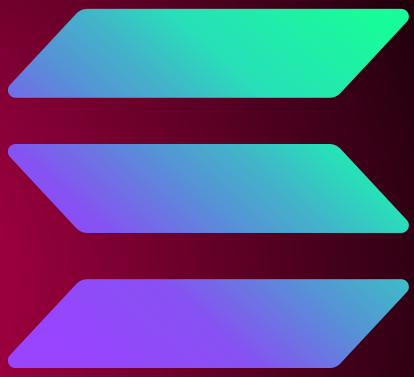
PDAO REPORT

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

PDAO

Intro.

This report is intended for cryptocurrency investors who may not have a background in blockchain technology or computer science, as well as for students looking to enter the blockchain ecosystem. We will explore existing Zero-Knowledge (ZK) technologies through three specific use cases within the Solana ecosystem. The goal is that after reading this report, you will have gained enough knowledge to understand articles about ZK-powered projects and use that understanding to inform your investment decisions.

INDEX

I. Introduction

1

Zero-Knowledge from an Investor's Perspective

Zero-Knowledge proof is a cryptographic technique frequently used in the blockchain ecosystem, a term that most cryptocurrency investors have likely encountered. According to Coinmarketcap, there are 67 projects listed in the "zero knowledge proof" category, and ZK-related projects like ARB and zkSync are actively traded on the KRW market on various domestic crypto exchanges. The increasing number of projects utilizing zero-knowledge technology, along with advancements in ZK technology for its effective implementation in blockchain, has been a major factor in the growth of the crypto industry.

Many projects claim to have enhanced specific properties by utilizing ZK technology. However, for the majority of cryptocurrency investors in the current market, ZK technology seems to be perceived more as a marketing buzzword rather than something to be understood and used as investment information when a project provides ZK-related explanations.

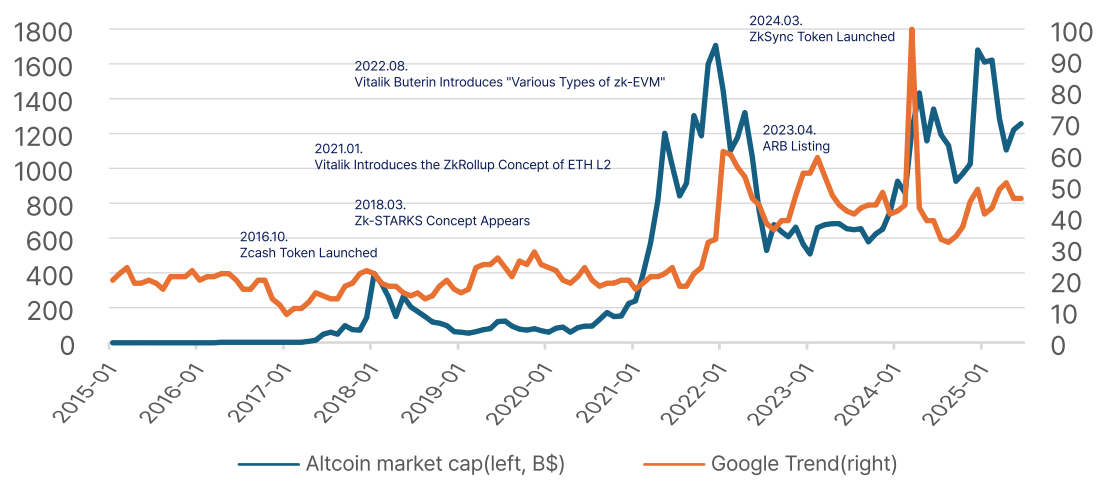
2

ZK: A Technology Inseparable from the Growth of the Crypto Market

Interest in ZK and the growth of the cryptocurrency market have moved in tandem. This trend becomes particularly clear when comparing it with the changes in the total market capitalization of altcoins. The image below combines Google Trends data for the search term "Zero-Knowledge Proof" with the fluctuations in altcoin market capitalization.

For instance, when new ZK technologies like zk-STARKs emerged in March 2018, the altcoin market cap experienced a sharp increase. Similarly, during the 2022–2024 period, which was a season of token launches and listings for ZK-related projects, both the Google Trends indicator and the altcoin market cap rose together. Although the altcoin market cap saw a steep drop in 2022 due to the Terra-Luna crisis, at many other points, there is a clear tendency for the altcoin market cap to increase when the Google Trends indicator surges. This demonstrates that interest in the technology and the market often move together.

Figure 1. Google Trend Indicators for Zero-Knowledge / Altcoin MarketCap Changes.



Source: Google Trend, Coingekco, PDAO

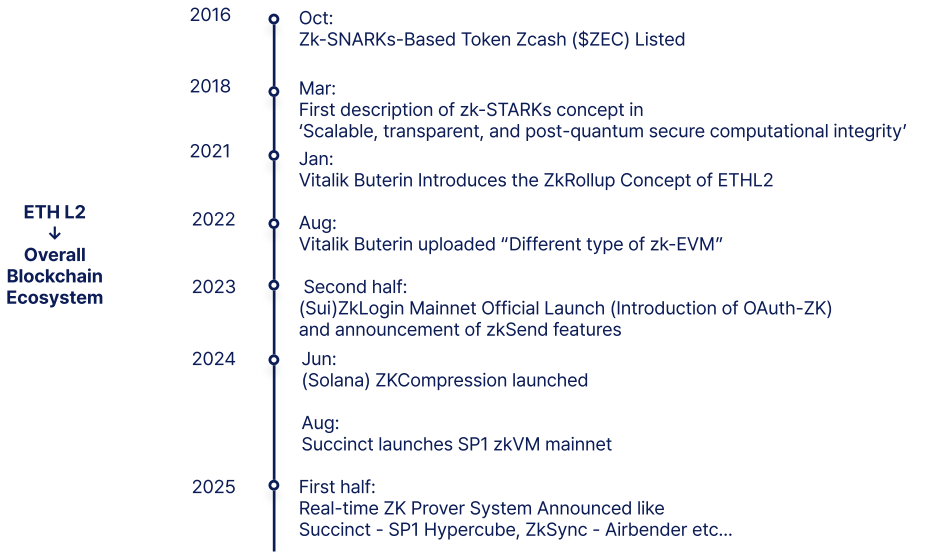
3

Expansion Beyond ETH L2 to All Ecosystems

Although the first project to implement ZK technology was Zcash, the crypto market truly began to pay attention to it when it was utilized as a scalability solution for the Ethereum ecosystem. This was likely driven by Vitalik Buterin's well-articulated blog posts starting in 2018, which introduced ZK-based solutions for Ethereum's technological development, such as zk-SNARKs, zk-STARKs, zk-Rollups, and zk-EVMs. This focus on Ethereum was possible because, at the time, it was the most mature Layer 1 altcoin ecosystem.

