

PDAO REPORT

2025.07.31.

ZK



Zero-Knowledge Technology in Solana Ecosystem

Reviewed by

Junha
X : @junha_yang

fakedev9999
X : @fakedev9999

Written by

seungjun
X : @seungjun_x

lmxx
linkedin : /lmxx

Paduck
X : @paohree

Dominick
linkedin : /juyoung_jeong



Intro.

이 리포트는 블록체인 기술 혹은 컴퓨터공학 관련 지식이 없는 대부분의 가상자산 투자자들 그리고 블록체인 생태계에 입문하고 싶은 학생들을 대상으로 하며, 현재 존재하는 zk 관련 기술을 Solana Ecosystem 내에 존재하는 3가지 사례를 바탕으로 알아본다. 이 리포트를 읽은 이후에는 투자를 위해 zk가 활용된 프로젝트 관련 글을 읽었을 때 그 의미를 이해하고 투자에 참고할 수 있는 수준으로의 지식을 얻어갈 수 있기를 바란다.

INDEX

I. 서론

- 투자자의 입장에서 바라보는 Zero-knowledge
- ZK는 Crypto Market의 성장과 뗄 수 없는 기술
- ETH L2를 넘어 모든 생태계로의 확장
- Solana 생태계 기술을 주목하는 이유
- Accerlate 행사로 알아보는 ZK Trend in SOL

II. 영지식 증명 (Zero - Knowledge Proof)

- 영지식 증명의 개념과 원리
- 비상호작용성 ZKP의 등장 → 블록체인에 ZK를 활용할 수 있게 된 계기
- zk의 특성과 크립토 산업에서 지니는 의미

III. ZK 활용 기술 1 - ZK Compression

- ZK Compression?
- Solana의 높은 저장소 비용 문제
- State Compression을 통한 비용 절감
- State Compression의 한계점
- State Compression → ZK Compression으로의 발전
- ZK Compression의 도입 효과
- ZK Compression과 vs ZK Rollup의 차이
- ZK Compression 활용 프로덕트 사례

IV. ZK 활용 기술 2 - zkSVM

- zkVM이란?
- zkVM의 특징
- zkSVM
- zkSVM의 기대효과 - 더 싸고 더 빠르게
- zkSVM의 기대효과 - 다른 체인으로의 확장성
- SOL 생태계 내 zkVM 프로덕트 사례

V. ZK 활용 기술 3 - zkBridge (ETH - SOL)

- 크립토 생태계에서의 브릿지의 의미
- 2022년 Ronin 해킹과 zkBridge의 필요성
- zkBridge를 활용한 ETH - SOL 자산 이동
- zkBridge 활용 시 이점
- SOL 생태계에서의 zkBridge 프로젝트 사례

VI. 결론

- SOL의 zk 기술 발전을 투자자가 주목해야하는 이유

I. 서론

1

투자자의 입장에서 바라보는 zero-knowledge

영지식 증명(Zero-Knowledge)은 블록체인 생태계에서 자주 쓰이는 암호학적 기술로, 가상자산 투자들이 한번쯤은 들어보았을 단어이다. Coinmarketcap 기준 zero knowledge proof 카테고리에 listing 종목이 67개이며, ARB, zkSync 등 zk 관련 프로젝트들이 국내 여러 코인거래소에서 KRW마켓에 상장되어 활발히 거래되고 있다. zero-knowledge 기술을 활용하는 프로젝트 수의 증가와, 블록체인 기술에 효과적인 도입을 위한 zk 기술의 발전은 크립토 산업의 성장에 주요하게 작용해왔다.

많은 프로젝트에서 zk 기술을 활용하여 특정 성질을 향상시켰다는 등의 말을 많이 한다. 하지만 현재 크립토 시장의 대다수를 차지하는 가상자산 투자자들에게는 zk 기술은 특정 프로젝트에서 zk 관련 설명이 존재할 때 이를 이해하고 투자정보로써 활용한다기 보다는, 하나의 마케팅 용어로써 인식되고 있다고 보여진다.

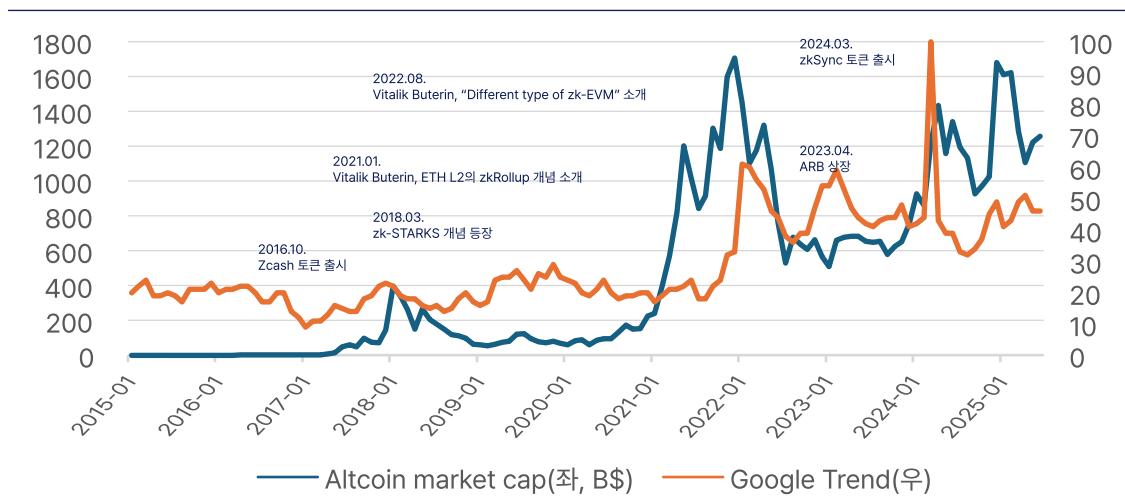
2

ZK는 Crypto Market의 성장과 뗄 수 없는 기술

ZK에 대한 관심도와, 가상자산 시장의 성장은 그 쾌를 같이 해왔다. 이는 특히 알트코인 시가총액의 변화량과 함께 비교를 해본다면, 그 경향성을 파악할 수 있다. 아래 이미지는 Google Trend 지표에서 영지식 증명을 주제로 한 검색 지표와, 알트코인 시가총액의 변화를 함께 표현한 것이다.

예컨데 2018년 3월 zk-STARKS 등 새로운 zk 기술이 등장하였을 때 알트코인 시가총액이 급등하는 것을 볼 수 있었으며, 2022년~2024년 zk 관련 프로젝트의 토큰 출시/상장 시즌에 Google Trend 지표와 Altcoin 시가총액이 함께 증가하는 모습을 보여준다. 알트코인 시가총액의 경우 2022년 테라-루나 사태로 인해 급감하는 위치가 존재하나, 이를 제외한 여러 시점에서 구글트랜드 지표가 급등하는 시점에 알트코인 시가총액이 증가하는 경향성을 보임에서 기술의 관심도와 마켓이 함께 움직임을 볼 수 있다.

그림 1. Zero-Knowledge에 대한 Google Trend 지표 / Altcoin MarketCap 변화



자료: Google Trend, Coingekco, PDAO

ETH L2를 넘어 모든 생태계로의 확장

zk를 실제로 활용한 프로젝트의 시작은 Zcash였으나, 실질적으로 크립토 시장에서 zk 기술에 주목하게 된 계기는 이더리움 생태계의 확장성 솔루션으로의 활용에 있다. 이는 2018년부터 업로드된 Vitalik Buterin의 블로그를 통해 zk-SNARKs, zk-STARKs, zk-Rollup, zk-EVM 등 zk에 기반한 이더리움 생태계의 기술 발전 솔루션을 잘 정리된 글로 소개한 데에 있을 것이며, 당시에 가장 성숙한 알트코인 Layer 1 생태계였기에 가능했을 것으로 보인다.

하지만 시대가 지나며 여러 Layer 1 체인들의 규모가 성장했고, 이더리움을 제외한 다른 생태계에서 zk 관련 프로덕트를 도입하고 있다. Solana의 ZK Compression, Sui의 zkLogin/zkSend 등 기존 Layer1 체인들에서의 활용, 여러 체인들에 공통적으로 활용되는 zkVMM 등을 통하여 이는 블록체인 생태계의 전반적인 방향으로 기술의 활용이 확산되고 있다.

