 뜻했고, 혹은 굳이 말하자면 “Zipped by Kryptography”를 의미했다. 오늘날 “ZK”는 보다 큰 개념을 담으며, 무결성(Integrity), 프라이버시(Privacy), 매직(Magic)이라는 세 속성을 포괄한다.

무결성(Integrity)

“무결성은 아무도 보고 있지 않거나 결코 알지 못하더라도 올바른 일을 하는 것이다.”

ZK는 수학, 오픈 소스, 블록체인의 근간인 “신뢰하지 말고 검증하라(don't trust, verify)”라는 정신을 반향한다. 재귀적 ZK 증명으로 어떤 규모에서도 구현되는 계산 무결성은 이 요소의 초석이다.

프라이버시(Privacy)

“전자 시대의 개방된 사회에는 프라이버시가 필수적이다.”

블록체인 영역에서 프라이버시는 기본권으로 간주되며, ZK가 고유하게 해결하는 도전과제를 제기한다. 프라이버시는 주어지는 선물이 아니라, 우리가 함께 주장하고 수호해야 할 기본권이어야 한다.

매직(Magic)

“충분히 진보한 기술은 마법과 구별되지 않는다.”

ZK는 애정 섞여 “매직 문 매스(Magic Moon Math)”라 불리는 기술의 경이로움이다. 복잡한 연산을 손쉬운 클릭으로 바꾸어 번거로움을 단순하게 만든다. 구성 요소들이 매끄럽게 동기화되는 통합 시스템을 가능하게 한다. 무엇보다, 사용자 프라이버시와 통제를 존중하면서 이러한 경이를 엮어낸다.

ZK 원칙



가치의 인터넷(Internet of Value)의 기반이 되기 위해서는, 탈중앙 네트워크가 다음 원칙을 준수해야 한다고 믿는다:

신뢰 불요성(Trustlessness). 사용자는 타인에 의존하지 않고도 트랜잭션과 네트워크 상태의 무결성을 독립적으로 검증할 수 있어야 한다.

보안성(Security). 어떤 개별 사용자에게 대한 공격도, 세계에서 가장 강력한 행위자라 하더라도, 전체 네트워크를 공격하는 것만큼 어렵고 비용이 많이 들어야 한다.

신뢰성(Reliability). 네트워크는 실패 없이 일관되고 정확하게 그 기능을 수행해야 한다.

검열 저항성(Censorship-Resistance). 사용자는 누구의 허락도 받지 않고 네트워크에서 트랜잭션을 수행할 수 있어야 한다.

프라이버시(Privacy). 사용자는 자신의 신원과 트랜잭션 세부 정보를 보호할 수 있어야 한다. 민감한 정보는 사용자의 동의 없이 네트워크 내 타인과 공유되지 않는다.

하이퍼스케일러빌리티(Hyperscalability). 네트워크는 다른 중요한 속성을 보존하면서도 상한 없이 성장할 수 있어야 한다.

접근성(Accessibility). 네트워크의 애플리케이션과 서비스는 최첨단 중앙화 대안만큼 저렴하고, 사용하기 쉬우며, 안전해야 한다.

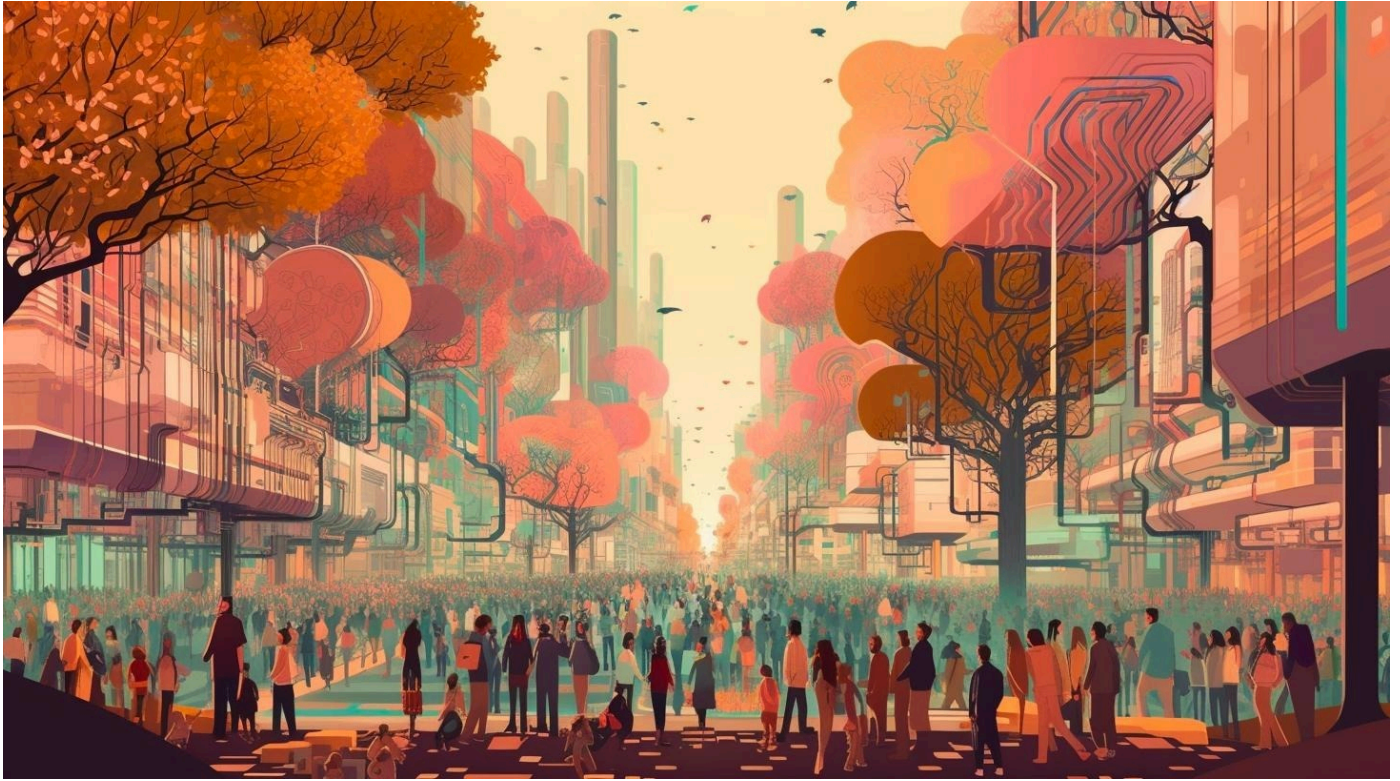
주권성(Sovereignty). 소수라 해도 어떤 사용자 집단이든 최소 비용으로 자산을 지닌 채 네트워크에서 이탈(즉, 포크)할 권리를 가져야 한다.