However, as time has passed, various other Layer 1 chains have grown, and ecosystems beyond Ethereum are now adopting ZK-related products. The technology's application is expanding across the broader blockchain landscape through its use in existing Layer 1 chains — like ZK Compression on Solana and zkLogin/zkSend on Sui — and through technologies like zkVMs, which can be used across multiple chains.

Figure 2. Timeline of Zero-knowledge key issues.



Source: PDAO

4

Why We Should Pay Attention to Technology in the Solana Ecosystem

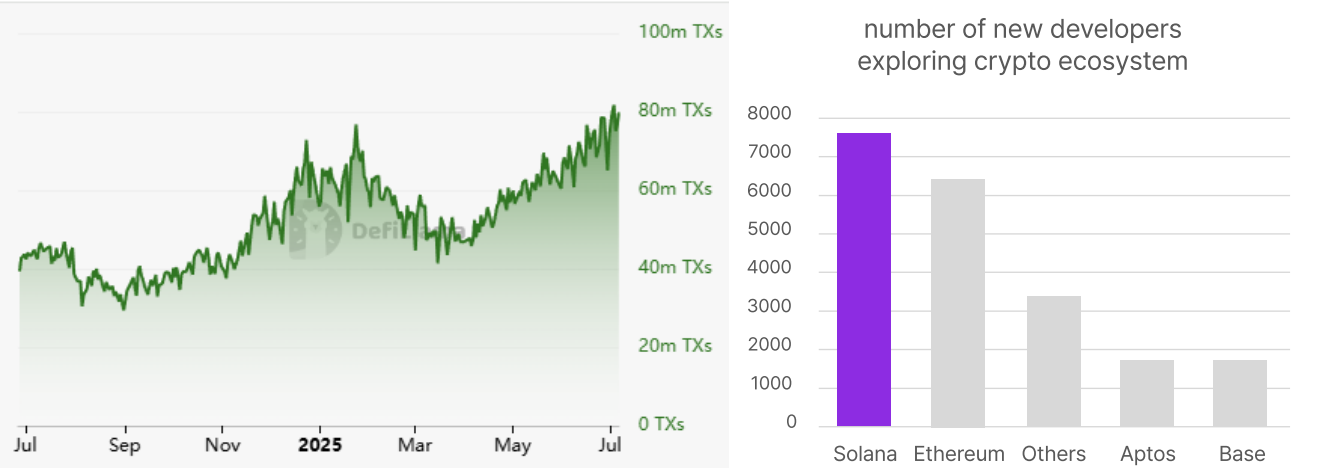
This report aims to specifically explain ZK technology within the Solana ecosystem. Among the various altcoin ecosystems today, Solana is gaining significant attention for its notable achievements across several fronts.

From an on-chain metrics perspective, the number of transactions on Solana has grown significantly, rising from approximately 40 million in July 2024 to around 80 million in July 2025. This appears to be a result of the sustained growth of various meme token ecosystems, including pump.fun and $TRUMP.

From a developer's standpoint, the Solana ecosystem boasts a large number of active developers. According to the 2024 Developer Report by Electric Capital, about 7,625 new developers joined the Solana ecosystem in the past year, which was the highest influx recorded among all blockchain ecosystems.

Finally, from a research perspective, Solana and Ethereum have contrasting approaches to scalability. I believe that examining these differences through the lens of Zero-Knowledge technology will offer a clearer understanding of the two chains.

Figure 3. Changes in Solana transactions (left), the number of new developers flowing in by blockchain ecosystem in 2024 (right)



Source: DeFilLama, Electric Capital, PDAO

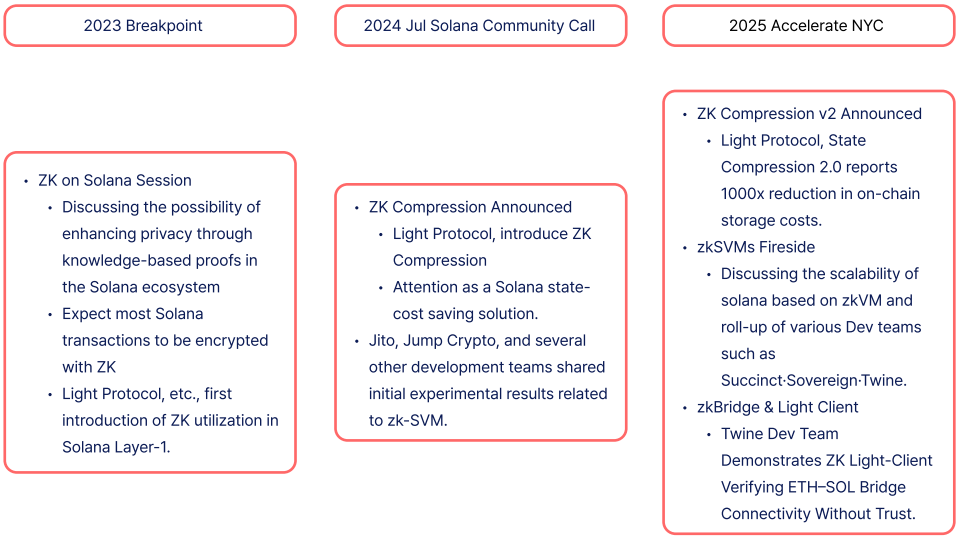
5

Understanding the ZK Trend in SOL through Accelerate

The Solana Foundation hosts an annual conference called "Accelerate" (which was rebranded from "Breakpoint"). The keynotes at this event reveal the significance of how ZK technology is being applied within the ecosystem and the developmental progress it is undergoing. For instance, the 2023 Breakpoint event featured a session titled "ZK on Solana: Private Solana Programs."

In addition to this, relevant information can be found in the "Solana Ecosystem Call," which is held on the first Thursday of every month. The Ecosystem Call in July 2024 included an announcement about the official launch of ZK Compression — one of the key technologies this report will focus on.

Figure 4. zk-related issues announced at Solana-related events



Source : PDAO

II. Zero—Knowledge Proof

6

The Concept and Principles of Zero-Knowledge Proofs

This chapter provides a brief introduction to Zero-Knowledge Proofs. A Zero-Knowledge Proof (ZKP) is a cryptographic method where one party (the prover) can prove (Proof) to another party (the verifier) that they know certain information (Knowledge) without revealing the information itself (Zero). A classic example used to explain ZKP is the "Ali Baba's Cave" analogy.