그림 2. Zero-knowledge 관련 주요 이슈 타임라인



자료: PDAO

Solana 생태계 기술을 주목하는 이유

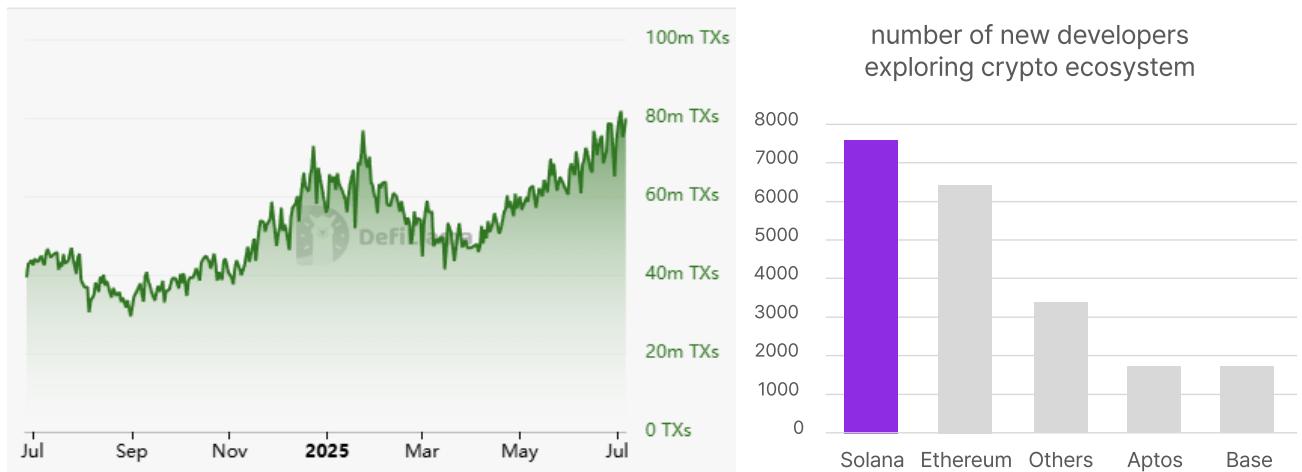
이 리포트에서는 그 중에서도 Solana 생태계에서의 zk기술에 대한 설명을 제공하고자 한다. 현재 다양한 altcoin ecosystem들 중, solana가 여러 방면에서 유의미한 성과를 보여오며 주목을 받고 있다.

온체인 지표 관점에서 바라볼 때, Solana의 온체인 트랜잭션 수의 경우 지난 2024년 7월 약 4000만 Tx에서 2025년 7월 약 8000만 Tx 수준으로 유의미하게 성장하였다. 이는 pump.fun, \$TRUMP 등 각종 meme token 생태계의 성장이 지속적으로 이뤄났음에 나타나는 현상으로 보인다.

블록체인 개발자의 입장에서 Solana 생태계는 Active 개발자 수가 많은 생태계이기도 하다. Electric Capital에서 발표한 Developer Report 2024에 따르면, 지난 2024년 약 7625명의 신규 개발자가 Solana 생태계에 유입되었으며, 이는 모든 블록체인 생태계 중 가장 높은 수를 기록하였다.

마지막으로 리서치를 하는 입장에서 ETH와 확장성 솔루션에 있어 대비되는 방향을 가지고 있기에, 이러한 점을 영지식기술에 관한 접근하면 두 체인간의 차이를 이해할 수 있을 것이라 생각하였다.

그림 3. Solana 트랜잭션 변화 (좌), 2024년 블록체인 생태계별 신규 개발자 유입 인원 수 (우)



자료: DeFiLama, Electric Capital, PDAO

5

Accelerate로 알아보는 ZK Trend in SOL

Solana Foundation은 매년 "Accerlerate"라는 명칭의 컨퍼런스를 주최하고 있는데(과거 "Breakpoint"로 부터 리브랜딩 되었다), 이 행사의 키노트로부터 생태계에서의 zk 기술 적용이 어떠한 의미이고, 어떠한 발전과정을 겪고 있는지 확인 할 수 있었다. 2023년의 경우 Breakpoint 행사에서 "ZK on Solana : Private Solana Programs"를 주제로 세션이 있었다. 이 외에도 매달 첫번째 목요일에 주최되는 "Solana Ecosystem Call"에서도 관련 정보를 찾을 수 있었다. 2024년 7월 이뤄진 Solana Ecosystem Call에서는 이번 리포트에서 중점있게 다룬 기술 중 하나인 ZK Compression 공식 출시에 대한 발표가 있었다.

그림 4. Solana 관련 행사에서 발표된 zk 관련 이슈 사례



자료: PDAO

II. 영지식 증명(ZK Proof)

6

영지식 증명의 개념과 원리

이번 챕터에서는 영지식 증명에 대한 간략한 소개를 진행한다. 영지식 증명이란, 정보(Knowledge)를 공개하지 않고서도(Zero) 그 정보를 알고 있음을 증명(Proof)하는 암호학적 기법이다. 영지식 증명을 잘 설명하는 대표적인 예시로, "알리바바의 동굴"이라는 예시가 있다.

두 사람 P(prover, 증명자)와 V(Validator, 검증자)가 있다고 하자. V는 P가 도어락의 비밀번호를 알고 있는지 확인하려한다. 하지만 그 비밀번호 자체를 알고자 하지는 않는다. 즉, 정보(비밀번호)는 공개하지 않으면서도 그것을 알고 있음을 증명하려는 것이다.

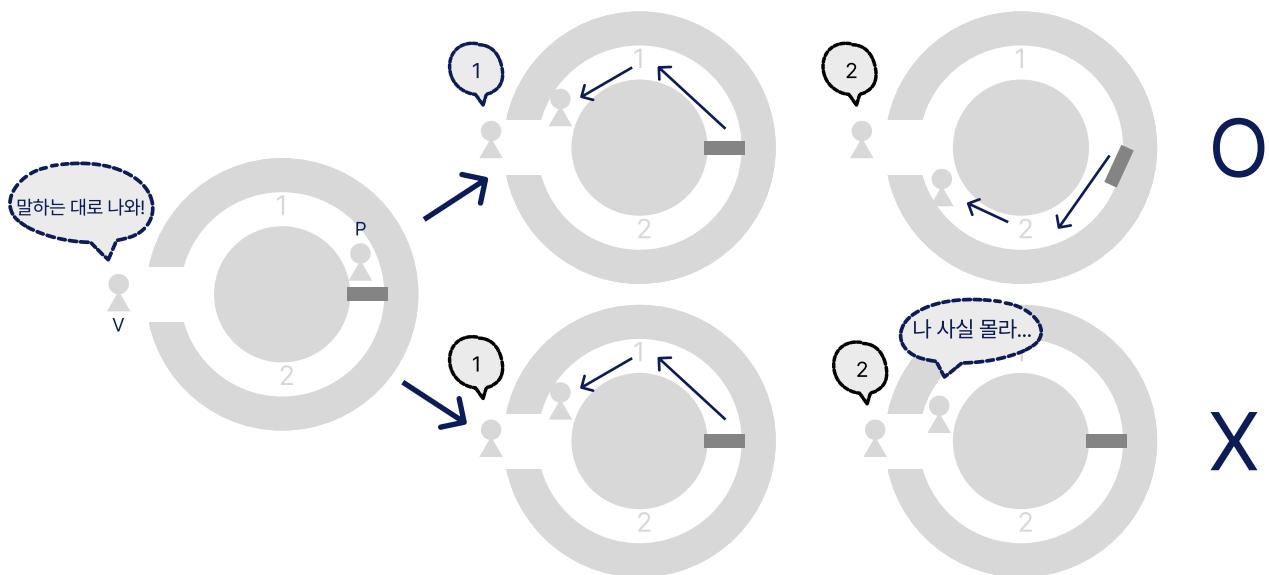
이를 위해 V는 동굴의 입구에 서 있고, P는 동굴 안으로 들어간다. V는 P에게 1번길로 나와, 혹은 2번길로 나와라고 무작위로 명령한다. 만약에 P가 주문을 알고 있다면, 어느쪽으로 P가 들어갔던 도어락을 열고 반대편으로 갈 수 있으니, 항상 V의 요청대로 나올 수 있을 것이다. 만약 그렇지 않다면, V의 요청대로 나오지 못하는 경우가 생길 것이다.