현재 이더리움은 가치의 인터넷의 백bones을 이루는 블록체인 네트워크라는 비전을 실현하는 데 가장 근접해 있다. 이더리움은 신뢰 불요성, 보안성, 신뢰성, 검열 저항성, 주권성을 갖춘 네트워크다. 그러나 아직 프라이버시, 하이퍼스케일러빌리티, 접근성이라는 나머지 전제조건을 충족하지는 못한다.

ZK의 매직을 통해, 이더리움 위의 웹3는 무결성을 유지하면서 프라이버시의 보루가 되고 무한대의 확장성을 달성할 수 있다. 이 변혁적 상태에서, 디지털 자기 소유권을 위한 접근 가능하고 저렴한 안식처가 될 것이다.

이는 ZK 비전과 부합하며, 전 세계 개인을 위치와 무관하게 역량 강화할 것이다. 이러한 역량을 열어젖힘으로써, 자유와 진보, 번영의 새로운 물결이 전 세계의 삶에 영향을 미칠 것이다.

집단적 행동



ZK 원칙은 사용자의 자산과 통제를 보호하기 위해 운영자에 대한 신뢰가 필요 없는 네트워크를 가능하게 한다. 설령 볼드모트 경이 우리의 서버에 접근하더라도, 사용자의 소유권을 해치거나 자산을 통제할 수 없다.

그러나 기술은 진화하며 블록체인의도 그러하다. ZK 원칙은 기술만으로 완전히 수호될 수 없다. 지속적인 보호를 위해서는 커뮤니티가 탈중앙화라는 아리송한 개념을 깊이 받아들여야 한다.

네트워크가 앞서 언급한 모든 속성을 갖추고도 그 거버넌스가 소수 특권층의 손에 떨어진다면, 그 네트워크는 실패할 운명이다. 그 소수는 개인의 이익을 위해 규칙을 조정하며, 네트워크의 가치를 훼손할 것이다. 인터넷의 역사는 경고의 본보기다. 출발은 탈중앙화를 약속했지만, 시간이 지나며 사용자 데이터와 트래픽은 소수의 거대 기술 기업의 통제하에 놓였고, 그들의 이익에 맞게 디지털 지형이 재편되었다.

이 같은 운명을 피하기 위해, 우리는 ZK 커뮤니티가 이탈권을 도덕적 의무의 수준으로 격상시켜 강력한 주권성을 가져야 한다고 믿는다. 네트워크가 그 원칙에서 벗어날 때, 커뮤니티는 단결해 이러한 가치를 지키기 위해 새로운 네트워크로 이주해야 한다.

이러한 가치 훼손을 식별하는 일은 간단하지 않다. 억압은 흔히 미묘하며, 천천히 자유를 갉아먹는다. 억압자는 또한 공공연히 반대자를 처벌하여 두려움을 조성하고 집단적 무행동을 부추길 수 있다.

이러한 전술에 맞서 집단적 행동이 필수적이다. 커뮤니티는 소수자를 보호하고, 억압에 용감히 맞서는 이들을 기려야 한다. 이 집단적 약속을 커뮤니티 깊숙이 새기는 일은 가치의 인터넷에서 자유를 보존하는 데 결정적이다.

이 원칙을 실현하려면 시간과 인내가 필요하다. 점진적이고 실용적인 탈중앙화 접근이 요구된다. 단기적으로는 타협이 있을 수 있으나, 흔들림 없는 장기 비전은 변함없다: 모두의 개인적 자유를 증진하는 것이다.

디지털 자기 소유권을 옹호하는 데 굳건히 서자.

전진하자.

ZKsync 거버넌스 시스템 노스 스타

ZKsync 거버넌스 시스템의 목적

스마트 컨트랙트, 위임 포털과 같은 인터페이스, 그리고 세 가지 거버넌스 기구로 구성된 ZKsync 거버넌스 시스템의 목적은 두 가지다:

1. 프로토콜 변경과 개선에 대한 통제를 탈중앙화하여 ZKsync 프로토콜을 안전하게 보호한다
2. ZK Credo 비전(자유 —> 진보 —> 번영)을 실현하는 프로그램을 활성화한다

ZKsync 거버넌스 제안의 영향 평가

제안은 ZK Credo의 비전을 지지하는 목표 달성을 지향해야 한다. 그에 따라, 대리인과 기타 거버넌스 시스템 참여자는 각 제안의 목표와 해당 KPI를 기준으로 제안의 영향을 정의하고 평가해야 한다. 각 KPI는 제안 목표와, ZKsync 거버넌스 시스템의 목적에 명확히 연관되어야 한다.

주요 목표와 KPI:

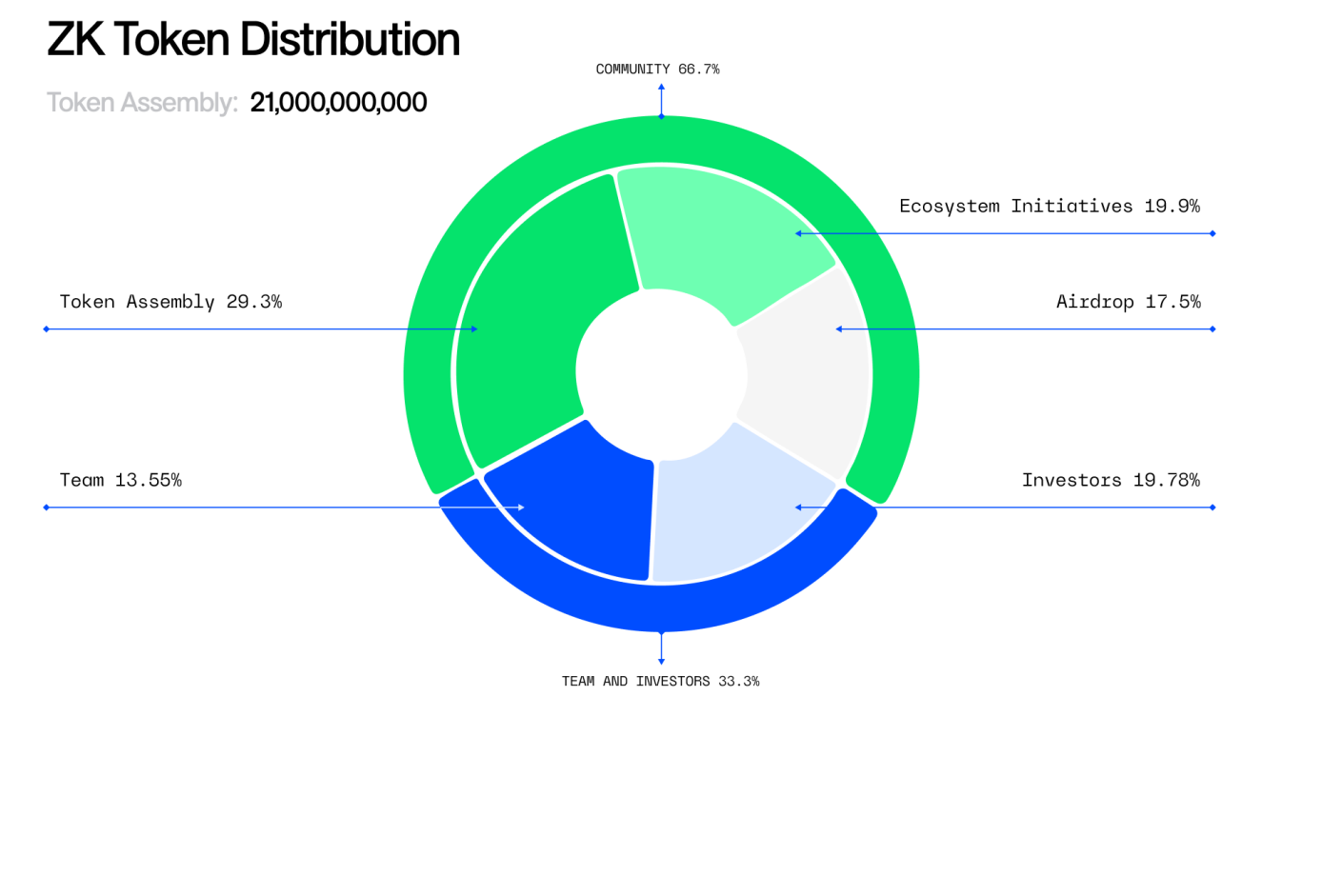
- **프로토콜 보안(Secure the Protocol):** ZKsync 프로토콜과 그 자산, 빌더, 커뮤니티는 프로토콜을 사익을 위해 장악하려는 적대적 행위자로부터 보호된다.
 - 예시 KPI: 사고 건수(목표 = 0)
- **온체인 자산 확대(Expand Onchain Assets):** ZKsync 프로토콜은 접근 가능하고 가치 있으며 다양한 온체인 자산을 보유하여, ZK 체인 내간 역동적 경제를 가능하게 한다.
 - 예시 KPI: ZKsync 체인에서 이용 가능한 자산의 총가치
- **활성 빌더 증가(Increase Active Builders):** ZKsync 프로토콜은 재능 있고 다양한, 그리고 충분히 자금 조달된 활성 빌더 네트워크를 보유하여 블록체인 및 ZK 관련 솔루션 개발을 가속한다.
 - 예시 KPI: FDV(완전 희석 가치) > \$100M인 프로젝트 수
- **ZK 커뮤니티 강화(Strengthen ZK Community):** ZKsync 프로토콜은 참여자(사용자, 아티스트, 개발자, 파트너 포함)로 구성된 참여적이고 상호 연결되며 지식이 풍부한 커뮤니티를 보유한다. 커뮤니티는 ZKsync와 ZK 기술을 사용하고 옹호한다.
 - 예시 KPI: 주간 활성 주소 수

ZK 토큰

토큰 속성

속성	값
토큰 티커	ZK
토큰 주소	0x5A7d6b2F92C77FAD6CCaBd7EE0624E64907Eaf3E
공급 상한	21,000,000,000
스냅샷	29710983
인플레이션	프로토콜 거버넌스 업그레이드를 통해 토큰 공급이 증가할 수 있다.
배포 네트워크	ZKsync Era
이더리움 메인넷으로 전송 가능	Yes

토큰 분배



카테고리	토큰 수	비율	설명
토큰 어셈블리	6,146,000,700	29.27%	토큰 어셈블리가 배분
에코시스템 이니셔티브	4,179,000,000	19.90%	ZKsync 재단이 ZKsync 생태계 성장을 지원하는 이니셔티브를 관리한다.
에어드롭	3,675,000,000	17.50%	락업이 없는 일회성 에어드롭.
투자자	4,154,642,006	19.78%	투자자 및 자문
팀	2,845,357,294	13.55%	Matter Labs 임직원
합계	21,000,000,000	100%	



투자자 및 팀 토큰 할당 수치는 2025년 6월에 업데이트된 계산을 반영하도록 수정되었다.

락업

투자자와 팀 토큰은 2024년 6월부터 2028년 6월까지 4년의 언락 기간을 가지며, 1년의 클리프를 포함한다. 2025년 6월에는 전체 공급의 3.6%가 팀 및 투자자 할당에서 언락된다. 2025년 6월 이후에는 2028년 6월까지 매월 최대 0.8%의 토큰 공급이 언락된다.

캡드 민터(Capped Minters)

대부분의 온체인 조직에서는 토큰이 출시 시 발행되어 지갑에 수동으로 보관된다. 이는 여러 문제를 야기한다. 투자나 재무 다각화 같은 금융 공학에 집중하도록 압력을 만들고, 수령자가 언제 어떤 방식으로 토큰을 받을지 결정할 권한을 앗아간다.

전체 토큰 공급을 한 번에 발행하는 대신, ZKsync는 **캡드 민터**를 사용한다. 캡드 민터는 “적시 발행(just-in-time minting)”을 가능하게 하는 고유한 스마트 컨트랙트다. 각 캡드 민터 컨트랙트는 발행할 수 있는 토큰의 최대치(캡)를 부여받는다. 캡드 민터의 민터 역할을 가진 자는 지정된 최대치까지, 원하는 시점에 해당 공급에서 토큰을 발행할 수 있다. 이 설계는 대규모 금고(treasury)에 수반되는 위험을 제거하고, 토큰 관리의 주체성을 캡드 민터와 그 지정 관리자에게 이전한다.

이는 [블록 탐색기](#)에 표시된 Max Total Supply와 프로그램된 공급 상한 21,000,000,000 사이의 차이를 설명한다. 지정된 캡드 민터가 모든 토큰을 아직 발행하지 않았기 때문이다.

ZK 토큰 출시 이후, ZKsync 재단, 에어드롭, 투자자, 그리고 Matter Labs 팀 구성원 베스팅 컨트랙트에 할당을 분배하기 위한 캡드 민터가 생성되었다. 토큰 어셈블리가 관할하는 29.3%는 캡드 민터에 있지 않으며, 단순히 ZK 토큰 컨트랙트의 잔여 물량이다. 토큰 어셈블리는 토큰 프로그램의 관리자에게 민팅 권한을 부여한다. [토큰 프로그램 제안\(Token Program Proposals\)](#)에 대해 더 읽어보라.

i 최신 버전의 ZK 캡드 민터 (현재 V2) 컨트랙트와 팩토리에 대해 더 읽어보라. 배포가 완료되면, 해당 컨트랙트와 관리자 멀티시그(해당되는 경우)는 보안위원회(Security Council) 구성원 또는 신뢰할 수 있는 보안 회사에 의해 최소 한 번의 보안 검토를 받아야 한다.