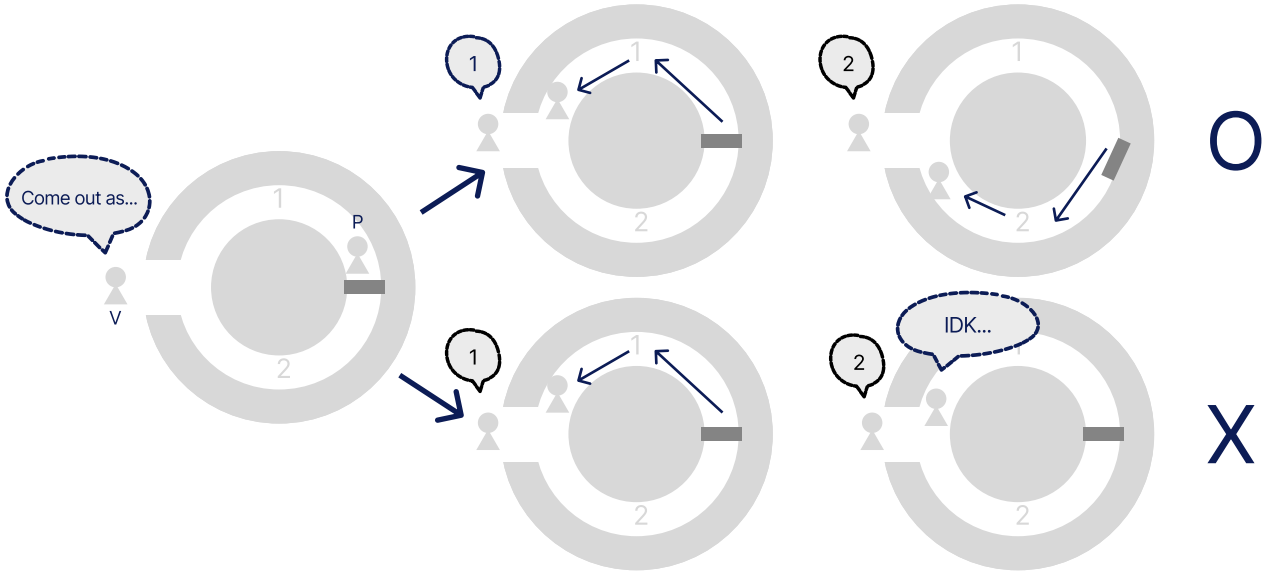
Let's say there are two individuals: P (the Prover) and V (the Validator). V wants to confirm that P knows the password to a locked door, but V does not want to learn the actual password. The goal is to prove knowledge of the information (the password) without disclosing it.

To achieve this, the cave has a single entrance that splits into two paths, Path 1 and Path 2, which are connected at the back by a door that requires a secret password.

P goes into the cave and walks down one of the paths. V, who waits outside, then randomly shouts for P to emerge from either Path 1 or Path 2. If P knows the password, they can unlock the door and move to the other path if needed, allowing them to always emerge from the path V calls out. However, if P does not know the password, they will eventually be unable to comply with V's request if asked to exit from the path they did not originally enter.

If this test is run only once or twice, P might pass by sheer luck (a 50% chance each time). But if the process is repeated dozens of times, and P successfully follows V's command every single time, it becomes probabilistically certain that P genuinely knows the password.

Figure 5. Alibaba's Cave Case.



Source : PDAO

This is the mechanism behind an "interactive ZKP," one of the most classic and representative forms of Zero-Knowledge Proofs. This method illustrates the three core properties that a ZKP must have:

- Completeness: If the prover (P) genuinely has the information, they can always convince the validator (V).
- Soundness: A dishonest prover who does not have the information cannot trick the validator.
- Zero-Knowledge: The validator (V) learns nothing other than the fact that the prover's claim is true.

7

The Advent of Non-Interactive ZKPs: The Catalyst for Using ZK in Blockchain

As described with the Ali Baba's Cave example, interactive ZK Proof methods require repetitive communication between the prover and the validator. This drawback leads to high transaction costs and significant time consumption, making them impractical for real-world applications.

However, with advancements in hardware and ongoing research, a non-interactive method for implementing ZKPs—known as zk-SNARKs—emerged. This innovation, which removes the need for back-and-forth interaction, dramatically increased the practical utility of ZKPs.

Following this breakthrough, blockchain scalability solutions like zk-Rollups and zk-EVMs were developed, helping to accelerate blockchain performance. More recently, various advanced algorithms such as zk-STARKs, which offer further improvements in speed and transparency, are being actively researched.

8

Characteristics of ZK and Its Significance in the Crypto Industry

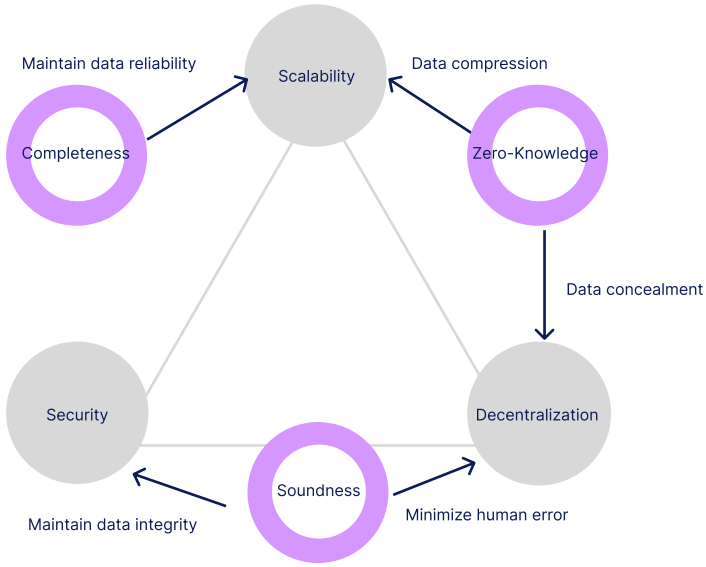
The adoption of ZK technology in blockchain began because its core characteristics can help address the "Blockchain Trilemma." The trilemma refers to the significant practical difficulty of simultaneously achieving the following three properties, which are essential for a blockchain's sustainability:

- Scalability: The ability to handle high transaction speeds and throughput to support large-scale user demand.
- Decentralization: All network participants must be able to participate equally in validation and decision-making.
- Security: The network and its data must be safely protected from malicious attacks.

The features of Zero-Knowledge Proofs can be used as a complementary measure to address the three aspects of the blockchain trilemma. For instance, the “zero-knowledge” property enhances decentralization by providing data privacy, as no one needs to see the original data. At the same time, ZKPs can be used for data compression, which contributes to greater scalability.

In this way, ZK technology is being utilized as a crucial tool to enhance sustainability within the blockchain ecosystem. Starting from the next chapter, we will examine specific case studies of ZK technology applied in the Solana ecosystem to understand the positive impact it is having on the crypto industry.