이를 한 두번만 반복한다면 P가 운이 좋게도 통과를 할 가능성이 생긴다. 하지만 이를 수십번 반복하게 되고, 그 기간동안 P가 모두 정확하게 V의 요청대로 나온다면 이는 P가 비밀번호를 알고 있다고 확률론적으로 볼 수 있다는 것이다.

이것이 영지식 증명의 가장 대표적인 형태이자 가장 고전적인 형태 중 하나인 "interactive ZKP"의 방식이다. 이 방식을 통하여 ZKP는 아래와 같은 3가지 특성을 가진다는 것을 보여준다.

- 완전성 : 정보를 가진 증명자(P)는 언제나 검증자(V)에게 올바른 답을 제공할 수 있다.
- 건전성 : 거짓된 정보를 가진 증명자는 검증자를 속일 수 없다.
- 영지식성 : 검증자는 증명자의 주장 외에는 어떤 추가 정보를 얻을 수 없다.

그림 5. 알리바바의 동굴 사례



자료: PDAO

7

비상호작용성 ZKP의 등장 → 블록체인에 ZK를 활용할 수 있게 된 계기

위에서 설명한 알리바바의 동굴과 같이, interactive ZK Proof 방식은 검증자와 증명자의 반복적인 정보 교환을 요구하기에, 많은 거래 비용과 시간이 소요된다는 단점으로 인해 실생활에서 쓰이지 못했다.

그러나 하드웨어의 발전과 지속적인 연구가 진행되며, 반복적인 상호작용 없이 ZKP를 구현하는 non-interactive한 방식, zk-SNARK가 등장하며 ZKP의 활용성이 급증하였다.

이후 이 과정에서 블록체인 확장성 솔루션으로써의 zk-rollup, zk-EVM 등이 등장하며 블록체인 성능 향상을 가속화하는데 도움을 주었고, 최근에는 속도와 투명성 분야에서 조금 더 발전된 zk-STARK 등의 다양한 알고리즘이 연구되고 있다.

8

zk의 특성과 크립토 산업에서 지니는 의미

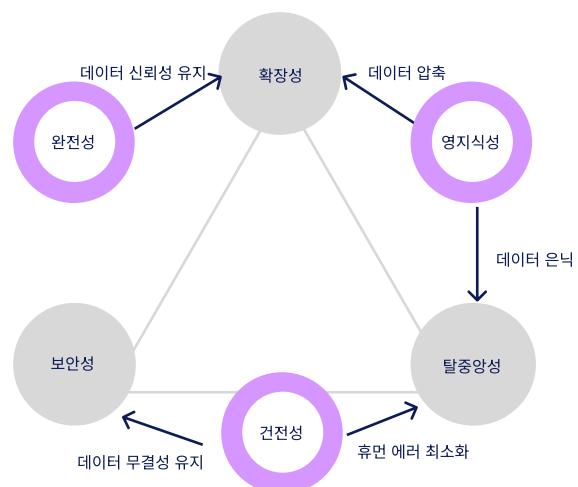
ZK 기술이 블록체인에 적용되기 시작한 배경에는, 영지식 증명의 핵심적인 특성이 블록체인 트릴레마의 해결에 기여할 수 있다는 점에 있다. 블록체인 트릴레마란, 블록체인의 지속가능성을 위해 지녀야 할 아래 3가지 특성이 한번에 달성되는 것이 현실적으로 매우 어려움을 뜻한다.

- 확장성 : 거래 처리 속도와 처리량이 높아, 대규모 사용자 수요를 감당할 수 있어야 한다.
- 탈중앙성 : 네트워크 참여자 모두가 등등하게 검증과 의사결정에 참여할 수 있어야 한다.
- 보안성 : 네트워크와 데이터가 악의적 공격에도 안전하게 보호되어야 한다.

영지식 증명이 지니는 특징들은, 블록체인 트릴레마의 3가지 특성에 대해 보완적인 수단으로 활용될 수 있다. 예를 들어 영지식성의 경우 모두가 원본의 데이터를 보지 못한다는 점에서 데이터 은닉에 기반한 탈중앙성 강화, zkP에 기반한 데이터 압축을 통해 확장성 강화에 기여할 수 있다.

이처럼 zk 기술이 블록체인 생태계에서 지속가능성을 보완하는데 중요한 수단으로 활용되고 있다. 다음 챕터부터는 Solana 생태계에 적용된 zk 기술 사례를 바탕으로, 어떠한 방식으로 zk 기술이 크립토 산업에 긍정적인 영향을 제공하는지 알아본다.

그림 6. ZK 기술의 3요소와 블록체인 트릴레마의 관계



자료: PDAO

III. ZK Compression

9

ZK Compression?

ZK Compression은 2023년 말 Light Protocol과 HELIUS Labs가 발표한 기술로, Solana 체인 내부에서 데이터를 압축하여 저장하는 것을 지원하는 기술이다. ZK Compression은 온체인에서의 저장소 비용을 기준 대비 최대 1000배까지 절감하는 효과를 보였으며, 이는 Solana 생태계 상에서 저비용으로 대규모 에어드랍이 가능하게 하는 등 솔라나 생태계의 성장에 효과적인 영향을 줄 것으로 기대하고 있다.

10

Solana의 높은 저장소 비용 문제

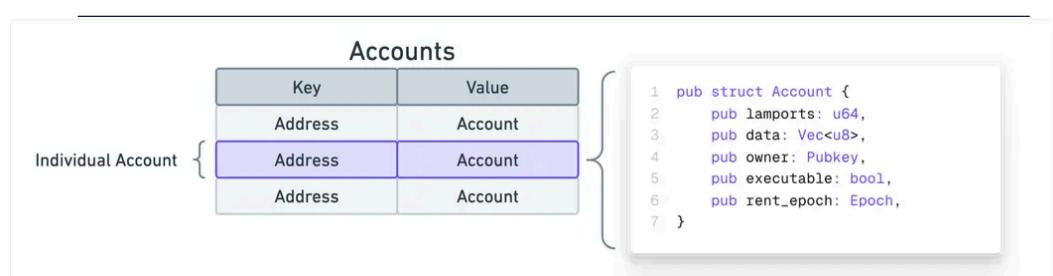
Solana는 블록체인 상의 다양한 모든 정보들을 Account라는 단위의 공간에 저장한다. 무분별한 Account 생성을 막기 위해, 새로운 Account를 생성하려면, 네트워크에 저장하는 데이터의 양에 비례하여 rent라는 최소 잔액을 유지해야 정상적으로 이용할 수 있다.

하지만 이 rent 비용이, 최대 용량인 10MB의 정보를 담은 Account를 생성하려는 경우 약 70 SOL (25년 6월 기준)이라는 높은 비용을 지불해야 한다.

블록체인 정보들의 종류

블록체인 내에 기록되는 데이터는 크게 두 가지 (Code, State)로 나눌 수 있다. Code는 스마트 컨트랙트와 같은 실행 로직을 의미하고, State는 계정 잔액 등과 같은 각종 변수 값을 의미한다. Solana에서는 이들을 Program account와 Data account로 부른다.

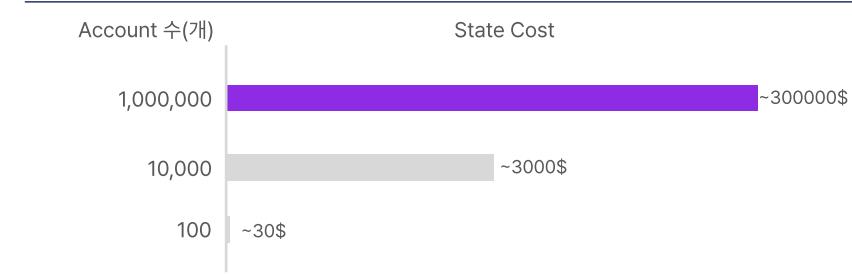
그림 7. Solana 생태계의 Account



자료: Solana Labs

이러한 높은 계정 비용은 Solana의 확장성을 근본적으로 제한한다. 초당 수만 건의 트랜잭션을 처리할 수 있다고 해도, 사용자가 늘어날 수록 계정 생성 비용이 기하급수적으로 증가하기 때문이다. 예를 들어 100만 명의 사용자를 온보딩하려면 매우 많은 양의 rent가 필요하다. 이는 대규모 채택을 꿈꾸는 dApp들에게 진입 장벽이 되며, 결국 개발자들은 여러 사용자 데이터를 하나의 계정에 몰아넣거나 오프체인 저장소를 활용하는 등 차선책을 택하게 된다.

