ZKApps 101

An Overview and Outlook of the ZKApps Landscape

Presto Research

ocular | OPENSPACE

July 29th, 2024

Jaehyun Ha | Research Analyst
jaehyunha@prestolabs.io

Yi-wei Lin | Analyst
yi-wei@ocular.vc

Summary

- The current ZK landscape can be broadly classified based on two main criteria. The first criterion is whether it functions as an application or as infrastructure, and the second is whether it prioritizes privacy or focuses on better utility and scalability.
- Among them, ZK-applications (ZKApps) are applications that leverage zero-knowledge proofs to enhance privacy and utility. ZKApps can benefit our lives especially in areas like credentials, payments, and even biomedical engineering.
- Investing trends and on-chain data suggest a growing recognition of the burgeoning demand for Zero-Knowledge Proof (ZKP) usage, indicating that the retail side has begun to embrace relevant applications.
- ZKApps have become more practical and feasible thanks to technical advancements in cryptographic proof systems and decentralized proving infrastructures. These developments have lowered the barriers of ZKP generation and verification processes, enabling more people to use ZKApps.

ZKApps 101:
An Overview and Outlook of the ZKApps Landscape.
RESEARCH PARTNERSHIP
Presto Research × ocular | OPENSPACE

Contents

1. Introduction

Why should we pay attention on ZKApps now?

The hype around Zero-Knowledge (ZK) technology in the Blockchain and Web3 industry has continued for several years and persists into the second half of 2024. As Vitalik Buterin stated, "*While further infrastructure development and prover optimization will be needed, **ZK will be the clear endgame** within 10 years*", ZK is undoubtedly regarded by industry insiders as a promising technology for solving the blockchain trilemma, which involves balancing Security, Scalability, and Decentralization without sacrificing any one of them.

Riding this wave of hype, many investors, irrespective of their technical expertise, have likely heard about terms such as SNARKs, STARKs, and KZG, which are technologically complex field and are being researched and developed particularly within the Ethereum community. However, from the consumer's perspective, one fundamental question inevitably arises: "I understand that ZK is a impressive technology, but when can we actually use a cool product that leverages it? And is the technology mature enough to replace existing non-Web3 solutions?".

Even a few years ago, the answer to this question would have been, "Not yet, and we don't know". As Vitalik mentioned, the infrastructure and cryptographic proof technologies needed to practically run ZK-based applications (ZKApps) on the client-side were still lacking, making its development challenging. However, as of 2024, although there is still much room for improvement, significant technological advancements have been made, allowing the potential for ZKApps commercialization to take root. Therefore, we now need to shift our focus to identifying the fields where ZK technology is truly needed and contemplating how to leverage it to practically improve the quality of our lives. From an investor's perspective, studying the categories of ZKApps that will be widely adopted in the future can also present promising new opportunities.