Figure 6. The relationship between the three elements of ZK technology and the blockchain Trilema



Source : PDAO

III. ZK Compression

9

What is ZK Compression?

ZK Compression is a technology announced by Light Protocol and Helius Labs in late 2023 that enables data to be stored in a compressed format on the Solana chain. It has been shown to reduce on-chain storage costs by up to 1,000 times compared to conventional methods. This is expected to have a significant impact on the growth of the Solana ecosystem by enabling capabilities such as large-scale, low-cost airdrops.

10

The Problem of High Storage Costs in Solana

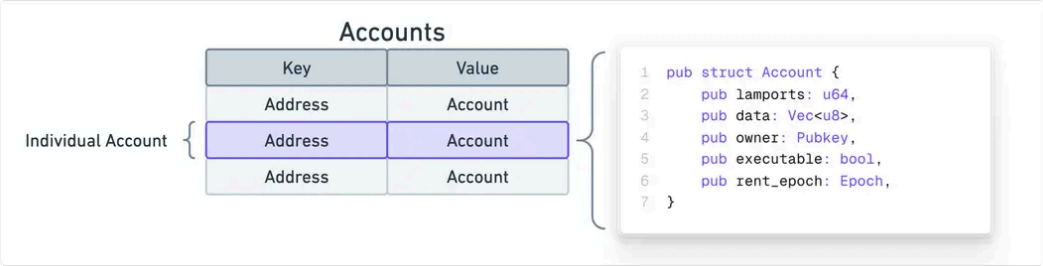
Types of Blockchain Information

Data recorded on a blockchain can be broadly divided into two categories: Code and State. "Code" refers to execution logic, such as smart contracts, while "State" refers to the values of various variables, like account balances. In Solana, these are called Program Accounts and Data Accounts, respectively.

Solana stores all the **various types of information*** on its blockchain in units of space called "Accounts." To prevent the reckless creation of these Accounts, a user must maintain a minimum balance known as "rent" to create a new Account. This rent is proportional to the amount of data being stored.

However, this rent can be prohibitively expensive. For example, creating an Account that stores the maximum capacity of 10MB of data would require paying approximately 70 SOL (as of June 2025), a significant cost.

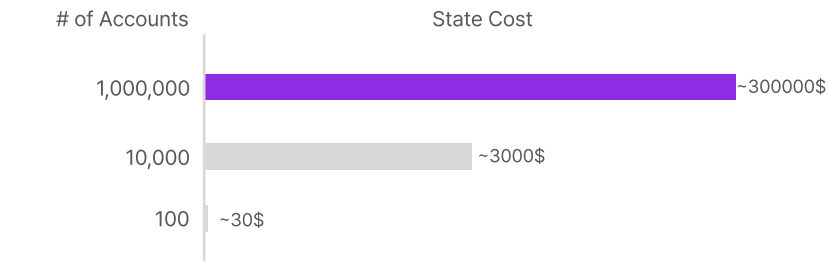
Figure 7. Accounts in the Solana Ecosystem



Source : Solana Labs

These high account costs fundamentally limit Solana's scalability. Even if the network can handle tens of thousands of transactions per second, the total cost of creating accounts grows exponentially as the user base expands. For example, onboarding one million users would require a massive amount of SOL for rent. This creates a significant barrier to entry for dApps aiming for mass adoption, forcing developers to resort to workarounds like consolidating data from multiple users into a single account or using off-chain storage.

Figure 8. Cost of generating large amounts of general accounts in Solana (assuming 1SOL = 150USD).



Source : PDAO

Cost Reduction through State Compression

State Compression is a technology developed for Solana by engineers from Solana Labs and Metaplex, designed to address Solana's high storage cost issues.

Instead of storing all data directly on-chain, it utilizes a structure called a Merkle Tree to store only a core summary of the data. A Merkle Tree has a tree-like data structure and represents data in the following way:

1. Each individual piece of data (the leaf nodes) is put through a **hashing*** process.
2. Pairs of these hashed data are then combined and hashed again. This process is repeated until only a single hash remains, which is known as the Root Hash.
3. Only this single Root Hash is stored on the blockchain, while the actual detailed content is kept in a separate **Ledger***.

Due to the properties of hashing, the existence of a specific piece of data can be verified without needing the entire dataset. Furthermore, if any data is altered, the Root Hash will change, allowing for the immediate detection of tampering.

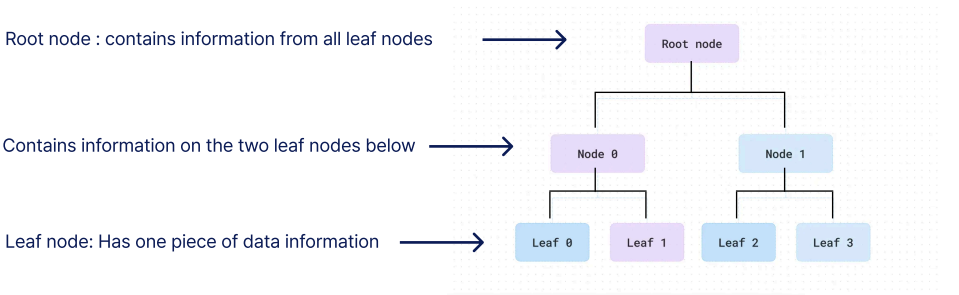
Hashing

A technique that converts data into a short, unique cryptographic code. It is used to verify integrity and detect tampering because even a slight change in the original data results in a completely different output value.

Ledger

A distributed ledger that stores the entire transaction history of a blockchain. In the context of Solana, this refers to the database managed by the nodes.

Figure 9. Image of tree data structure



Source : PDAO

When examining the cost-effectiveness of State Compression using standard NFT metadata (approximately 380 bytes) as a baseline, the cost for a single NFT actually increases from $0.114 before compression to $0.25 after. This is due to the initial setup cost required for the Merkle Tree structure.

However, the benefits of compression become dramatic as the scale increases. For a 10,000 NFT collection, the cost drops from $1,140 to $248, achieving a saving of about 78% and lowering the per-item cost to $0.025.

This effect is even more pronounced for larger collections. For 1,000,000 NFTs, the cost plummets from $114,000 before compression to just $248 after, a reduction of over 99.8%. At this scale, the cost per NFT is a mere $0.00025, making it approximately 456 times cheaper than the uncompressed alternative.

12

Two Limitations of State Compression

Despite its advantages, State Compression still faced the following two limitations:

1. Account and Transaction Size Limits: While a Solana Account can technically store up to 10MB, the rent cost increases sharply for data exceeding 1232 bytes. More importantly, the proofs required to verify data within large (deep) Merkle Trees used by State Compression often exceeded Solana's transaction size limit of 1232 bytes, making them difficult to process.