10월 24일부터 10월 30일 사이에, 팀 토큰이 한 수탁(custody) 제공업체에서 다른 업체로 이전되었다. 이 토큰들은 위의 락업(Lock Ups) 항목의 세부 사항에 따라 언락되기 시작했다.

ZKsync 거버넌스 101

ZKsync 거버넌스 시스템은 무엇을 거버넌스하는가?

자세한 내용은 [ZKsync Governance Procedures: Overview](#) 및 [Schedule 1: Standard Governance Procedures](#)를 참조하라.

- **ZKsync 프로토콜:** ZKsync 거버넌스 시스템은 ZKsync 프로토콜을 거버넌스한다. ZKsync 프로토콜은 이더리움과 ZKsync 체인 자체(L2 시스템 컨트랙트)에 배포된 일련의 연결된 스마트 컨트랙트로 구성된다. ZKsync 체인(예: Era, Abstract, Lens)은 ZKsync 스택 툴킷으로 구축되며 ZKsync 프로토콜로 구현된다. 프로토콜 업그레이드는 프로토콜 거버너를 통해 ZIP을 통과시켜 승인된다.
- **토큰 어셈블리 ZK 토큰 할당:** 토큰 어셈블리는 2024년 6월 토큰 출시 시 총 공급(210억 ZK)의 29.3%에 대한 통제를 부여받았다. 이 할당은 [ZK Credo](#)와 [ZKsync Governance North Star](#)에 부합하는 이니셔티브에 자금을 제공하는 데 목적이 있다. ZK 배분 제안은 토큰 거버너를 통해 TPP를 통과시켜 승인된다.
- **거버넌스 자문 제안(GAPs)을 통한 “GovOps”:** GAP는 온체인 토큰 어셈블리 대리인 투표를 통해 오프체인 의사결정에 정당성을 부여한다(예: 표준 및 정책 비준, 선거).

ZKsync 거버넌스의 구성 요소

ZKsync 거버넌스 시스템에는 3개의 거버너, 3가지 제안 유형, 3개의 거버넌스 기구가 있다.

3 거버너(Governors)

ZKsync 거버넌스 시스템은 세 가지 OZ 표준 거버너(프로토콜 거버너, 토큰 거버너, GovOps 거버너)를 사용한다. 각 거버너에 대한 자세한 내용과 컨트랙트 주소는 [여기](#)에서 확인할 수 있다.

세 거버너를 분리함으로써 각 거버너에 대해 더 큰 유연성 및 커스터마이징이 가능해진다. 예를 들어, 프로토콜 거버너의 파라미터는 토큰 거버너의 파라미터와 다를 수 있다.

3 제안 유형(Proposal Types)

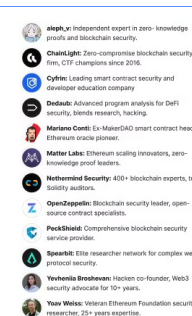
ZKsync 거버넌스 시스템에는 초기 단계에서 세 가지 유형의 제안이 있다:

- **ZKsync 개선 제안("ZIPs")**: 프로토콜 업그레이드 거버너를 통해 ZKsync 프로토콜 컨트랙트의 변경을 기술한다.
- **토큰 프로그램 제안("TPPs")**: ZKsync 생태계를 적극적으로 개발하는 참여자가 ZK 토큰을 민트/번하도록 하는 새로운 메커니즘을 활성화한다.
- **거버넌스 자문 제안("GAPs")**: ZKsync 프로토콜이나 ZK 토큰과 직접적으로 관련되지 않지만 토큰 어셈블리의 승인이 필요한 오프체인 의사결정 및 행동을 명시한다. 예: 비준, 선거, 기타 온체인 투표가 필요한 결정.

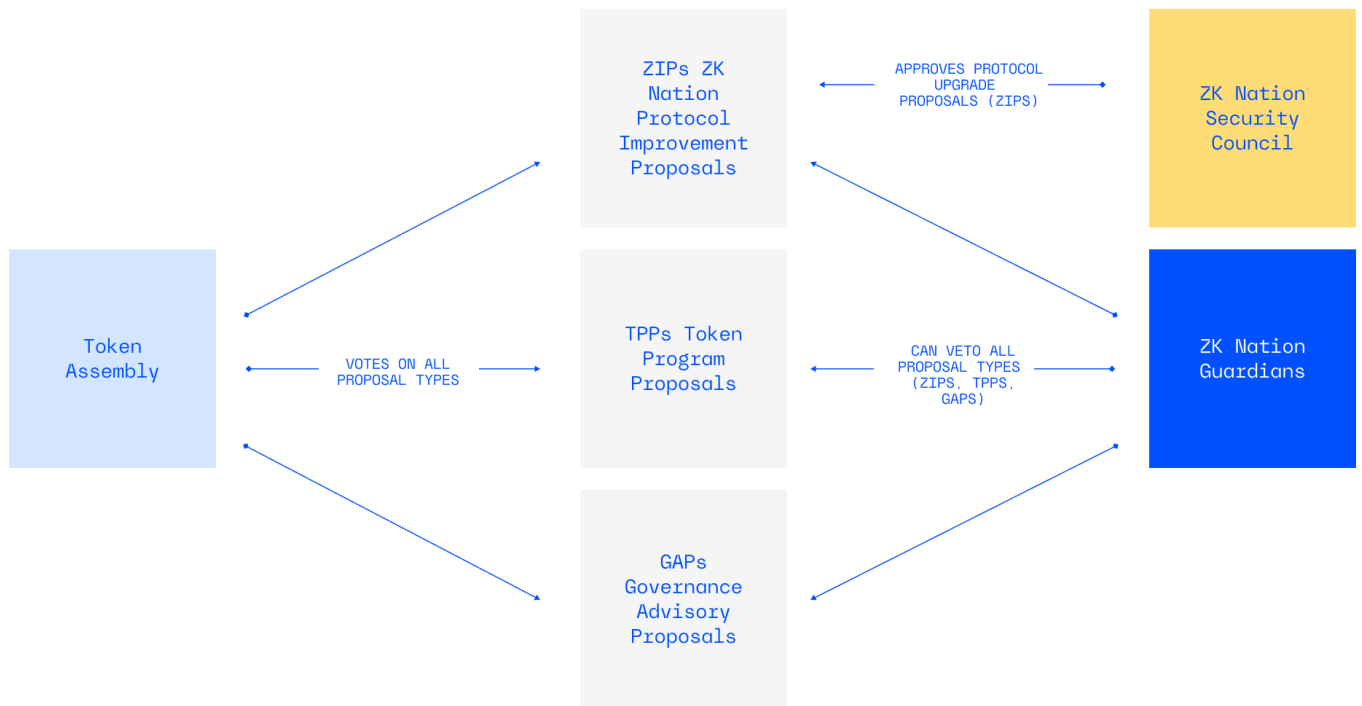
모든 제안은 온체인에서 직접 작동하는 ZKsync 거버넌스 스마트 컨트랙트에 의해 관리된다. 투표 기간 및 타임락과 같은 거버너의 파라미터는 [ZKsync Governance Procedures](#)에 명시되어 있다.