그림 8. Solana에서 다양한 General Account를 생성하는데 드는 비용(USD 기준, 1SOL = 150USD 가정)



자료: PDAO

State Compression을 통한 비용 절감

해싱(Hashing)

데이터를 짧고 고유한 암호코드로 변환하는 기술. 원본이 조금만 바뀌어도 결과값이 완전 달라지는 특성이 있어 위변조 검증에 활용된다.

Ledger

블록체인의 전체 거래 기록을 저장하는 분산 원장. Solana에서는 노드들이 관리하는 데이터베이스를 의미한다.

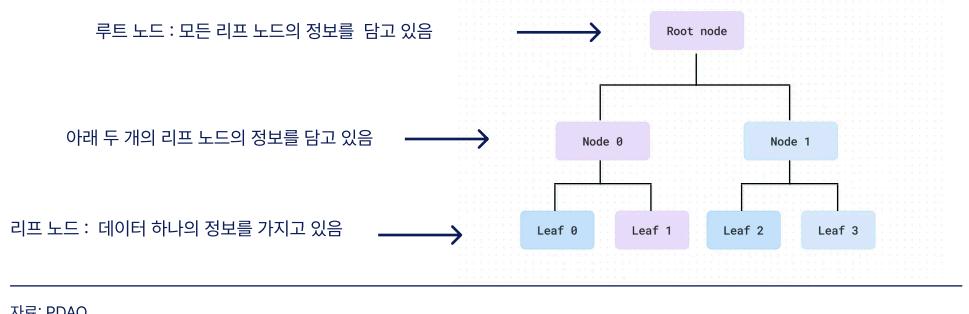
State Compression은 Solana Labs와 Metaplex의 개발자들이 Solana에 구축한 기술로 Solana의 고비용 문제를 해결하기 위한 기술이다.

모든 데이터를 온체인에 저장하는 대신, 머클트리(Merkle Tree)라는 구조를 활용하여 데이터의 핵심적인 요약 정보만을 저장할 수 있게 한다. 머클트리는 나무처럼 생긴 데이터 구조를 가지고 있으며, 아래와 같은 방식으로 데이터를 표현한다.

- 각각의 작은 데이터들(leaf node)에 대해 해싱*을 수행한다.
- 해싱된 데이터 두개를 묶어 다시 해싱을 수행한다. 이 과정을 계속 반복하여 하나의 데이터가 되도록 만들며, 이를 Root hash Node라고 한다.
- 이 Root Hash 하나만 블록체인에 저장하고, 실제 내용은 Ledger*에 보관한다.

해시의 특징으로 인하여 전체 데이터가 없어도 특정 데이터의 존재를 증명할 수 있으며 데이터가 변조되더라도 Root Hash 가 달라지기 때문에 변조 즉시 탐지할 수 있다.

그림 9. 트리 구조에 대한 이미지



자료: PDAO

일반적인 NFT 메타 데이터 (약 380 bytes)를 기준으로 State Compression의 비용 효율성을 살펴보면, 단일 NFT의 경우 압축 전 \$0.114에서 압축 후 \$0.25로 오히려 비용이 증가한다. 이는 Merkle Tree 구조를 위한 초기 설정 비용 때문이다.

하지만 규모가 커질수록 압축의 효과가 극적으로 나타난다. 10,000개 NFT 컬렉션에서는 압축 전 \$1,140에서 압축 후 \$248로 약 78% 비용 절감을 달성하며, 해당 비용이 \$0.025 까지 낮아진다.

대규모 컬렉션에서는 이 효과가 더 드러나는데, 1,000,000개 NFT의 경우 압축 전 \$114,000에서 압축 후 단 \$248로 99.8% 이상의 비용 절감을 보여준다. 이때 해당 비용은 \$0.00025에 불과해, 압축 전 대비 약 456배 저렴해진다.

State Compression의 두가지 한계점

이러한 장점에도 state compression에는 여전히 아래 두가지의 한계가 존재했다.

- 계정 크기 제한 : Solana의 Account는 최대 10MB 까지 저장할 수 있지만, 실제로는 1232 bytes 를 초과하면 rent 비용이 급격하게 증가한다. State Compression의 경우에도 크기가 큰 (깊은) Merkle Tree에서 Solana의 Transaction Size Limit인 1232 bytes를 초과하는 경우가 많았다.
- 확장성 문제 : Instagram의 NFT 프로젝트 개발 과정에서 시작되어 Solana에 도입되었다. Compressed NFT로 대규모 NFT를 발행할 때, 체인 외부에 데이터를 저장해 데이터 관리를 위해 지불해야 하는 Account Space의 rent 비용을 99.9% 절감하는 효과가 있었지만 이 때문에 NFT 메타데이터 스키마에 최적화된 설계로 인해 확장성이 부족했다.

State Compression → ZK Compression으로의 발전

Compressed PDA (Program Derived Address)

블록체인 상에서 프로그램이 자동으로 생성하고 관리

하는 특별한 계정 주소이다.

은행이 고객을 위해 자동으로 만드는 가상계좌번호와
비슷한 개념이다.

State Tree Hash

전체 데이터 구조 (State Tree)를 대표하는 고유한 암호코드로, 수천 개의 계정 정보가 담긴 트리 구조 전체를 단 하나의 짧은 코드로 요약한 것이다.

Leaf Index

머클트리에서 특정 데이터(리프)의 위치를 나타내는
번호이다.

Groth16

영지식 증명 알고리즘 중 하나로, 매우 작은 크기(128 바이트)의 증명을 생성하면서도 빠른 검증이 가능한 기술이다.

ZK Compression은 State Compression의 압축 개념을 모든 Solana 계정 타입으로 확장했다. 핵심은 계정 데이터를 오프체인에 저장하고, 온체인에는 32바이트 해시만 남겨두되, 영지식 증명 (ZKP)으로 데이터의 무결성을 보장하는 것이다.

이를 위해 ZK Compression은 **Compressed PDA***라는 형태의 Account를 사용하는데, 이는 일반 Solana 계정과 유사한 구조이며 아래와 같은 내용이 기록되어 있다.

- Owner: 계정을 수정할 권한을 가진 프로그램 ID
- Lamports : SOL 잔액
- Data : 프로그램 상태를 저장하는 필드
- Address : 선택적 필드로, 고유성이 필요한 경우에만 사용

이 Account와 함께, **State Tree Hash***와 **Leaf index***라는 두 가지 정보를 추가하여 리프 노드를 만들어낸다. Account 정보에 이 두 값을 함께 기록함으로써 여러 State Tree가 존재하더라도 각 압축된 계정이 전역적으로 고유하게 식별되게 한다.

ZK Compression은 **Groth16*** 기반의 Validity Proof를 도입한다. 압축된 계정을 읽거나 수정할 때마다 128 바이트 크기의 영지식 증명이 생성된다. 이 증명은 실제 데이터를 공개하지 않으면서도 해당 계정이 State Tree에 유효하게 존재함을 증명한다.

Light Protocol은 온체인에서 이 Proof를 검증하여, 오프체인 데이터가 변조되지 않았음을 확인한다.

그림 10. ZK Compression에서 활용되는 Merkle Tree 구조



자료: Messari

14

ZK Compression 도입 효과

ZK Compression을 도입하게 될 시, 100 개의 압축된 토큰 계정을 생성하는데 소모하는 비용이 약 0.00004 SOL로 추정되며, 이는 기존 Account 생성 비용인 0.2 SOL 대비 5000배 가량 저렴하다. 100만 개의 토큰 계정을 생성한다고 가정할 경우 기존 방식으로는 30만 달러가 필요하지만, ZK Compression을 이용하면 단 50달러면 충분하다.

이러한 획기적인 수준의 비용 감축은 기존의 고비용으로 인해 부담되었던 대규모 토큰 발행/생성 등을 요구하는 프로젝트들에게 희소식이다. 이는 에어드랍, 대규모 NFT 컬렉션, 게임 아이템 등 적게는 수천 ~ 많게는 수백만 개의 계정이 필요한 애플리케이션들을 비용의 걱정 없이 실현할 수 있도록 돋는다.

