지케이싱크(ZK)

주요내용설명서(국문백서)

Korean White Paper

2026년 8월 20일

Disclaimer

본 번역본은 2026년 8월 20일 기준 지케이싱크(ZK) 백서에 공개된 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

지케이싱크 에라(ZKsync Era)는 이더리움에서 암호학적 유효성 증명[1]을 이용하여 확장 가능한 저비용 트랜잭션[2]을 제공하는 무신뢰[3] 프로토콜이자 레이어2 zk롤업[4]입니다. 지케이싱크 에라에서는 오프체인 방식으로 계산이 이루어지며, 대부분의 데이터가 역시 오프체인 방식으로 저장됩니다. 트랜잭션은 유효성 증명을 생성하기 전에 번들[5]로 묶여 일괄 처리됩니다. 이더리움에서 모든 유효성 증명이 입증되면 사용자에게는 레이어1에서와 동일한 보안성이 보장됩니다.

지케이싱크(ZK)는 토큰 소유자들이 프로토콜 업그레이드를 도입하고, 이에 대해 투표하며, 지케이싱크의 네이티브 계정 추상화[6]를 사용하여 네트워크 수수료를 지불할 수 있게 해주는 프로토콜 토큰입니다. 커뮤니티는 거버넌스 기반의 프로토콜 업그레이드를 통해 스테이킹[7] 및 기타 기능을 도입하도록 ZK를 진화시킬 수 있습니다.

비즈니스 모델

지케이싱크 에라는 외형과 느낌이 이더리움과 비슷하게 만들어졌지만 처리량은 더 많고 수수료는 더 적습니다. 이더리움에서와 마찬가지로 스마트 컨트랙트[8]는 솔리디티[9] 또는 바이퍼[10] 언어로 작성되며, 다른 EVM[11] 호환 체인에서와 동일한 클라이언트를 사용하여 불러올 수 있습니다.

---

[1] Validity proof
[2] Transaction
[3] Trustless
[4] Zero-knowledge rollup
[5] Bundle
[6] Native account abstraction
[7] Staking
[8] Smart contract
[9] Solidity
[10] Vyper
[11] Ethereum virtual machine

주요 특징

- 타사에 전혀 의존하지 않는, 이더리움에서 상속받은 보안성
- 무허가형[12] EVM 호환 스마트 컨트랙트
- 스마트 컨트랙트 결합성[13]과 같은 EVM의 핵심 특성 유지
- 표준 웹3.0 API(애플리케이션 프로그래밍 인터페이스)[14]
- 트랜잭션 입력에 비해 유의미한 비용 절감 효과를 제공하는 트랜잭션 출력을 통한 상태 업데이트(상태 변화라고도 함)
- EIP4337[15]에 비해 기능이 향상된 네이티브 계정 추상화(이더리움 및 기타 롤업에서 구현됨)

개발자 경험

지케이싱크 에라는 이더리움과 유사한 개발자 경험을 제공하도록 만들어졌습니다.

- 스마트 컨트랙트는 솔리디티 또는 바이퍼 언어로 작성 가능합니다.
- 스마트 컨트랙트는 zksolc 및 zkvyper와 같은 커스텀 컴파일러[16]로 변환됩니다.
- 대부분의 컨트랙트가 즉시 작용하므로 프로젝트 마이그레이션[17]이 원활하게 이루어집니다.
- 하드햇[18]과 파운드리[19]같은 기존 프레임워크, Ethers, Viem, web3.js와 같은 라이브러리, 더그래프, 써드웹[20], 체인링크와 같은 도구를 사용합니다.
- 웹3.0 API 호환성을 통해 대부분의 개발자 도구를 지원할 수 있습니다.
- 로컬 테스트 및 디버깅을 위한 다양한 도구를 제공합니다.

---

[12] Permissionless

[13] Composability

[14] Application programming interface

[15] Ethereum improvement proposal 4337

[16] Compiler

[17] Migration

[18] Hardhat

[19] Foundry

[20] Thirdweb

사용자 경험

지케이싱크 에라 기반 애플리케이션과의 상호 작용이 원활히 이루어지며, 저렴하고 빠릅니다.

- 트랜잭션은 레이어1에서 즉각적으로 확인되고 빠르게 완결됩니다.
- 트랜잭션 수수료가 극도로 저렴합니다(평균적인 트랜잭션 비용).
- 네이티브 계정 추상화 및 페이마스터[21] 덕분에 트랜잭션 수수료를 ERC20[22] 토큰(예: 유에스디코인(USDC))으로 편리하게 결제할 수 있습니다.
- 메타마스크[23], 트러스트월렛[24], 제리온[25], 래비[26] 등 기존의 이더리움 기반의 지갑을 지원합니다.