2. Limited Extensibility: The technology originated from the development of Instagram's NFT project before being broadly introduced to Solana. While it was highly effective for minting large NFT collections—achieving over 99.9% rent savings by storing data off-chain—it was specifically designed and optimized for the NFT metadata schema. This specialized design resulted in a lack of extensibility, making it difficult to apply to other use cases beyond NFTs.

13

The Evolution from State Compression to ZK Compression

ZK Compression expands the core concept of State Compression to all Solana account types. The key idea is to store account data off-chain, leaving only a 32-byte hash on-chain, while using Zero-Knowledge Proofs (ZKPs) to guarantee the data's integrity.

To achieve this, ZK Compression uses a type of account called a **Compressed PDA***, which has a structure similar to a standard Solana account and records the following information:

- Owner: The program ID with the authority to modify the account.
- Lamports: The SOL balance.
- Data: The field for storing the program's state.
- Address: An optional field used only when uniqueness is required.

Compressed PDA (Program Derived Address)

A special account address on the blockchain that is automatically generated and managed by a program. The concept is similar to a virtual account number that a bank automatically creates for its customers.

Along with this account data, a leaf node is created by adding two more pieces of information: the **State Tree Hash*** and the **Leaf Index***. By recording these two values alongside the account information, each compressed account can be globally and uniquely identified, even when multiple State Trees exist.

ZK Compression introduces a Validity Proof based on **Groth16***. Whenever a compressed account is read or modified, a 128-byte Zero-Knowledge Proof is generated. This proof confirms that the account validly exists within the State Tree without revealing the actual underlying data.

Light Protocol then verifies this proof on-chain to confirm that the off-chain data has not been tampered with.

State Tree Hash

A unique cryptographic code that represents an entire data structure (a State Tree). It summarizes a whole tree structure, which can contain information for thousands of accounts, into a single, short code.

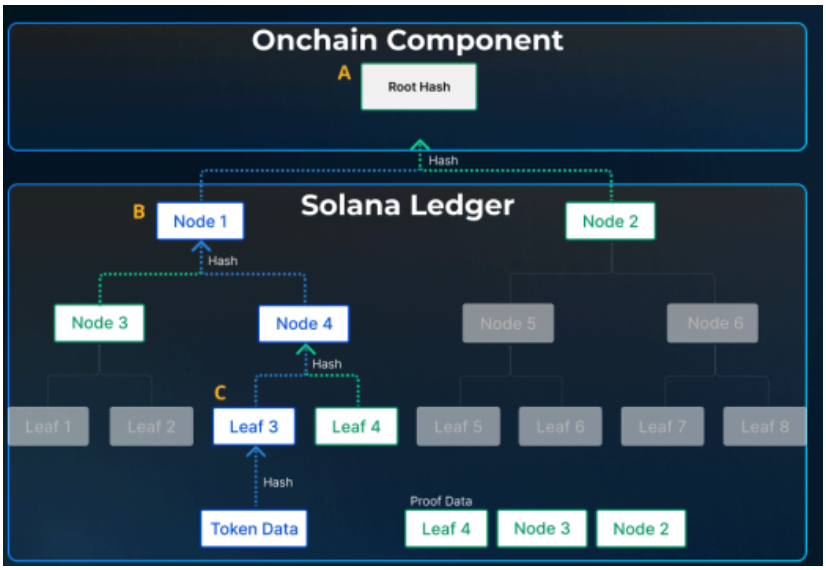
Leaf Index

A number indicating the position of a specific piece of data (a leaf) within a Merkle tree.

Groth16

A type of Zero-Knowledge Proof algorithm known for its ability to generate extremely small proofs (as small as 128 bytes) that can still be verified very quickly.

Figure 10. Merkle Tree Structure Utilized in ZK Compression.



Source : Messari

14

The Impact of Adopting ZK Compression

With the introduction of ZK Compression, the estimated cost to create 100 compressed token accounts is just 0.00004 SOL. This is approximately 5,000 times cheaper than the 0.2 SOL required to create the same number of standard accounts. To put it another way, creating one million token accounts using the traditional method would cost around $300,000; with ZK Compression, it costs only $50.

This groundbreaking level of cost reduction is welcome news for projects that require large-scale token minting or account creation and were previously burdened by high costs. It allows applications that need thousands or even millions of accounts—such as for airdrops, large NFT collections, and in-game items—to be developed without the concern of prohibitive expenses.

15

ZK Compression vs ZK Rollup

ZK Compression shows clear differences from the ZK-Rollup methods that have been widely used in the Ethereum ecosystem.

A ZK-Rollup is a Layer 2 scalability solution that processes hundreds of transactions off-chain and then submits the results to the mainchain along with a Zero-Knowledge Proof. This allows the mainchain to verify the validity of the entire batch without processing each transaction individually. ZK-Rollups can handle hundreds to thousands of transactions per second while inheriting the full security of the mainchain, offering gas fee reductions of up to 99%.

The most fundamental difference between ZK Compression and ZK-Rollups lies in their operational scope and purpose. While ZK-Rollups focus on “horizontal scaling” by building a separate Layer 2 network to increase transaction throughput, ZK Compression pursues “vertical optimization” by compressing data within the mainchain to enhance storage efficiency.

Architecturally, ZK-Rollups require additional infrastructure like sequencers and provers, and a bridge between the mainchain and the Layer 2 is essential. In contrast, ZK Compression can be directly integrated into existing programs without needing a separate network configuration. Furthermore, ZK-Rollups must still post transaction data on-chain for data availability, whereas ZK Compression saves storage space by replacing the original data with a compressed proof.

calldata

The essential data containing the details of a transaction that must be sent to the blockchain to execute it.

These differences do not imply that one technology is superior to the other. Rather, the two are complementary and can maximize a blockchain's efficiency when used together. By utilizing ZK Compression within a ZK-Rollup, the rollup's **calldata*** can be further compressed, leading to additional savings on Layer 1 storage costs. Theoretically, this has the potential to significantly increase the number of transactions a ZK-Rollup can handle.

The combination of these technologies becomes a particularly powerful solution for enterprise applications where privacy is critical. This is because high throughput can be achieved with ZK-Rollups while sensitive transaction information is protected with ZK Compression. This hybrid approach is expected to become a cornerstone of next-generation blockchain infrastructure that simultaneously delivers scalability, privacy, and cost-effectiveness.