15

ZK Compression vs ZK Rollup

이러한 ZK Compression은 기존의 ETH 생태계에서 활용되어온 ZK rollup 계열의 방식과 명백한 차이점을 보여준다.

ZK Rollup은 레이어 2 확장성 솔루션으로, 수백 개의 트랜잭션을 오프체인에서 처리한 후, 그 결과를 영지식 증명과 함께 메인체인에 제출하는 방식이다. 이를 통해 메인체인은 모든 트랜잭션을 개별적으로 처리하지 않고도 전체 배치의 유효성을 검증할 수 있다. ZK Rollup은 메인체인의 보안성을 그대로 상속받으면서도 초당 수백에서 수천 건의 트랜잭션을 처리할 수 있어, 가스비를 최대 99%까지 절감하는 효과를 제공한다.

ZK Compression과 ZK Rollup의 가장 근본적인 차이는 작동 범위와 목적에 있다. ZK Rollup이 별도의 레이어 2 네트워크를 구축하여 트랜잭션 처리량을 늘리는 '수평적 확장'에 초점을 맞춘다면, ZK Compression은 메인체인 내에서 데이터를 압축하여 저장 효율성을 높이는 '수직적 최적화'를 추구한다.

아키텍처 측면에서 ZK Rollup은 시퀀서, 프로버 등 추가 인프라가 필요하며, 메인체인과 레이어 2 간의 브리지가 필수적이다. 반면 ZK Compression은 기존 프로그램에 직접 통합 가능하며 별도의 네트워크 구성이 불필요하다. 또한 ZK Rollup은 데이터 가용성을 위해 트랜잭션 데이터를 여전히 온체인에 저장해야 하지만, ZK Comperssion은 원본 데이터를 압축된 증명으로 대체하여 저장 공간을 절약한다.

calldata

거래를 실행하기 위해 블록체인에 전송해야 하는 필수 정보들로 거래의 세부사항을 담은 데이터이다.

두 기술의 차이가 존재한다고 하여 이 간의 우열관계가 존재하는 것은 아니다. 오히려 두 기술은 상호 보완적 관계로, 함께 사용될 때 블록체인의 효율성을 극대화할 수 있다. ZK Rollup 내에서 ZK Compression을 활용하면, Rollup의 **calldata***를 추가로 압축하여 레이어 1 저장 비용을 더욱 절감할 수 있다. 이론적으로는 기존 ZK Rollup이 처리하는 트랜잭션 수를 상당히 증가시킬 수 있는 잠재력을 가지고 있다.

특히 프라이버시가 중요한 기업용 애플리케이션에서는 두 기술의 결합이 강력한 솔루션이 된다. ZK Rollup으로 높은 처리량을 확보하면서, ZK Compreression으로 민감한 거래 정보를 보호할 수 있기 때문이다. 이러한 하이브리드 접근법은 확장성, 프라이버시, 비용 효율성을 동시에 달성하는 차세대 블록체인 인프라의 핵심이 될 것으로 전망된다.

그림 11. ZK Compression vs ZK Rollup 비교 표

구분	ZK Compression	ZK Rollup
작동 위치	L1에서 직접 작동	L2 별도 네트워크 필요
주요 목적	데이터 저장 비용 절감	트랜잭션 처리량 증가
인프라 요구사항	추가 인프라 불필요	시퀀서, 프로버, 브리지
데이터 처리	압축된 상태만 온체인 저장	모든 트랙잭션 데이터 온체인 저장

자료: PDAO

16

ZK Compression 활용 프로덕트 사례

ZK Compression을 활용한 대표적인 사례로는 Helius Labs가 개발한 Airship이 있다. Airship은 ZK Compression을 활용하여 Solana 토큰 에어드롭 비용을 5000배까지 절감하는 오픈소스 도구이다. 기존에 1만 명에게 토큰을 배포하는데 20 SOL (약 \$2800)이 필요했다면, Airship을 사용하면 단 0.01 SOL (약 \$1.4)로 가능하다.

SLINKY 토큰은 Airship을 통해 2,777만 개 지갑에 토큰을 배포했으며, 이는 Solana 역사상 최대 규모의 에어드롭이다. 압축된 토큰은 필요시 즉시 일반 토큰으로 변환 가능하여 DeFi 등 기존 인프라와의 호환성을 유지한다.

그림 12. ZK Compression 활용 사례 - Airship



자료: Helius

IV. zkSVM

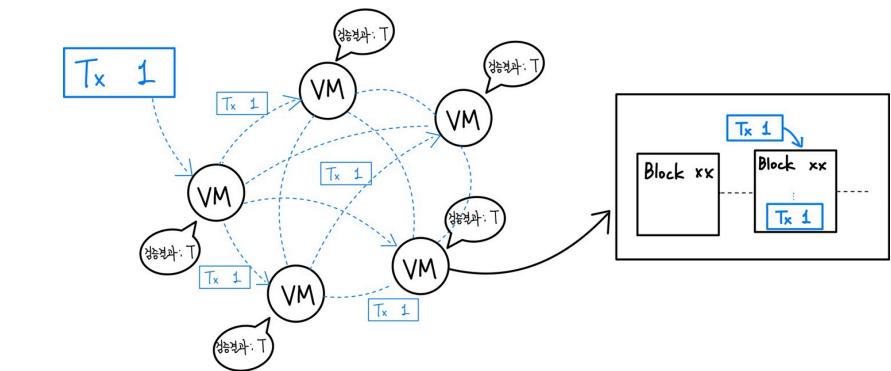
17

zkVM이란?

zkVM은 프로그램의 실행을 영지식 증명으로 검증할 수 있는 특별한 가상 머신(VM, Virtual Machine)이다. 가상머신이라는 것은 말 그대로 가상의 컴퓨터 환경을 의미하는데, 블록체인 생태계에서는 트랜잭션을 처리하기 위해 만들어진 특별한 환경이라고 말할 수 있다. 흔히 말하는 블록체인 네트워크에서 노드 하나가 이 VM이라고 볼 수 있다.

예를 들어 하나의 트랜잭션이 생겨났다고 하자. 이 트랜잭션은 블록체인 네트워크에 브로드캐스팅되어 각 가상머신에서 이를 검증한다. 각 노드에서의 검증 결과에 따라, 체인에서 정해진 합의 알고리즘에 맞추어 트랜잭션을 승인할 지, 거절할지 결정하고, 승인되는 경우 블록에 트랜잭션이 추가된다.

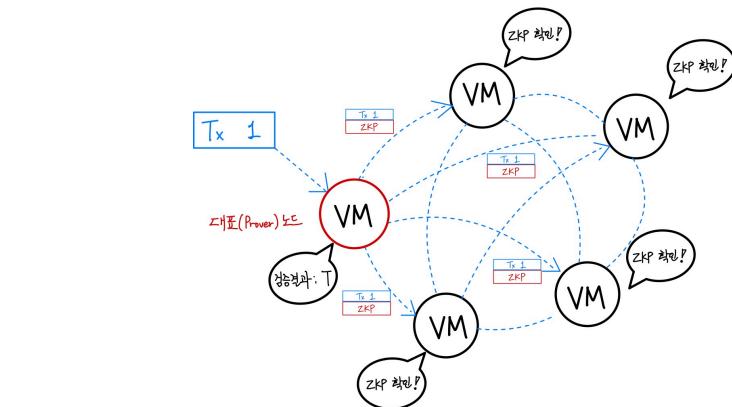
그림 13. 기존 환경에서의 트랜잭션 검증 과정



자료: PDAO

전통적인 가상 머신은 단순히 코드를 실행하는 것에 그친다면, zkVM은 그 실행이 올바르게 이루어졌다 는 암호학적 증명을 함께 생성한다. 그리고 이를 함께 다른 노드에 전달하는 것이다. 이 경우 기존에는 각 노드에서 전부 연산을 따로 따로 수행하던 것을, 대표적인 노드(Prover) 한 두개만 트랜잭션에 대해 검증을 해도 충분하게 된다. 다른 노드들의 경우 각자 연산을 직접 해보지 않더라도, 이 대표 노드들이 생성한 증명을 확인하기만 하면 올바른 트랜잭션임을 알 수 있기 때문이다.

그림 14. zkVM에서의 트랜잭션 검증 과정



자료: PDAO

18

zkVM의 특징

zkVM의 아키텍처는 전통적인 VM보다 훨씬 복잡하며, 여러 특수한 구성 요소들이 유기적으로 연결되어 있다.