토크노믹스

기본 정보

토큰 티커	ZK
토큰 주소	0x5A7d6b2F92C77FAD6CCaBd7EE0624E64907Eaf3E
총발행량	21,000,000,000개
스냅샷[27]	29,710,983

[21] Paymaster

[22] Ethereum request for comment 20

[23] Metamask

[24] TrustWallet

[25] Zerion

[26] Rabby

[27] Snapshot

인플레이션[28]	토큰 발행량은 거버넌스 프로토콜 업그레이드를 통해 증가할 수 있습니다.
배포 대상	지케이싱크 에라
이더리움 메인넷[29]**으로 이동 가능성**	있음

토큰 유통

분류	토큰	비율	설명
토큰 어셈블리 (Token Assembly)	6,146,000,700	29.27%	토큰 어셈블리에서 할당 예정
생태계 이니셔티브	4,179,000,000	19.90%	생태계 이니셔티브 할당분은 지케이싱크 재단에서 관리하며 생태계 성장을 위해 활용합니다.
에어드랍[30]	3,675,000,000	17.50%	락업[31] 없는 일회성 에어드랍
투자자	4,154,642,006	19.78%	투자자 및 어드바이저
팀	2,845,357,294	13.55%	매터 랩스(Matter Labs) 직원
합계	21,000,000,000	100%	

* 2025년 6월 투자자 및 팀 할당분의 수량이 업데이트된 계산 방식을 반영하여 변경되었습니다.

[28] Inflation

[29] Mainnet

[30] Airdrop

[31] Lockup

투자자 및 팀 토큰은 1년의 클리프[32]를 포함하여 2024년 6월부터 2028년 6월까지 4년의 언락[33] 기간을 가집니다. 2025년 6월에는 총발행량의 3.6%가 팀 및 투자자 할당에서 언락됩니다. 2025년 6월 이후부터 2028년 6월까지 매달 최대 0.8%의 토큰 공급량이 언락됩니다.

캡드 민터(Capped Minter)

대부분의 온체인 조직에서 토큰은 출시 시점에 발행되어 수동적으로 지갑에 보관됩니다. 이것은 여러 가지 문제로 이어집니다. 투자 또는 트레저리[34] 다각화 같은 금융 공학에 집중해야 한다는 부담을 주며, 토큰 수령자가 토큰 수령 시점과 수령 방법을 주체적으로 결정할 수 있는 권리를 배제시킵니다.

지케이싱크는 **캡드 민터** 제도를 이용합니다. 캡드 민터는 토큰 발행량 전체를 한 번에 발행하는 대신 '적시에 발행'할 수 있습니다. 각 캡드 민터에게는 발행이 허용되는 최대 토큰 수가 지정됩니다. 따라서 이들은 원하는 시점에 언제든 정해진 최대 공급량을 넘지 않는 선에서 토큰을 발생할 수 있습니다. 이 방식은 대규모 트레저리와 연관된 위험을 없애고 그 대신 토큰 관리 에이전시의 역할을 캡드 민터가 하도록 만듭니다.

이는 블록 익스플로러에서 볼 수 있는 최대 총발행량과 프로그래밍된 공급 한도 21,000,000,000개 사이의 불일치를 설명해 줍니다.

ZK 출시 이후 재단, 에어드랍, 투자자, 팀원 베스팅 컨트랙트들에 항목별 할당분을 분배하기 위한 캡드 민터가 만들어지게 되었습니다. 토큰 어셈블리에서 관리하는 29.3%의 물량은 캡드 민터가 아니라 ZK 토큰 컨트랙트에 남아 있습니다. 토큰 어셈블리는 토큰 프로그램 관리자들에게 발행 권한을 부여할 수 있습니다.

*지정된 캡드 민터가 모든 토큰을 발행하는 것은 아닙니다.
* 컨트랙트 및 관리자 멀티시그[35](해당하는 경우) 배포 시 보안 위원회(Security Council) 구성원 혹은 공신력 있는 보안 기업에 의해 최소 1회의 보안 검토를 받아야 합니다.

[32] Cliff
[33] Unlock
[34] Treasury
[35] Multisig

* 지난 10월 24일부터 10월 30일에 걸쳐 팀 할당분을 기존 수탁 업체에서 다른 수탁 업체로 이전했습니다. 팀 할당분은 상기 '락업' 항목에서 제시한 베스팅 일정에 따라 언락되기 시작했습니다.