3 거버넌스 기구(Governance Bodies)

ZKsync 거버넌스 시스템은 세 가지 거버넌스 기구(토큰 어셈블리, ZKsync 보안위원회, ZKsync 가디언)에 의해 거버넌스된다. 세 기구에 대한 자세한 내용은 [여기](#)를 참조하라.

Token Assembly	Security Council	Guardians
Delegates 64k+	Token Holders 370k+	 Security Council members list including: shay2k, Chainlight, Cyfrin, Dedee, Martino Cantù, Matter Labs, Hethermind Security, OpenZeppelin, PeckShield, Spencer, Yevhenia Broshchuk, Yusei Wilson.

각 거버넌스 기구는 제안 유형과 어떻게 상호작용하는가?



ZKsync 거버넌스는 어디에 배포되어 있는가?

i 모든 관련 거버넌스 컨트랙트 주소는 [여기](#)에서 확인하라. 소스 코드는 [zk-governance 레포](#)에서 제공된다.

ZK 토큰은 Era에 배포되어 있다. 더 자세한 내용은 [여기](#)를 읽어보라. 모든 거버너 컨트랙트는 Era와 이더리움에 배포되어 있다.

- Era: 토큰 어셈블리가 제안에 대해 투표할 수 있게 하는 거버너 컨트랙트.
 - ZkToken Governor
 - ZkProtocol Governor
 - ZkGovOps Governor
- 이더리움: ZKsync 개선 제안(ZIPs)의 L1 실행을 가능하게 하는 컨트랙트
 - Protocol Upgrade Handler
 - Emergency Upgrade Board - 모든 거버넌스 기구(ZkProtocolGovernor 투표 결과, 보안위원회, 가디언, 재단)의 승인을 수락하고 업그레이드를 수행하는 컨트랙트.

ZKsync 협회는 모든 거버넌스 컨트랙트 배포를 담당했다. 이는 ZKsync 협회가 거버넌스 시스템의 “유틸리티 제공자(utility provider)”로 간주되는 이유 중 하나다.

ZKsync에서 거버넌스를 통한 토큰 할당은 다른 온체인 조직과 어떻게 다른가?

캡드 민터(Capped Minters)

ZK 토큰 페이지에 설명된 바와 같이, 모든 ZK 토큰이 출시 시 발행된 것은 아니다. ZK 토큰의 총 공급은 ZK 토큰 컨트랙트에서 관리된다. ZKsync는 새로운 ZK 토큰의 발행 요청을 위해 **캡드 민터** 컨트랙트를 사용하며, 이를 통해 “적시 발행”이 가능하다.

각 캡드 민터는 발행할 수 있는 토큰의 최대치를 부여받는다. 캡드 민터 컨트랙트에서 민터 역할을 가진 누구든 지정된 최대치까지, 원하는 시점에 그 공급에서 토큰을 발행할 수 있다. 이 설계는 대규모 금고에 따른 위험을 제거하고, 토큰 관리의 주체성을 캡드 민터에게 이전한다.

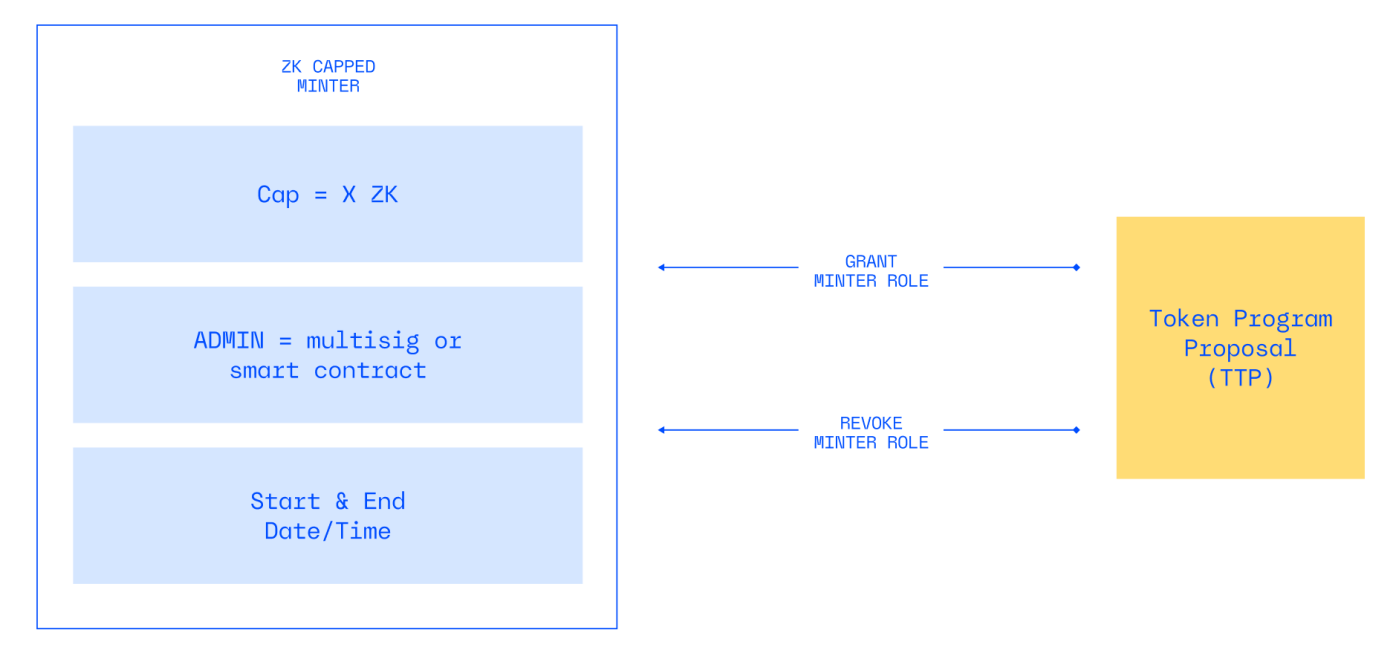
토큰 프로그램 제안(TPPs)

ZKsync 거버넌스 프레임워크에서 **토큰 프로그램 제안(TPPs)**은 지정된 캡드 민터에게 ZK 토큰의 민트/번 권한을 부여하고, 새로운 토큰 메커니즘을 활성화하는 데 사용된다.

하나의 프로그램은 하나 이상의 캡드 민터를 가질 수 있다. 또한 “부모” 캡드 민터 아래에 “자식” 캡드 민터를 중첩하는 것도 가능하다. 캡드 민터 V2 컨트랙트에 대한 자세한 내용은 여기에서 확인하라.