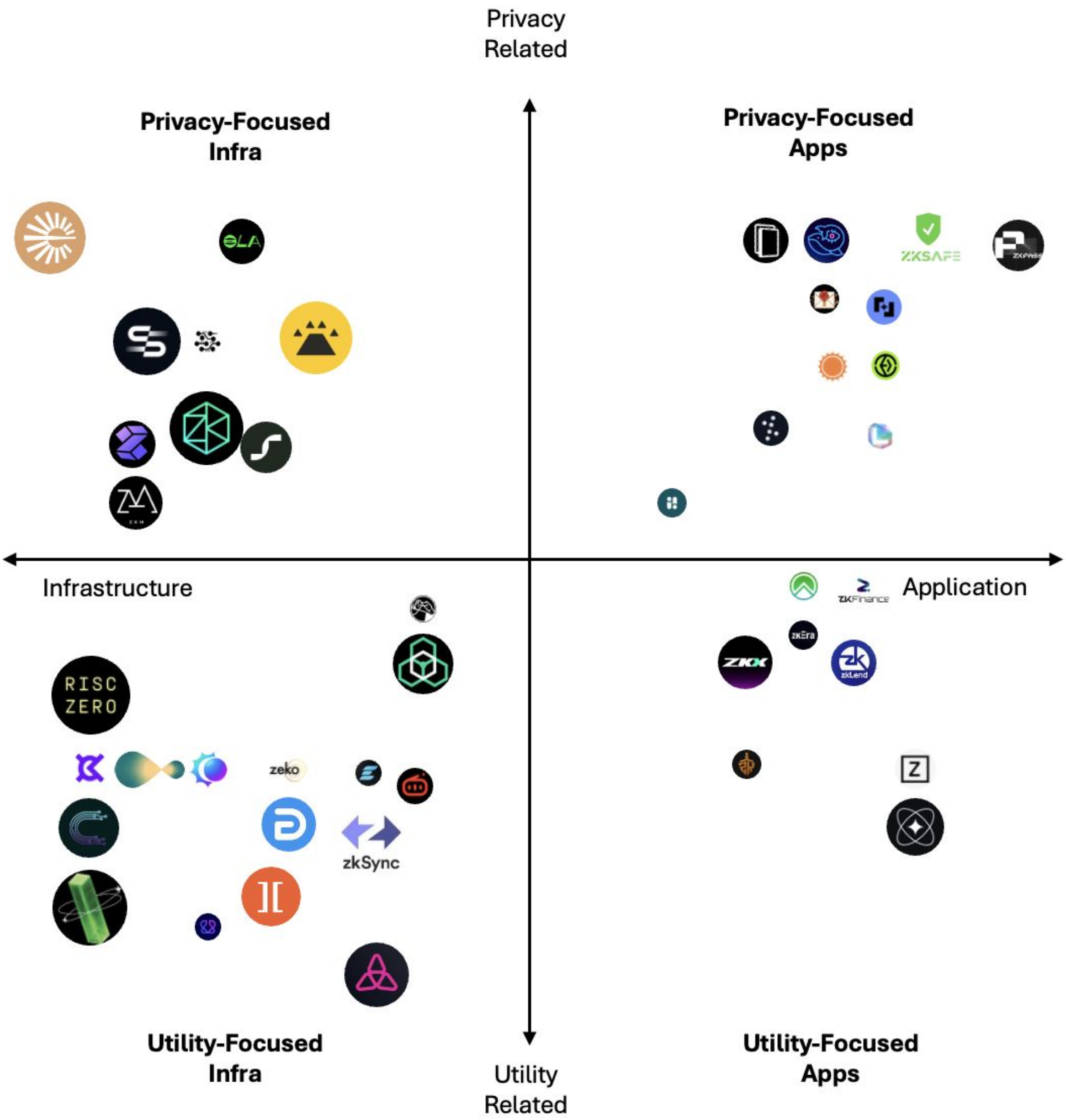
In this joint ZK research by **Presto Research** and **Ocular VC**, we provide an overview and outlook of the ZKApp industry, leveraging marketing trend analysis and cutting-edge technology insights from both research groups. In Section 2, we first cover the current ZK adoption landscape and highlight which ZK Infrastructures and ZKApps are gaining attention. Among them, Section 3 hones in on ZKApps' development history, discussing their necessity and practical benefits. In the following Section 4, we examine the investment trends and on-chain data analysis in the ZK industry as of 2024, explaining why ZKApps are poised to become the next major trend. Lastly, in Section 5, we will discuss the on-going R&D efforts and technical achievements thus far in infrastructures to make ZKApps practical and a mainstream trend.

2. Current ZK Adoption Landscape

The current ZK adoption landscape can be categorized under many different criteria, but here we broadly bucket them based on the following: whether the service functions as an infrastructure or as an application, and whether it prioritizes privacy by leveraging the zero-knowledge property, or prioritizes utility by leveraging the succinctness property.

Figure 1: Current ZK Adoption Landscape

Source: Ocular VC



2.1. ZK Infrastructure

Type 1: Privacy-focused infrastructure

Services in this category primarily aim to address privacy issues in ZK systems, as many ZKP providers may still have the capability to inspect transactions, posing a risk of sensitive data exposure. In other words, privacy leakage often occurs during the process where clients submit their transactions to a ZKP provider to create a ZK proof. Thus, these privacy-focused infrastructure can be offered through both the prover layer (more explanations in Section 5.2) and the virtual machine (VM) component to enhance access control and ensure end-to-end data privacy. Representative examples include Ingonyama, Succinct, and Espresso.