Figure 11. ZK Compression vs ZK Rollup Comparison

Area	ZK Compression	ZK Rollup
Data Compression	Operates directly on L1	Requires a separate L2 network
Transaction	Reduces data storage costs	Increases transaction throughput
In-Proof Operation	No additional infrastructure needed	Requires sequencer, prover, and bridge
Data Processing	Only compressed state stored on-chain	All transaction data stored on-chain

Source : PDAO

16

Product Use Case for ZK Compression

A prime example of a product utilizing ZK Compression is Airship, developed by Helius Labs. Airship is an open-source tool that leverages ZK Compression to reduce the cost of Solana token airdrops by up to 5,000 times. Whereas it previously cost 20 SOL (approximately $2,800) to distribute tokens to 10,000 people, Airship makes it possible for just 0.01 SOL (approximately $1.40).

The SLINKY token was distributed to 27.77 million wallets using Airship, marking the largest-scale airdrop in Solana's history. These compressed tokens can be instantly converted into standard tokens whenever needed, ensuring compatibility with existing infrastructure like the DeFi ecosystem.

Figure 12. ZK Compression Use Case—Airship.

Source : Helius

IV. zkSVM

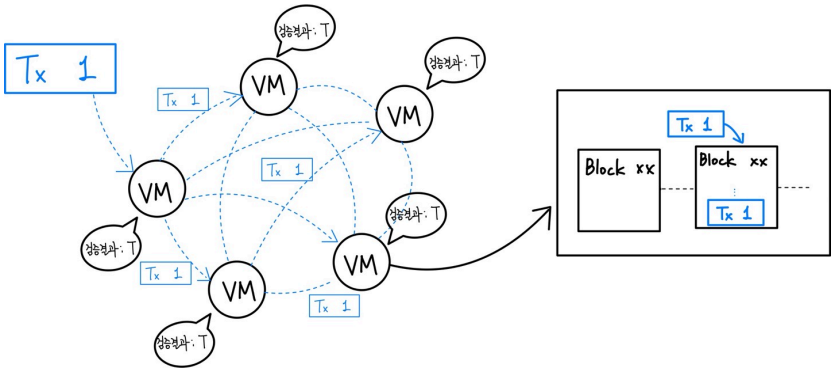
17

What is a zkVM?

A zkVM is a special type of Virtual Machine (VM) where the execution of a program can be verified using a Zero-Knowledge Proof. A virtual machine is, as the name suggests, a virtual computer environment. In the blockchain ecosystem, it can be described as a specialized environment built to process transactions. You can think of a single node in a typical blockchain network as one of these VMs.

For example, let's say a transaction is created. This transaction is broadcast across the blockchain network, and each virtual machine validates it. Based on the validation results from the nodes, a decision is made to either approve or reject the transaction according to the chain's consensus algorithm. If approved, the transaction is added to a block.

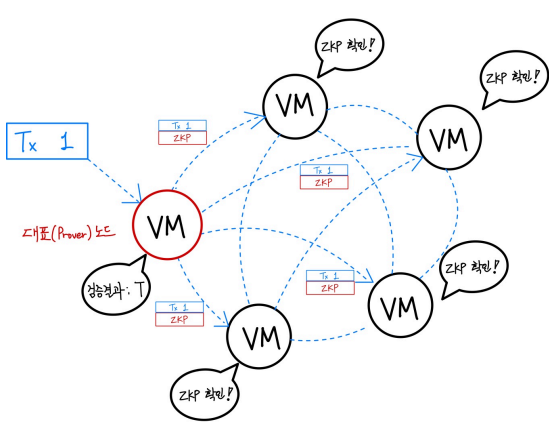
Figure 13. Transaction verification process in general chain.



Source : PDAO

While a traditional virtual machine simply executes code, a zkVM goes a step further by also generating a cryptographic proof that the execution was performed correctly. This proof is then transmitted to other nodes along with the transaction. In this model, instead of every node independently re-executing the entire computation, it is sufficient for just one or two representative nodes (Provers) to validate the transaction. The other nodes can then confirm the transaction's validity simply by verifying the proof generated by these representative nodes, without having to perform the computation themselves.

Figure 14. Transaction Verification Process in zkVM.



Source : PDAO

18

Features of a zkVM

The architecture of a zkVM is far more complex than that of a traditional VM, comprising several specialized components that work together seamlessly.

- Execution Engine: This is the heart of the zkVM. It runs the program and meticulously records every state change. This process goes beyond simple execution, tracking all details, including the inputs and outputs of each instruction, memory access patterns, and register states.
- Arithmetization Module: This module converts the execution trace into a set of mathematical constraints. During this process, the logical flow of the program is transformed into a system of polynomial equations.
- Proof System: The Proof System generates a Zero-Knowledge Proof attesting that all of these mathematical constraints have been satisfied. This is achieved through complex cryptographic protocols, and the specific method differs depending on the chosen proof system (e.g., SNARK, STARK).
- Verifier: The Verifier is responsible for confirming the validity of the generated proof. The verification process is significantly faster than proof generation, which is how it contributes greatly to a blockchain's scalability.

19

zkSVM?

Each blockchain network handles data differently, so it's necessary to use a virtual machine specifically suited for each chain. For instance, what is handled by a single smart contract on Ethereum is separated into Programs and Accounts on Solana.
A zkSVM, then, can be understood as a zkVM that is specifically tailored for use on the Solana chain. By executing complex computations off-chain and only verifying a simple proof on-chain, it boosts processing speed, dramatically cuts costs, and ensures complete privacy. Currently, several companies, such as Zpoken, are leading the development in this field.

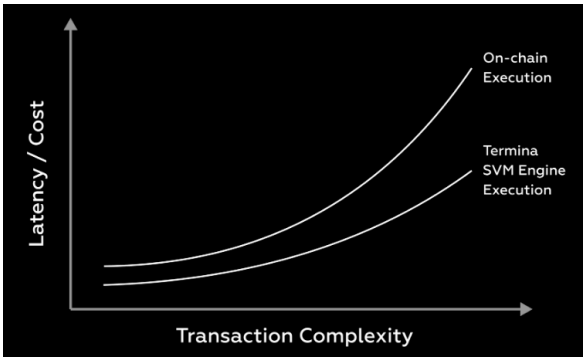
20

Expected Benefits of zkSVM—Cheaper and Faster

In April 2025, Solayer's InfiniSVM, a fast ZK proof system centered on GPU-accelerated parallel processing, achieved 340,000 Transactions Per Second (TPS) on its Devnet. Considering that Solana's actual average TPS at the time was around 1,200—and its theoretical limit is estimated to be about 65,000 TPS—this demonstrates the potential for zkSVMs to enable extremely high-speed transaction processing.

From a cost perspective, zkSVMs are also highly effective. Termina, for instance, offers zkSVM proving through Succinct Labs' sp1-solana. As of May 2025, Termina's documentation states that proving 100 complex SPL transactions using their zkSVM Prover costs less than $1.