프로그램용 캡드 민터는 TPP가 온체인에 제출되기 전에 배포되어야 한다. 캡드 민터는 배포 시 관리자, 캡, 시작 및 종료 시간을 설정할 수 있다. V2 팩토리에서 캡드 민터 배포 방법은 여기에서 더 알아보라.

TPP가 토큰 어셈블리를 통해 성공적으로 통과되면, 캡드 민터는 ZK 토큰 컨트랙트로부터 MINTER 역할을 부여받는다.



토큰 프로그램 표준(Token Programs Standards)

토큰 프로그램 설계 표준은 다른 생태계의 자금 지원 제안과 다르다. 토큰 프로그램 표준의 핵심 요소는 다음과 같다:

- 거버넌스 노스스타 지표 / 토큰 어셈블리 우선순위(GAP-1 참조) 지원
- 온체인, 검증 가능한 지표에 대한 보상

- 배분의 자동화 > 수작업 실행에 대한 의존 축소
- 동일한 목표/지표를 향해 작업하는 다수 참여자에 대한 보상 > 특정 단일 당사자에 대한 보상

토큰 프로그램과 토큰 메커니즘에 대해서는 이 [TPP FAQ](#)와 문서의 [TPP 가이드라인](#)을 참고하라.

ZK 투표 권한 위임(Delegating ZK Voting Power)

ZK 토키는 위임 과정을 통해 참여자에게 투표 권한을 제공하기 위해 ZKsync 거버넌스 시스템에서 사용된다. 각 ZK 토키는 1표를 가진다.

ZK 토한의 투표 권한을 활성화하려면, 토한 보유자는 자신의 토한의 투표 권한을 ZKsync 주소로 위임해야 한다. 이 주소는 자신의 주소일 수도 있고 제3자의 주소일 수도 있다. 한 주소가 투표 권한을 위임받으면, 해당 주소의 컨트롤러는 거버넌스 제안에 투표할 수 있는 대리인(Delegate)이 된다.

위임 작동 방식

- 토한 투표 권한의 위임은 ZK 토한의 소유권을 변경하지 않으며, 단지 ZK 토한의 투표 권한을 활성화하고 토한 보유자가 선택한 주소에 그 권한을 부여할 뿐이다.
- 위임은 토한 보유자가 언제든지 delegate.zknation.io에서 변경할 수 있다. 일단 토한 투표 권한이 위임되면, 위임이 변경되거나 토한이 다른 주소로 매도/이전될 때까지 위임 상태가 유지된다.
- 위임은 여러 주소로 분할할 수 없다. 한 번 위임하면, 한 지갑이 보유한 모든 투표 권한은 단일 주소로 위임된다.
- ZK 토한 투표 권한은 지갑 소유자만 위임할 수 있다. 중앙화 거래소 지갑에 보관된 토한은 위임할 수 없다.
- 6월 15일(토) 11:59pm UTC 이전에 프로필을 생성한 대리인은 ZK 토한 클레임 플로우에 포함될 고려 대상이 된다.

위임이 중요한 이유

위임은 ZK 토한의 투표 권한을 활성화한다. 생태계가 정족수 충족과 거버넌스 제안 승인에 적극적인 대리인 기반을 필요로 하는 경우가 있다.

위임을 통해, ZK 토한을 보유하지 않은 사람도 직접 ZK 토한을 취득하지 않고 투표 권한을 가질 수 있다. 이는 ZKsync 거버넌스 참여를 증가시킨다.

대리인으로 참여하는 데 관심이 있다면, [Getting Started as a ZKsync Delegate](#)를 방문해 더 많은 정보를 확인하라.

거버넌스 포털을 통한 위임

- vote.zknation.io를 방문
- 지갑을 연결하고, 표시되면 로그인
- ZKsync Era 메인넷 네트워크에 있는지 확인
- 화면 오른쪽의 "Delegate" 버튼 선택
- 위임 대상 선택: "Myself" 또는 "Someone else"
- 본인에게 위임하는 경우, 트랜잭션에 서명하여 셀프 위임 실행
- 다른 주소에 위임하는 경우, 해당 주소를 입력하고 트랜잭션에 서명하여 위임 실행

Safe UI를 통한 위임

- [Safe 지갑](#)에 로그인하고 좌측 상단에서 "New transaction"을 선택한다.
- "Transaction Builder"를 선택한다.
- ZK 토큰 컨트랙트를 입력한다. 모든 거버넌스 컨트랙트는 [ZKsync Governance Cotnract Addresses](#) 페이지에서 확인할 수 있다. 주소를 입력하면 ABI가 자동으로 로드되어야 한다.
- 페이지를 아래로 스크롤하여 *Contract Method Selector* 입력값을 `delegate`로 변경한다.
- 위임하려는 대리인의 주소(본인 또는 다른 대리인)를 입력한다.
- "Add new transaction"을 선택한다.
- 우측 상단의 "Create branch"를 선택하고 Safe UI의 안내에 따라 트랜잭션을 검토 및 실행한다.

Tally에서 투표 권한을 위임하는 방법에 대한 자세한 내용은 [이 가이드](#)를 참조하라.

ZKsync 거버넌스 절차: 개요

2024년 9월 12일자 버전

1. 소개

1. ZKsync 거버넌스 절차는 ZKsync 프로토콜의 거버넌스를 담당하는 ZKsync 거버넌스 시스템을 설명한다.
2. ZKsync 거버넌스 시스템에는 표준 및 비상 대응 절차와 함께, ZKsync 보안위원회와 ZKsync 가디언 등 거버넌스 기구에 대한 명세가 포함된다.
3. ZK 토큰은 ZKsync 거버넌스 시스템 내에서 거버넌스 제안에 대한 투표 권한을 배분하고 위임하는 데 사용되는 프로토콜 토큰이며, 본 거버넌스 절차에 기술된 프로세스에 따라 승인되는 경우 향후 추가

기능을 가질 수 있다.

1. ZK 토큰 컨트랙트는 ZKsync Era의 [0x5A7d6b2F92C77FAD6CCaBd7EE0624E64907Eaf3E](#)에 배포되어 있다.
4. ZKsync 거버넌스 시스템을 구성하는 스마트 컨트랙트, 코드 및 온체인 메커니즘에 변경이 있는 경우, 해당 변경 사항을 반영하도록 ZKsync 거버넌스 절차가 업데이트된다.
 1. ZKsync 협회는 필요에 따라 본 ZKsync 거버넌스 절차를 유저업데이트할 것으로 예상된다.
 2. 다만, ZKsync 협회는 본 거버넌스 절차의 완전성에 대한 책임을 지지 않으며, 본 절차는 ZKsync 프로토콜의 거버넌스 및 관련 프로세스에 대한 고수준이자 이해하기 쉬운 설명으로 기능하도록 의도되었다. 거버넌스 절차는 그 사양에 따라 결정론적으로 작동하는 스마트 컨트랙트, 코드 및 온체인 메커니즘과 연관되므로 불완전할 수 있다. 따라서 ZKsync 거버넌스 절차는 해당 스마트 컨트랙트, 코드 및 온체인 메커니즘에 대한 충분한 이해와 함께 읽혀야 하며, 본 절차 자체는 관련 위험, 불확실성, 부정적 사실 및 면책조항을 모두 포괄하는 포괄적 설명으로 의도되지 않았다.