- 실행 엔진 (Execution Engine)은 zkVM의 심장부로, 프로그램을 실행하고 모든 상태 변화를 세밀하게 기록한다. 이는 단순한 실행을 넘어, 각 명령어의 입력과 출력, 메모리 접근, 레지스터 상태 등 모든 세부사항을 추적한다.
- 산술화 모듈 (Arithmetization Module)은 실행 추적을 수학적 제약조건으로 변환한다. 이 과정에서 프로그램의 논리적 흐름이 다항식 방정식의 집합으로 표현된다.
- 증명 시스템 (Proof System)은 이러한 제약 조건들이 모두 만족된다는 것을 증명하는 영지식 증명을 생성한다. 이는 복잡한 암호학적 프로토콜을 통해 이루어지며, 선택된 증명 시스템 (SNARK, STARK 등)에 따라 구체적인 방법이 달라진다.
- 검증자 (Verifier)는 생성된 증명의 유효성을 확인하는 역할을 한다. 검증 과정은 증명 생성보다 훨씬 빠르며 이로 인해 블록체인의 확장성에 크게 기여한다.

19

zkSVM?

각 블록체인 네트워크별로 데이터를 다루는 방식의 차이가 존재하기에, 각 체인별로 적합한 형태의 가상 머신을 활용할 필요가 있다. 예를 들어 이더리움의 경우 스마트 컨트랙트 하나로 다루어 질 것이, 솔라나에서는 프로그램과 어카운트로 나누어 다뤄진다.

zkSVM은 그 중에서도 솔라나 체인에서의 활용을 위해 맞추어진 zkVM이라고 볼 수 있다. 오프체인에서 복잡한 계산을 수행하고 온체인에서는 간단한 증명만 검증함으로써, 처리 속도는 높이고 비용은 획기적으로 줄이면서도 완전한 프라이버시를 보장한다. 현재 Zpoken 등 여러 기업이 이 분야를 주도하고 있다.

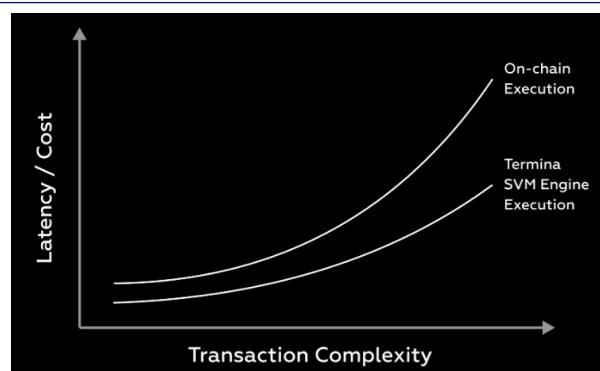
20

zkSVM의 기대효과 - 더 싸고 더 빠르게

2025년 4월, GPU 가속 병렬 처리를 중심으로 빠른 zk 증명 시스템을 제공하는 Solayer의 InfiniSVM은 Devnet에서 340,000 TPS를 달성했다. 당시 Solana의 실제 TPS가 평균 1200 TPS였다는 점, 현재 Solana 네트워크의 이론적인 트랜잭션 처리의 한계가 약 65000 TPS로 추정된다는 점을 고려할 때, 이는 zkSVM을 통해 매우 빠른 속도의 처리가 가능해질 수 있음을 보여준다.

비용의 관점에서도 zkSVM은 효과적인 수단이다. Termina의 경우 Succinct Labs의 sp1-solana를 통하여 zkSVM Proving을 제공하고 있는데, 2025년 5월 기준 Termina Docs에서는, Termina에서 제공하는 zkSVM Prover를 통해 100개의 복잡한 SPL 트랜잭션을 증명하는데 1달러 미만의 아주 작은 비용이 소비된다고 언급한다.

그림 15. Termina SVM을 활용시 기존 대비 Latency/Cost 비율의 우위를 경험할 수 있다.



자료: Termina

21

zkSVM의 기대효과 - 다른 체인으로의 확장

zkSVM은 Solana 가상 머신(SVM)에서 실행된 프로그램의 결과를 ZK Proof로 생성하고, 이 증명이 다른 블록체인에서도 검증될 수 있도록 설계되고 있다. 이를 통해 Solana의 프로그램 실행 결과를 타 체인에 안전하게 전달할 수 있는 상호운용성 솔루션으로 주목받고 있다.

zkSVM은 다음과 같은 확장성을 제공한다.

첫째, Solana의 고속 처리 능력을 활용하여 트랜잭션을 실행하고, 생성된 STARK 증명을 Groth16으로 압축하여 이더리움 같은 다른 체인에서 효율적으로 검증할 수 있다. 이는 각 체인의 장점을 최대한 활용하는 하이브리드 솔루션이다.

Sovereign SDK

개발자들이 자신만의 독립적인 블록체인(앱체인)을 쉽게 만들 수 있도록 도와주는 개발 도구 모음이다.

둘째, SP1과 같은 범용 zkVM을 통해 Solana와 다른 생태계 간의 신뢰 최소화 브리지가 가능해진다. 기존의 멀티시그 방식을 영지식 증명으로 대체하여 보안성을 향상시킨다. **Sovereign SDK*** 를 활용한 앱체인들은 이미 Solana에 정착하면서 zkSVM의 이점을 활용하고 있다.

SOL 생태계 내 zkVM 프로덕트 사례

RISC-V 아키텍처

오픈소스 기반의 간단하고 모듈화된 명령어 집합 구조로, 다양한 하드웨어에서 유연하게 사용되고 있다.

Precompile

블록체인에서 자주 쓰이는 연산(예: 해싱 등)을 빠르게 처리하기 위해 미리 컴파일된 특수한 시스템 계약이다.

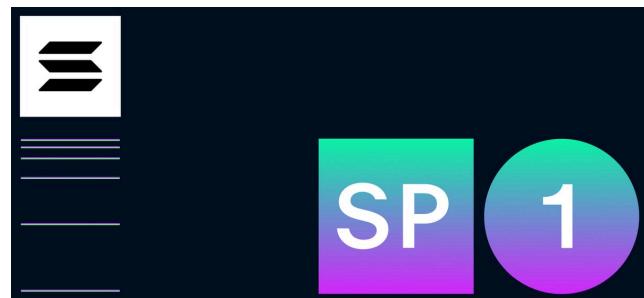
Solana 생태계에서의 zkVM 프로덕트 활용 사례로는 SP1 (Succint Processor 1)을 들 수 있다. SP1은 Succint Labs가 개발한 zkVM으로 일반 Rust 코드로 영지식 증명을 생성할 수 있다. 2024년 8월 Succint Labs에서 발표한 정보에 따르면 당시 SP1은 기존 zkVM 대비 최대 36배 빠른 성능을 자랑하였다. SP1은 여러 체인에서 활용 가능한 범용 zkVM이나, 2024년 12월 Solana Verifier(검증자) library를 공개하여 Solana 생태계에서도 사용할 수 있게 되었다.

SP1은 **RISC-V*** 아키텍처를 기반으로 하여 제작되었으며, **Precompile*** 중심 설계라는 중요한 특징을 바탕으로 높은 성능을 보여주고 있다. SHA256, Keccak256 해시와 secp256k1, ed25519 서명 검증 등 핵심 암호화 연산을 최적화된 회로로 처리해 RISC-V 사이클을 5-10배 감소시킨다.

SP1은 단일 머신에서 900 KHz에서 수 MHz의 처리량을 보이며, GPU 클러스터 활용 시 실시간에 근접한 증명 생성이 가능하다. 2025년 5월에는 SP1 Hypercube를 소개하며 이더리움 블록의 증명이 실시간으로 가능하도록 개선하였다. 발표된 자료에 따르면 SP1 Hypercube는 이더리움 블록의 93% 이상을 12초 이내에 증명하는 아주 빠른 속도를 가지고 있다.