Figure 15. the advantage of the Latency/Cost ratio using Terminala SVM



Source: Termina

21

Expected Benefits of zkSVM—Expansion to Other Chains

Sovereign SDK

A software development kit that helps developers easily create their own independent blockchains (appchains).

zkSVM is being designed to generate ZK Proofs from the results of programs run on the Solana Virtual Machine (SVM), enabling these proofs to be verified on other blockchains. Consequently, it is gaining attention as an interoperability solution that can securely transmit the outcomes of Solana programs to other chains.

zkSVM offers extensibility in the following ways:
First, it can use Solana's high-speed processing to execute transactions, then compress the resulting STARK proof into a Groth16 proof for efficient verification on other chains like Ethereum. This creates a hybrid solution that maximizes the strengths of each chain.

Second, universal zkVMs like SP1 enable trust-minimized bridges between Solana and other ecosystems. This improves security by replacing traditional multi-sig mechanisms with Zero-Knowledge Proofs. Appchains built with the **Sovereign SDK*** are already settling on Solana to take advantage of the benefits of zkSVM.

22

zkVM Product Use Case in the SOL Ecosystem

RISC-V Architecture

A simple, modular, open-source instruction set architecture that is used flexibly across a wide variety of hardware.

Precompile

A special, pre-compiled system contract on a blockchain designed to rapidly execute frequently used operations (such as hashing).

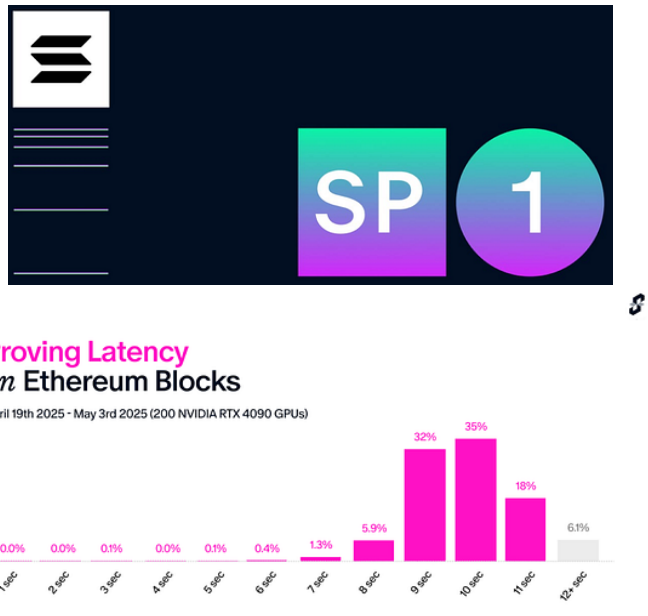
A key example of a zkVM product used in the Solana ecosystem is SP1 (Succinct Processor 1). Developed by Succinct Labs, SP1 is a zkVM that can generate Zero-Knowledge Proofs directly from standard Rust code. According to information released by Succinct Labs in August 2024, SP1 boasted performance up to 36 times faster than other zkVMs at the time. Although SP1 is a universal zkVM compatible with multiple chains, it became accessible to the Solana ecosystem in December 2024 with the release of its Solana Verifier library.

SP1 is built on the **RISC-V*** architecture and achieves high performance thanks to a crucial feature: a **precompile***-centric design. It processes core cryptographic operations—like SHA256 and Keccak256 hashing, and secp256k1 and ed25519 signature verification—with highly optimized circuits, reducing the required RISC-V cycles by a factor of 5 to 10.

On a single machine, SP1 shows a throughput of 900 KHz to several MHz, and it can achieve near-real-time proof generation when using a GPU cluster. In May 2025, SP1 Hypercube was introduced, further improving performance to enable real-time proving of Ethereum blocks. Published data shows that SP1 Hypercube is extremely fast, capable of proving over 93% of Ethereum blocks in under 12 seconds.

From a Solana developer's standpoint, SP1 offers the major advantage of supporting the languages used for Solana program development, like Rust and C++. This means developers can run their existing code on the zkVM with almost no modifications to leverage its high-performance computation. Several projects within Solana, including Spicenet, Termina, and Soon, are already using SP1. It has also completed security audits from Veridise, Cantina, and KALOS, confirming it is safe for use in production environments.

Figure 16. SP1 in Solana Verifier (up), Real-time Ethereum Proving (down).



Souce: Succinct

V. zkBridge (ETH - SOL)

23

The Significance of Bridges in the Crypto Ecosystem

Blockchains are designed to maintain network security by rewarding participants with native crypto assets for adding new blocks. These assets are inherently a means of reward valid only within their own blockchain and lack direct compatibility with external chains.

However, because each blockchain has a different user base, security model, design philosophy, and especially, a different economic structure, there's a growing demand to use assets from one chain on another.

The technology that fulfills this need is the bridge. A bridge is a system that transfers data or moves assets between two or more blockchains, enabling interoperability between these otherwise disconnected chains.

You can think of the creation of wrapped tokens as a direct result of this technology. For example, to use Ethereum's native ETH on the Solana chain, a bridge is used to lock the ETH on Ethereum and mint an equivalent amount of WETH (Wrapped ETH) on Solana.

24

The 2022 Ronin Hack and the Need for zkBridges

Multi-signature (Multisig)*

A method that requires signatures from multiple users before a transaction can be executed.

Relay Server*

A server that submits a blockchain user's transaction on their behalf, allowing the user to use a service without needing to pay gas fees directly.

Single Point of Failure (SPOF)*

A vulnerable part of a system where, if it fails, the entire system will stop working.

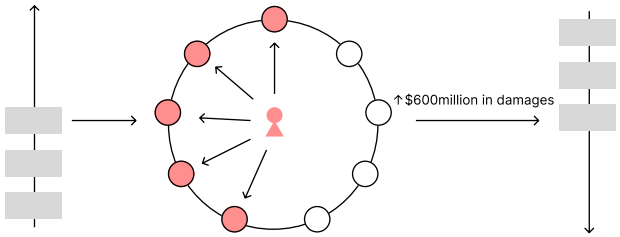
Traditional bridges typically rely on trusted intermediaries, such as a **multi-signature*** structure, a centralized **relay server***, or a set of delegated validators. This architecture can create a security **single point of failure*** and has been the root cause of severe security issues, including major bridge hacks.

A prominent case is the Ronin Bridge hack of 2022, which starkly exposed the structural vulnerabilities of such trusted bridges. At the time, Ronin used a multi-signature (multisig) scheme that required approval from 5 of its 9 validator nodes to process asset transfers between Ethereum and its native sidechain.

The attackers managed to acquire five private keys through methods that have not been fully disclosed, allowing them to steal over $600 million (approximately 700 billion KRW). This incident clearly demonstrated a critical structural flaw: the entire system could be compromised by controlling just five nodes.