로드맵

[지케이싱크 2026년 로드맵]

프리비디움(Prividium) : 프라이버시 엔진에서 금융 기술 스택[36]으로

프라이버시는 가상자산 분야의 가장 중요한 요소입니다. EVM과 완벽하게 호환되고, 세세한 설정이 가능하며 즉시 사용할 수 있는 프리비디움은 이미 가장 고도화된 프라이버시 블록체인 플랫폼로서 입지를 구축한 바 있습니다. 개발자는 낯선 개발 언어로 코드를 다시 작성하거나, 익숙한 이더리움 도구 혹은 사용자 경험을 포기하거나, 유동성 혹은 결합성을 타협할 필요 없이 프라이빗 애플리케이션을 개발할 수 있습니다.

2026년에는 프리비디움을 통해 쌓은 기반을 바탕으로 프라이버시를 기업용 애플리케이션의 기본 설정값으로 만들고, 기술적 역량을 입증하는 것에서 더 나아가 실제 운영 환경에서 원활하게 비공개 작업 실행을 구현하는 것으로 초점을 바꾸고자 합니다. 이를 위해 신원 및 접근 권한 관리, 트랜잭션 승인 과정, 보고 및 기록, 감사, 기존 금융 및 운영 소프트웨어와의 통합 등 기업의 현재 작업 흐름 및 시스템에 프라이버시 기능을 직접 통합할 수 있게 지원하려 합니다. 기업용 인프라에 익숙한 팀들의 경우 지케이싱크를 기반으로 프라이버시 애플리케이션을 개발하고 운영한다면 개별적인 가상자산 기술 스택을 사용하는 것과는 달리 자연스럽고 친숙한 사용자 경험을 느끼게 될 것입니다.

지케이 스택(ZK Stack) : 개별 체인에서 조화로운 시스템으로

아틀라스(Atlas) 업그레이드는 지케이 스택을 고성능의 레이어2 스택으로서 실제 시스템 부하가 발생하는 기관 및 기업용 체인을 지원할 수 있도록 바꿔 놓았습니다. 아틀라스 업그레이드를 통해 지케이 스택은 대규모 작업을 안정적으로 처리할 수 있게끔 자체적인 EVM 호환성과 인프라를 갖추게 되었습니다.

지난 성과를 토대로 삼아 2026년 지케이 스택을 앱체인이 일급 객체[37]처럼 작동되고 다수의 체인이 단일 시스템으로서 조화롭게 운영될 수 있는 하나의 플랫폼으로 발전시키고자 합니다. 애플리케이션은 외부 브리지[38]나 개별적인 통합 과정 없이도 여러 퍼블릭 및 프라이빗 지케이 체인에 걸쳐 유동성을 활용하고, 작업을 실행하며, 공유 서비스를 이용할 수 있게 됩니다. 또한 크로스체인 작업이 결합 가능한 방식으로 자체적으로 가능해지면서도, 대부분의 과정이 사용자와 개발자 관점에서 비가시적으로 진행됩니다. 결과적으로 지케이 스택은 앱체인 개발 시 기본적으로 찾게 되는 선택지가 될 것입니다. 성능 분리,

[36] Technology stack

[37] First-class citizen

[38] Bridge

시스템 내부적으로 보장되는 연결성, 공유 서비스, 보안 구성 요소, 인프라 지원 도구 등 모든 것을 즉시 활용할 수 있습니다. 자체 체인 구축을 원하는 이에게 지케이 스택은 파편화된 다른 프로젝트들과 다르게 운영상의 복잡성을 크게 완화하고 결합성은 한층 강화하여 실제 운영까지 가장 빠르게 도달할 수 있는 길을 제시하게 될 것입니다.

에어벤더(Airbender) : 초고속 zkVM[39]에서 범용 표준으로

에어벤더는 속도 측면에서는 이미 세상에서 가장 뛰어난 RISC-V[40] 기반의 zkVM입니다. 2026년에는 더욱 철저한 감사와 정형 검증[41], 개발자 경험 대폭 개선을 거쳐 신뢰성과 범용성까지 최고 수준으로 끌어올릴 계획입니다. 에어벤더는 지케이싱크 스택뿐 아니라 이더리움의 영지식 중심 장기 로드맵과 검증 가능한 고성능 연산이 필요한 모든 시스템을 지원함으로써 가상자산 분야와 그 외의 분야에서도 기본적으로 사용되는 zvVM의 표준으로 거듭나고자 합니다.

[39] Zero-knowledge virtual machine

[40] Reduced instruction set computer V

[41] Formal verification