2. ZKsync 프로토콜

1. ZKsync 거버넌스 시스템은 다음을 포함하되 이에 한정되지 않는 ZKsync 프로토콜 관련 스마트 컨트랙트를 거버넌스할 것으로 예상된다:
 1. 이더리움에 배포된 DiamondProxy 컨트랙트:
[0x32400084C286CF3E17e7B677ea9583e60a000324](#)
 2. 이더리움에 배포된 레거시 ZKsync ERC20 브리지:
[0x57891966931Eb4Bb6FB81430E6cE0A03AAbDe063](#)
 3. ZKsync에 배포된 ZKsync ERC20 브리지:
[0x11f943b2c77b743AB90f4A0Ae7d5A4e7FCA3E102](#)
 4. 이더리움에 배포된 ZKsync 공유 브리지:
[0xD7f9f54194C633F36CCD5F3da84ad4a1c38cB2cB](#)
 5. ZKsync에 배포된 ZKsync 비콘 프록시:
[0x1Eb710030273e529A6aD7E1e14D4e601765Ba3c6](#)
 6. 이더리움에 배포된 ZKsync 밸리데이터 타임락:
[0xa8CB082A5a689E0d594d7da1E2d72A3D63aDc1bD](#)
 7. ZKsync에 배포된 ZKsync 래핑드 이더 컨트랙트:
[0x57891966931Eb4Bb6FB81430E6cE0A03AAbDe063](#)

3. ZK Credo

1. [ZK Credo](#)는 ZKsync의 비전과 가치를 제시한다.
 1. ZK Credo에 명시된 ZKsync의 미션(스케줄 4에서 정의됨)의 수호자로서 ZKsync 가디언의 역할이 규정된다.

4. 거버넌스 기구

1. ZKsync 거버넌스 시스템에 참여하는 거버넌스 기구는 다음과 같다:

1. **토큰 어셈블리:** 토큰 어셈블리는 ZK 토큰 보유자로 구성된 거버넌스 기구로서, 자신이 보유한 ZK 토큰의 투표 권한을 ZKsync 주소로 위임하여 ZKsync 거버넌스 시스템에 (간접적으로) 참여한다.
 1. 토큰 어셈블리의 투표 권한은 투표 권한이 위임된 ZKsync 주소의 컨트롤러(“**대리인 (Delegates)**”)에 의해 보유·행사된다.
 2. ZK 토큰 보유자는 자신이 컨트롤하는 ZKsync 주소로 위임함으로써, 자신의 ZK 토큰의 투표 권한을 스스로에게도 위임할 수 있다.
 3. 대리인은 거버넌스 제안을 발의하고 투표할 수 있다.
2. **ZKsync 보안위원회(“Security Council”):** 보안위원회는 총 12석 중 최소 9명으로 구성된 거버넌스 기구이며, 그 권한, 절차, 구성은 스케줄 3: ZKsync 보안위원회에 규정되어 있다.
 1. 보안위원회는 다음의 이더리움 L1 멀티시그를 관리한다:
[0x66E4431266DC7E04E7d8b7FE9d2181253df7F410](#)
 2. 보안위원회의 주요 책무는, 대리인에 의해 승인된 프로토콜 거버너 제안(아래 정의)을 온체인 실행 전에 평가하고 승인하는 것이다.
 3. 보안위원회는 비상시 ZKsync 프로토콜을 동결할 수 있다.
 4. 보안위원회는 비상 업그레이드를 개시 및/또는 승인할 수 있으며, 이는 ZKsync 가디언과 ZKsync 재단의 추가 승인을 조건으로 실행된다.
3. **ZKsync 가디언(“Guardians”):** 가디언은 ZK Credo의 수호자로 활동하는 거버넌스 기구로, 총 8석 중 최소 5명의 개인으로 구성되며, 그 권한, 절차, 구성은 스케줄 4: ZKsync 가디언에 규정되어 있다.
 1. 가디언은 다음의 이더리움 L1 멀티시그를 관리한다:
[0x600dA620Ab29F41ABC6596a15981e14cE58c86b8](#)
 2. 가디언은 ZK Credo와 일치하지 않는 거버넌스 제안을 독립적으로 거부(veto)할 권한을 가진다. 여기에는 남용적이거나 악의적이거나 ZKsync 또는 그 거버넌스 시스템에 부정적 영향을 미칠 수 있는 제안의 거부 권한이 포함된다. 가디언의 결정은 전적인 재량에 따라 이루어진다.
 3. 가디언은 거버넌스 제안의 적법성을 평가할 의무가 없다.
 4. 가디언은 위험 검토 기간 동안 어떠한 이유로든 보안위원회가 승인을 행사하지 않는 경우, 대리인이 승인한 프로토콜 거버너 제안을 평가하고 승인할 수 있다.
 5. 가디언은 비상 업그레이드를 승인할 수 있으며, 이는 보안위원회와 ZKsync 재단의 추가 승인을 조건으로 실행된다.

5. 지원 단체

1. **ZKsync 재단:** ZKsync 재단은 케이맨 재단으로서, 그 외에도 ZKsync, ZKsync 관련 기술, 이더리움 L1 블록체인 시스템 또는 보다 광범위한 영지식 기반 암호 기술과 관련하여 작업하는 다양한(경쟁 가능성이 있는) 시장 참여자에게 보조금을 제공하고 계약을 체결한다. 이는 ZKsync 및 관련 기술의 사용 또는 기능을 연구, 평가, 테스트, 모니터링, 유지, 촉진, 조성 및 개선하는 목적을 포함한다.
 1. ZKsync 재단은 다음의 이더리움 L1 멀티시그(“**ZKsync Foundation Multisig**”)를 관리한다: [0xbC1653bd3829dfEc575AfC3816D4899cd103B51c](https://etherscan.io/address/0xbC1653bd3829dfEc575AfC3816D4899cd103B51c)
 2. ZKsync 재단은 비상 업그레이드를 승인할 수 있으며, 이는 ZKsync 가디언과 ZKsync 보안 위원회의 승인을 조건으로 실행된다.
2. **ZKsync 협회:** ZKsync 협회는 오스트리아 협회(Verein)(“**ZKsync Association**”)로서 주로 다음을 담당한다: (i) ZKsync 거버넌스 시스템 설계; (ii) 초기 거버넌스 및 토큰 스마트 컨트랙트 배포; (iii) 아래에 설명된 거버넌스 기구의 초기 구성원 임명; (iv) ZK 토큰 에어드롭 수행; (v) 그 정관에 따라 예상되는 바와 같이 ZKsync 프로토콜의 지속적 거버넌스 지원(예: 본 거버넌스 절차의 정기적 업데이트); (vi) 다음 인터페이스에서, 전적인 재량에 따라 오스트리아 법률을 위반하거나 상충하거나, 부정적 세부 결과를 초래할 수 있는 콘텐츠를 제거:
 1. <https://vote.zknation.io> 및 <https://delegate.zknation.io>에서 제공되는 ZKsync 거버넌스 포털.
 2. <https://docs.zknation.io>에서 제공되는 ZK Nation 거버넌스 문서.
 3. <https://forum.zknation.io>에서 제공되는 ZKsync 거버넌스 포럼.