Following the event, Ronin's operators announced they would strengthen security by revoking the compromised nodes' permissions and increasing the required signature threshold from 5 to 8. They also revealed plans to expand the total number of nodes in the network. However, these measures still fail to fundamentally solve the problem of "who to trust."

Figure 17. Vulnerability of Multi-Sign Method (Ronin Bridge Hacking).



Source : PDAO

A zkBridge does not require trust in any specific set of validators. Every transaction can be verified by anyone through a cryptographically generated zero-knowledge proof, creating a structure where threats like a **man-in-the-middle (MITM) attack*** or an insider attack are fundamentally invalid.

As such, ZK-based bridges represent a technological evolution that shifts the security model from 'trust-based' to 'math-based,' significantly elevating the security and reliability of bridge technology.

Man-in-the-Middle (MITM) Attack*

A type of hacking where an attacker intercepts communication between two parties to secretly eavesdrop on or manipulate the data being exchanged.

25

Asset Transfer Between ETH and SOL Using a zkBridge

In a November 2021 article, the =nil; Foundation detailed the process of verifying Solana's chain activity on Ethereum using a **Light Client*** and ZKPs.

Light Client

A client that interacts with the blockchain by verifying only the minimum necessary information, without needing to store the entire blockchain's data.

Figure 18. ETH—SOL Token Transfer Process.

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.

Source : PDAO

26

Advantages of Using a zkBridge

between chains, which can create structural trust issues. In contrast, a zkBridge enables verification without trusting any third party by directly proving a transaction's validity with a zero-knowledge proof. This approach significantly enhances security and decentralization while also strengthening censorship resistance. Since a primary role of bridges is to transfer tokens, improving the security and decentralization of this process contributes directly to the healthy development of the entire blockchain ecosystem.

Technically, a zkBridge also compresses a large amount of complex transaction data into a single, simple proof. This leads to lower verification costs and more efficient on-chain data storage. Furthermore, through the use of ZK circuits, a zkBridge can support various chain structures under a single protocol, providing a superior architecture for scalability and interoperability. These technical advantages create a strong foundation for zkBridges to become a core piece of infrastructure in the multi-chain ecosystem.

Figure 19. Comparison of the characteristics of existing bridges and zkBridge.

Features	Bridge	zkBridge
Competitive dependency	High	Low
Verification cost	High	Low
Scalability	Low	High
Interoperability	Low	High
Degree of decentralization	Low	High

Source : PDAO

27

zkBridge Project Use Cases in the SOL Ecosystem

The practical adoption of zkBridges is gradually expanding within the Solana ecosystem. A leading example is the Solana-Ethereum zkBridge prototype, jointly designed by the Wormhole team and the =nil; Foundation. This implementation verifies Solana's light client on Ethereum using zk-SNARKs. The design converts Solana's block headers and state transition data into a ZK circuit, which is then submitted to Ethereum, enabling trustless state synchronization without third parties.

Light Protocol is also developing a new solution on Solana that combines privacy and bridging functions using ZK technology. This is gaining attention as a foundational technology for future expansions into zk-Rollups and zkBridge-based interoperability.

Wormhole, a multi-chain bridge that originated in the SOL ecosystem, is also progressively implementing zkBridge technology. In 2024, Wormhole officially announced a roadmap to transition from its existing message verification structure, which relied on 19 "Guardians" (its validator network), to a permissionless verification system based on zero-knowledge proofs (ZKPs). In collaboration with Lurk Lab, Wormhole is currently preparing to introduce a ZK light client that will use zk-SNARKs to easily generate proofs and perform ZK-based message verification across multiple chains.

VI. Conclusion

28

Why Investors Should Pay Attention to the Advancement of ZK Technology in SOL

Throughout this report, we have explored what Zero-Knowledge (ZK) technology is and how it is being utilized within the Solana ecosystem. However, for some investors, this discussion might feel abstract—a technical narrative disconnected from market reality.

In the crypto market, it's often said that assets "lack fundamentals." This is because their prices are difficult to explain using traditional valuation models. As a result, investors often interpret price indirectly, based on metrics like coin supply and demand, user count, transaction throughput, the number of projects, community activity, and recurring market narratives.

Ultimately, technological progress lies at the foundation of all these metrics. Without technologies like ZK, blockchains would inevitably hit their limits in terms of user growth, transaction volume, and the capacity to host new projects. Conversely, advancements in ZK technology provide the foundation to break through these limits, becoming a key element in forming the very narratives that positively influence price.

Solana, in particular, is one of the most active Layer 1 chains today. It consistently sees a stream of new projects, memecoins, launchpads, and diverse user inflows, distinguishing itself in terms of technical scalability and ecosystem diversity. If structural advancements based on ZK technology are added to this mix, Solana can secure a foundation for sustainable growth that goes beyond short-term trends.

Indeed, for Ethereum in 2025, the Pectra Upgrade and Vitalik Buterin's roadmap announcement served as a turning point that reversed the stagnant price trend of ETH. Technology doesn't directly dictate price, but it creates the credible narratives that move it. Viewed in this context, ZK technology is not just a technical term but a basis for value judgment that investors must consider. The development and ecosystem application of ZK-related technologies—not only in Solana but across the entire crypto market—can become a tangible factor that helps investors make informed decisions. We hope this report has been a helpful starting point for understanding that.

Outro.

ZK has long played a vital role in the blockchain ecosystem, and it will continue to do so. As ZK-based blockchain infrastructure companies and projects move forward with their own token launches, a solid understanding of the technology will become increasingly important for investors.

On July 3, 2025, Google announced on its official blog that it was open-sourcing a library based on Zero-Knowledge Proof (ZKP) technology. This signals that understanding ZK is also becoming crucial for interpreting the exponential advancements in the current tech paradigm, especially those centered around Large Language Models (LLMs).
Amidst these powerful trends, we hope this report has offered you, the reader, a new perspective and will serve as a small milestone in making future technology-based investment decisions.

PDAO

PDAO is a crypto-blockchain community based at POSTECH (Pohang University of Science and Technology).

PDAO began in early 2022 as a crypto community and open-source development group at POSTECH. Built on the identity of being "a DAO that develops DAOs," it created the decentralized DAO protocol, Simperby, and has used it to host itself. Additionally, PDAO has contributed to the blockchain industry as a development organization through its members' participation in various hackathons and its involvement in the 2023 open-source contribution project under the South Korean Ministry of Science and ICT.

As of 2025, PDAO operates as an open community where anyone can freely join. It functions as an organization where people interested in the blockchain ecosystem can plan and engage in various activities to contribute to the industry. In the first half of 2025, this has included planning, operating, and participating in projects with various foundations and companies, such as serving as the Superteam KR Guild Lead and as Monad Blitz Seoul Supporters.

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)