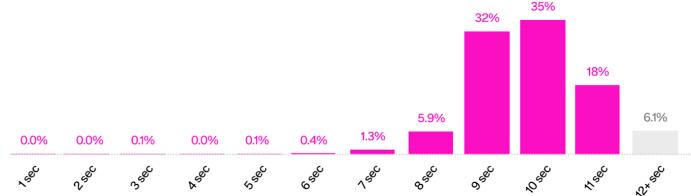
Solana 개발자의 입장에서 SP1을 바라보면, Solana 프로그램 개발에 활용되는 Rust, C++ 등 언어를 모두 지원하기에 기존 코드를 거의 수정 없이 zkVM에서 실행하여 고성능 연산을 활용할 수 있다는 장점이 있다. 현재 Spicenet, Termina, Soon 등 Solana 내 여러 프로젝트에서 SP1을 활용하고 있으며, Veridise, Cantina, KALOS의 보안 감사를 완료해 프로덕션 환경에서 안전하게 사용할 수 있다.

그림 16. SP1 in Solana Verifier (위), Real-time Ethereum Proving 지표 (아래)



Proving Latency on Ethereum Blocks

April 19th 2025 - May 3rd 2025 (200 NVIDIA RTX 4090 GPUs)



자료: Succinct

V. zkBridge (ETH - SOL)

23

크립토 생태계에서의 브릿지의 의미

블록체인은 네트워크를 안전하게 유지하고 새로운 블록을 추가한 참여자에게 보상으로 가상자산을 지급하는 구조를 갖고 있다. 이러한 코인은 본래 해당 블록체인 내부에서만 유효한 보상 수단이며, 외부 체인과는 직접적인 호환성이 없다.

그러나 블록체인마다 사용자 기반, 보안 모델, 설계 철학, 그리고 특히 수익 구조 측면에서 차이가 존재하기 때문에, 한 체인에서 발행된 자산을 다른 체인에서도 활용하고자 하는 수요가 점차 증가하고 있다. 이러한 요구를 충족시키기 위한 기술이 바로 브릿지(Bridge)다. 브릿지는 둘 이상의 블록체인 간에 데이터를 전송하거나 자산을 이동시키는 시스템으로, 이질적인 체인들 간의 상호운용성을 가능하게 한다.

이러한 브릿지의 활용을 통해서 Warpped 토큰이 나오는 것이라고 이해할 수도 있다. 이더리움 체인의 ETH를 솔라나 체인에서 사용하기 위해, 브릿지를 활용하여 이더리움 체인의 ETH를 잠그고, 솔라나 체인에 WETH를 발행하여 활용하는 것이다.

24

2022년 Ronin 해킹과 zkBridge의 필요성

멀티시그 (multi-Signature)

여러 사용자의 서명이 모여야 트랜잭션이 실행되도록 하는 방식이다.

릴레이 서버

블록체인 사용자의 트랜잭션을 대신 제출해주는 서버로, 사용자가 가스를 직접 낼 필요 없이 서비스를 이용할 수 있게 한다.

단일 실패 지점

하나의 구성 요소에 문제가 생기면 전체 시스템이 마비될 수 있는 취약한 구조.

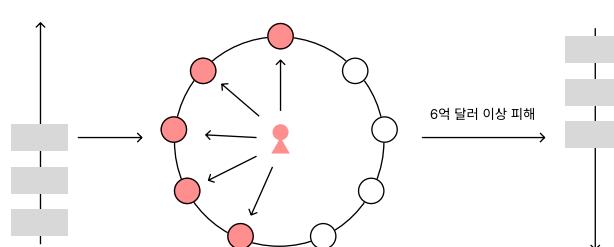
전통적인 브릿지는 일반적으로 **멀티시그(multi-signature)*** 구조, 중앙화된 **릴레이 서버***, 또는 위임된 검증자 세트와 같은 신뢰 기반 중개자(trusted intermediaries)에 의존하여 동작한다. 이러한 구조는 보안상의 **단일 실패 지점***을 초래할 수 있으며, 브릿지 해킹 등 심각한 보안 이슈의 원인이 되어 왔다.

대표적인 사례로, 2022년 발생한 Ronin Bridge 해킹 사건은 신뢰 기반 브릿지(trusted bridge)가 갖는 구조적 취약점을 적나라하게 드러낸 바 있다. 당시 Ronin은 이더리움과 자체 사이드체인 간 자산 이전을 처리하기 위해 9개의 검증 노드 중 5개의 서명을 요구하는 멀티시그(Multisignature) 구조를 채택하고 있었다.

해커는 아직 구체적인 경로가 완전히 밝혀지지 않은 방식으로 5개의 프라이빗 키(private key)를 확보하는 데 성공했고, 이를 통해 6억 달러(약 7,000억 원) 이상의 자산을 탈취하는 데에 이르렀다. 이는 단 5개의 노드만 장악하면 전체 시스템을 무력화할 수 있는 구조적 한계를 명확히 보여준 사례다.

사건 이후 Ronin 운영사는 공격에 사용된 노드의 권한을 차단하고, 기존에 요구되던 5개 서명을 8개로 상향하는 등 보안성을 강화하겠다고 발표했다. 또한 전체 네트워크의 노드 수도 확대하겠다는 계획을 내놓았다. 그러나 이러한 방식은 여전히 “누구를 신뢰할 것인가”라는 문제를 근본적으로 해결하지는 못한다.

그림 17. 멀티시그 방식의 취약점 (Ronin 브릿지 해킹)



자료: PDAO

중간자 공격

두 사용자의 통신 사이에 공격자가 끼어들어 데이터를 몰래 가로채거나 조작하는 해킹 방식.

zkBridge는 특정 검증인에 대한 신뢰를 요구하지 않는다. 모든 트랜잭션은 암호학적으로 생성된 증명(zero-knowledge proof)을 통해 누구나 검증 가능하고, 누구에게나 검증받을 수 있는 구조를 갖추고 있다. 이로 인해 해커가 일부 키를 탈취하여 트랜잭션을 조작하는 **중간자 공격(MITM)***이나 내부자 공격과 같은 위협 자체가 성립되지 않는다.

이처럼 zk 기반 브릿지는 근본적으로 보안 모델의 방향을 '신뢰 기반' → '수학 기반'으로 전환하며, 브릿지 기술의 보안성과 신뢰성을 한층 더 끌어올리는 기술적 진화를 의미한다.

25

zkBridge를 활용한 ETH - SOL 자산 이동

그림 18. ETH - SOL 자산 이동 프로세스

Light Client

전체 블록체인 데이터를 저장하지 않고 최소한의 정보만 검증해 블록체인과 상호작용하는 클라이언트.

1. Event (State Change) Occurs on Solana
 - A user initiates a transaction on Solana, causing a change in the blockchain's state.

2. Composing the Solana Light Client State
 - The necessary information for the Light Client is gathered by tracking certain data off-chain.

3. ZKP Generation
 - Based on the Light Client and block state information, a Zero-Knowledge Proof is generated to mathematically prove a specific state on the Solana chain.

4. Submitting the ZKP to the Ethereum Chain
 - The generated ZKP, along with other necessary information, is submitted to the zkBridge smart contract on Ethereum.
 - The Solana Light Client running on Ethereum verifies that the submitted proof accurately reflects a valid state from the Solana chain.

5. ZKP Verification and Event Triggering on Ethereum
 - The smart contract on Ethereum automatically and mathematically verifies the submitted proof on-chain.
 - If the proof is valid, an event is triggered on Ethereum based on the result.

자료: PDAO

zkBridge 활용 시 이점

기존 브릿지는 체인 간 데이터를 전달할 때 제3자 검증자에 의존하여 구조적으로 신뢰 문제가 발생할 수 있었다. 반면, zkBridge는 트랜잭션의 유효성을 영지식 증명을 통해 직접 입증함으로써 제3자에 대한 신뢰 없이도 검증을 가능하게 한다. 이로 인해 보안성과 탈중앙성이 크게 향상되며, 검열 저항성 또한 강화된다. 브릿지의 특성 상 톤튼 전송에 가장 많은 역할을 하는데, 자산이 움직이는 과정에 대한 보안성 / 탈중앙성의 증가는 건전한 블록체인 생태계에 효과적인 발전을 가져온다.

기술적으로도 zkBridge는 복잡한 트랜잭션 데이터 전체를 단일한 증명으로 압축하여 전달하므로, 검증 비용이 낮고 온체인 데이터 저장도 효율적이다. 나아가 ZK 회로를 통해 다양한 체인 구조를 단일 프로토콜로 수용할 수 있어, 체인 간 확장성과 상호운용성 측면에서도 유리한 아키텍처를 제공한다. 이러한 기술적 이점은 zkBridge가 멀티체인 생태계의 핵심 인프라로 자리 잡을 수 있는 기반이 된다.