6. 표준 거버넌스 절차

1. ZK 토큰이 부여하는 투표 권한을 사용하는 대리인이 투표하고, 탈중앙 온체인 거버넌스를 위해 배포된 스마트 컨트랙트(이하 “**거버너(Governors)**”)에 의해 실행되는 거버넌스 제안의 표준 절차는 스케줄 1: 표준 거버넌스 절차에 규정되어 있다.
2. ZKsync 거버넌스 시스템에는 세(3) 가지 거버너가 있으며, 각 거버너는 특정 유형의 거버넌스 제안에 책임을 진다:
 1. **프로토콜 거버너:** ZKsync 개선 제안(“**ZIPs**”)을 실행하여 ZKsync 프로토콜 및/또는 ZKsync 거버넌스 시스템의 구성 요소를 업그레이드하는 데 책임이 있다.
 1. 프로토콜 거버너는 ZKsync Era에 배포된 OpenZeppelin 스마트 컨트랙트다: [0x76705327e682F2d96943280D99464Ab61219e34f](https://etherscan.io/address/0x76705327e682F2d96943280D99464Ab61219e34f)
 2. 프로토콜 거버너 타임락은 ZKsync Era에 배포된 OpenZeppelin 스마트 컨트랙트다: [0x085b8B6407f150D62adB1EF926F7f304600ec714](https://etherscan.io/address/0x085b8B6407f150D62adB1EF926F7f304600ec714)
 2. **토큰 거버너:** 토큰 프로그램 가이드라인에 부합하고 ZK Credo 비전을 지지하는 목표 달성에 기여하는 토큰 프로그램을 위해 ZK 토큰의 민팅 및 번 권한을 할당하는 토큰 프로그램 제안(“**TPPs**”)을 실행하는 데 책임이 있다.
 1. 토큰 거버너는 ZKsync Era에 배포된 OpenZeppelin 스마트 컨트랙트다: [0xb83FF6501214ddF40C91C9565d095400f3F45746](https://etherscan.io/address/0xb83FF6501214ddF40C91C9565d095400f3F45746)

2. 토큰 거버너 타임락은 ZKsync Era에 배포된 OpenZeppelin 스마트 컨트랙트다:
[0xe5d21A9179CA2E1F0F327d598D464CcF60d89c3d](#)
3. **GovOps 거버너**: 직접적인 온체인 결과를 갖지 않는 거버넌스 및 운영 관련 거버넌스 자문 제안(“GAPs”)을 촉진하는 데 책임이 있다.
 1. GovOps 거버너는 ZKsync Era에 배포된 OpenZeppelin 스마트 컨트랙트다:
[0xEEa739a8b6fB1b8f703E23C9Be03CeeA643b160](#)
 2. GovOps 거버너 타임락은 ZKsync Era에 배포된 OpenZeppelin 스마트 컨트랙트다:
[0xC9E442574958f96C026DeF9a50C3236cab17428a](#)

7. 비상 대응 절차

1. ZKsync 생태계 및/또는 ZKsync 거버넌스 시스템에 즉각적인 보안 위험을 초래하는 위협에 대응하기 위한 ZKsync 프로토콜의 프로토콜 업그레이드 실행 절차는 스케줄 2: 비상 대응 절차에 규정되어 있다.
2. ZKsync 거버넌스 시스템에서 실행될 수 있는 비상 대응에는 두(2) 가지 유형이 있다:
 1. 레이어 1 컨트랙트의 동결; 그리고/또는
 2. 비상 업그레이드의 실행.
3. 각자의 멀티시그(“**비상 업그레이드 서명자(Emergency Upgrade Signers)**”)와 함께 비상 업그레이드의 개시 및/또는 승인에 관여하는 세(3) 가지 거버넌스 기구는 다음과 같다:
 1. 보안위원회;
 2. 가디언; 그리고
 3. ZKsync 재단.
4. 각 비상 업그레이드 서명자는, 서명자(“**Signer**”)로 구성된 멀티시그로 ZKsync 거버넌스 시스템에 표현된다. 본 거버넌스 절차에서 “Signer”란 (1) 멀티시그 월렛 또는 (2) 외부 소유 계정(EOA)을 의미한다.

8. 법적 고지

1. 본 거버넌스 절차는 정보 제공 목적일 뿐이며, 구속력 있는 법적 합의가 아니며, 보안 취약점 또는 유사한 사안을 해결하기 위해 ZKsync 거버넌스 시스템 출시 이전에 변경될 수 있다.
2. 출시 시점부터 ZKsync 거버넌스 시스템은 ZKsync 협회나 제3자에 의해 통제되지 않으며, ZKsync 프로토콜에 대한 변경 또는 업데이트는 토큰 어셈블리의 승인이 필요하다. ZKsync 협회는 ZKsync 거버넌스 시스템에 대한 변경 또는 업데이트를 본 거버넌스 절차에 성실히 반영하기 위해 노력할 것이다. 다만, 최신성 또는 완전성은 보장되지 않는다.
3. 본 ZKsync 거버넌스 절차와, 여기서 설명된 사항과 관련하여 어떤 개인 또는 단체가 체결한 계약이나 의무(본 ZKsync 거버넌스 절차에 언급된 코드 포함) 사이에 충돌이 있는 경우, 해당 계약 또는 의무, 또는 관련 코드는 모든 측면에서 우선한다.

4. 본 ZKsync 거버넌스 절차는 여기에 기술된 위험 요소 및 면책조항의 적용을 받으며, 이는 본문에 전부 인용된 것으로 간주된다.
5. 본 문서의 어느 부분도, 또는 그렇게 해석되어서는 안 되며, 여기에 설명된 어떤 개인 또는 단체와 다른 개인 또는 단체(해당 당사자가 서면으로 명시적으로 합의한 경우를 제외하고) 사이에 다음을 생성하거나 생성하는 것으로 해석되어서는 안 된다: (1) 대리 또는 신의성실 의무 관계, 또는 어떠한 의무나 책임의 수임, (2) 서비스 또는 고용 관계, 또는 (3) 공동사업, 비즈니스 기회 관계, 파트너십, 비법인 조합 또는 유사한 관계.