그림 19. 기존 브릿지와 zkBridge의 특징 비교

Bridge	특징	zkBridge
높음	검증자 의존도	낮음
높음	검증 비용	낮음
낮음	확장성	높음
낮음	상호 운용성	높음
낮음	탈중앙화 정도	높음

자료: PDAO

SOL 생태계에서의 zkBridge 프로젝트 사례

zkBridge는 Solana 생태계 내에서도 점차 실용적 도입이 확산되고 있다. 대표적으로, Wormhole 팀과 Nil Foundation이 공동 설계한 Solana-Ethereum zkBridge 프로토타입은, Solana의 경량 클라이언트를 이더리움 상에서 zkSNARK로 검증하는 구조로 구현되었다. 해당 설계는 Solana의 블록 헤더 및 상태 전이 데이터를 zk 회로로 변환하고, 이를 이더리움에 제출함으로써 제3자 없이도 트러스트리스한 상태 동기화를 가능하게 한다.

Light Protocol은 Solana 상에서 ZK 기술을 이용해 개인 정보 보호와 브릿지 기능을 결합한 새로운 솔루션을 개발 중이며, 이는 향후 zkRollup 및 zkBridge 기반 상호운용성 확장을 위한 기반 기술로 주목받고 있다.

SOL 생태계에서 시작한 멀티체인 브릿지인 Wormhole의 경우에도 zkBridge 도입을 순차적으로 진행하고 있다. Wormhole은 기존의 19개 Guardians(검증자 네트워크)에 의존했던 Message 검증 구조에서, zero-knowledge proofs (ZKPs) 기반의 permissionless verification(허가 없는 검증) 시스템으로 전환하는 로드맵을 2024년 공식 발표했다. 현재 Wormhole은 Lurk Lab과의 협업을 통해 zk-SNARK를 쉽게 생성하여 여러 체인의 메세지 검증을 zk 기반으로 수행하는 zk light client 도입을 준비하고 있다.

VI. 결론

28

SOL의 zk 기술 발전을 투자자가 주목해야하는 이유

우리는 이 리포트를 통해 Zero-Knowledge(zk) 기술이 무엇인지, 그리고 Solana 생태계에서 이 기술이 어떻게 활용되고 있는지를 살펴보았다. 그러나 이러한 논의는 일부 투자자들에게는 다소 추상적이고, 현실과 동떨어진 기술 이야기로 느껴질 수도 있다.

가상자산 시장에서는 흔히 “펀더멘털이 없다”는 말이 회자된다. 이는 전통적인 밸류에이션 모델로는 가격을 설명하기 어렵기 때문이다. 그렇기 때문에 투자자들은 코인의 수요와 공급, 유저 수, 트랜잭션 처리량, 프로젝트 수, 커뮤니티 활동, 그리고 반복적으로 등장하는 네러티브 등의 지표를 바탕으로 가격을 간접적으로 해석한다.

이러한 지표들의 기반에는 결국 기술적 진보가 존재한다. zk와 같은 기술이 없다면, 블록체인은 사용자 증가, 트랜잭션 증가, 프로젝트 수용의 측면에서 한계에 부딪힐 수밖에 없다. 반대로 zk 기술의 발전은 이러한 한계를 돌파할 수 있는 기반이 되며, 결과적으로는 가격에 긍정적인 영향을 주는 네러티브를 형성하는 핵심 요소가 된다.

특히 Solana는 현재 가장 활발한 활동이 이루어지는 Layer 1 체인 중 하나다. 수많은 신규 프로젝트와 믿코인, 런치패드, 다양한 유저 유입이 지속적으로 나타나고 있으며, 기술적 확장성과 생태계 다양성 면에서 두각을 나타내고 있다. 여기에 zk 기술 기반의 구조적 발전이 더해진다면, Solana는 단기적 유행을 넘어 지속 가능한 성장 기반을 확보할 수 있을 것이다.

실제로 2025년 이더리움의 경우, 페그트라 업그레이드와 비탈릭 부테린의 로드맵 발표가 침체된 ETH 가격 흐름을 반전시키는 전환점이 되기도 했다. 기술은 가격을 직접 설명하지 않지만, 가격을 움직이는 신뢰 가능한 내러티브를 만들어낸다.

이러한 맥락에서 볼 때, zk 기술은 단지 기술적인 용어가 아닌, 투자자가 반드시 짚고 넘어가야 할 가치 판단의 근거가 될 수 있다. zk 관련 기술의 발전과 생태계 적용은 Solana뿐만 아니라 전체 크립토 시장에서 투자자에게 투자 판단에 도움을 줄 수 있는, 이해할 수 있는 내용이 될 것이다. 이 리포트가 그 시작을 이해하는 데 도움이 되길 바란다.

Outro.

zk는 오랫동안 블록체인 생태계에서 중요한 역할을 해왔고, 앞으로도 계속 그려질 것이다. 특히 zk 기반 블록체인 인프라 기업이나 프로젝트들이 토큰 발행을 추진하는 과정에서, 투자자 입장에서는 해당 기술의 이해가 점점 더 중요해질 것이다.

2025년 7월 3일, Google이 공식 블로그를 통해 Zero-Knowledge Proof(ZKP) 기술 기반의 라이브러리를 오픈소스로 공개하였다. 이는 zk 기술을 이해하고 있는 것이, 최근 LLM을 중심으로 한 기술 패러다임의 지수적 발전 흐름을 읽는 데에도 중요한 도움이 될 것임을 알려준다. 이 리포트가 그러한 흐름 속에서, 독자 여러분께 새로운 관점을 제시하고 향후 기술 기반 투자를 판단하는 데 있어 작은 이정표가 되어주길 바란다.

PDAO

PDAO는 POSTECH(Pohang University of Science and Technology)을 거점으로 한 크립토-블록체인 커뮤니티입니다.

PDAO는 2022년 초 POSTECH의 크립토 커뮤니티이자 오픈소스 개발 그룹으로 시작되어, “DAO를 개발하는 DAO”라는 정체성을 바탕으로, 탈중앙화 DAO 프로토콜인 Simperby를 개발하며 이를 통해 스스로를 호스팅해왔습니다. 이외에도 멤버들의 각종 해커톤 참여 및 2023년 과기부 산하 오픈소스 컨트리뷰션 프로젝트 등 개발조직으로써 블록체인 산업에 기여해왔습니다.

2025년 현재 PDAO는 누구나 자유롭게 참여할 수 있는 커뮤니티로써, 블록체인 생태계에 관심있는 사람들이 자유롭게 이 산업에 기여할 수 있는 여러 활동들을 기획하고 참여할 수 있는 단체로 운영되고 있습니다. 이에 2025년 상반기 Superteam KR Guild Lead, Monad Blitz Seoul Supporters 활동 등 각종 재단 및 기업과 각종 프로젝트를 기획, 운영, 참여하고 있습니다.

Official Website : <https://dao.postech.ac.kr>

X : @postech_dao

Reviewed by

Junha

X : @junha_yang

Founder & Lead Dev, PDAO (2022 -)

CTO, Hyperithm (2024 -)

fakedev9999

X : @fakedev9999

Simperby Core Team Head, PDAO (2022 -)

Software Engineer, Succinct (2025 -)

Written by

seungjun

X : @seungjun_x

Organizer, PDAO (2025)

Researcher, Bithumb (2022-2023)

lmxx

linkedin : /lmxx

Active Member, PDAO (2025)

VA, KITRI BoB 13th (2024)

Paduck

X : @paohree

Director, PDAO (2025)

BD intern, Streami (GOPAX) (2024)

Dominick

linkedin : /juyoung-jeong

Active Member, PDAO (2025)

Organizer Lead, Flutter Daegu (2022-2025)

Disclaimer

- 본 리포트는 투자 결과에 대한 법적 책임소재의 증빙자료로 사용될 수 없습니다.
- 투자에 관한 모든 결정과 책임은 투자자 본인에게 있습니다.
- 본 리포트는 신뢰할 만한 자료 및 정보를 토대로 작성되었으나 그 정확성에 대해 보장하지 않습니다.
- 본 자료의 저작권은 PDAO에 있으며, 출처 표기 하에 자료의 일부의 배포를 허용합니다.
- 단, 어떠한 경우에도 조직의 동의 없이 자료의 전체를 복제 및 재배포 할 수 없습니다.