Type 2: Utility-focused infrastructure

ZK technology is not only useful for preserving privacy but also for enhancing the utility of ZKApps. One of the best examples of leveraging the utility of ZK is ZK L2 (i.e., ZK-rollups). It is now a well-known fact that among the ongoing ZK L2s, there are very few instances that actually guarantee end-to-end transaction privacy. Nevertheless, ZK L2 chains such as Taiko, zkSync, Intmax, and Zeko leverage the succinctness property of ZK technology to greatly enhance blockchain scalability by consolidating the validity of thousands of transactions into a single ZK proof and submitting it to L1. Another utility-focused use case is the prover layer. Prover layers are entities that provide computational power to help individuals with weak devices participate in the ZKP generation and verification process. Services such as RiscZero, Cysic, Irreducible, and Aligned Layer are currently operating in this space.

2.2. ZK Applications

Type 3: Privacy-focused applications

Privacy-focused applications are often the use case that first comes to mind when we think of "ZK Applications". Services in this category are primarily applications that leverage the zero-knowledge property of ZK technology and prioritize privacy above other properties. This property is widely adopted in fields that handle sensitive personal information, such as KYC, verification, and credentials, for protecting clients' privacy. Notable on-going projects include zkPass, Lumina, 0xKYC, and zkMe. This landscape is also expanding to areas such as secure wallets and emails, with examples like ZKSafe and zkEmail.

Type 4: Utility-focused applications

Utility-focused applications primarily operate on top of ZK L2s. Currently, DeFi-related applications such as DEXs and lending platforms dominate this space. Although ZK L2s do not guarantee privacy, these applications leverage the utility of ZK L2s in order to offer fast and low-cost transaction processing, which is crucial in the DeFi sector. Noteworthy applications currently in operation include zkFinance, ZKX, zkEra Finance, zkLend, and eZKalibur.

3. ZKApps: Origin and Evolution

3.1. The Roads to the Modern ZK Landscape

Zero-Knowledge Proofs (ZKPs) have emerged as a transformative technology within the blockchain industry, offering revolutionary advancements in privacy and scalability. Originating from cryptographic research, ZKPs have evolved from theoretical concepts into practical ZK applications (ZKApps), significantly shaping the landscape of decentralized finance (DeFi), cybersecurity, and beyond.

The Genesis of ZKPs

The concept of ZKPs was first introduced in 1985 by Shafi Goldwasser, Silvio Micali, and Charles Rackoff. Initially, it was a theoretical breakthrough in cryptography, demonstrating the ability to prove possession of certain knowledge without revealing that knowledge itself. ZKPs are particularly useful in authentication systems where passwords are involved, as they allow verification without exposing it. Notably, web infrastructure companies like Cloudflare have adopted ZKP mechanisms for secure web verification using vendor hardware.

Transition to Blockchain Technology

The integration of ZKPs into blockchain technology marked a pivotal moment in its evolution. One of the early adopters was Zcash, which introduced the ZK concept into its payment system to ensure end-to-end transaction privacy. ZKPs allow transactions to be verified (i.e., the sender has enough amount of coin, and it is not double-spended) without revealing the sender, receiver, or transaction amount. This use case highlights the potential for integrating ZKPs directly within blockchain platforms, presenting an intriguing application.

The expansion of ZKP integration gained momentum with the initial deployment on Ethereum L2 solutions like zkSync and Starknet. These platforms utilize ZKPs as scaling solutions to address the low TPS rates that are a common bottleneck in blockchain systems. The successful implementation of ZKPs in these contexts has spurred further interest in developing more practical applications that leverage the existing infrastructure, enhancing both privacy and efficiency.

As the infrastructure has consolidated and matured in the recent years, people are starting to look at ZKApps. We talk about the details and benefits of ZKApps in the following section.

3.2. Definition and Benefits of ZKApps

As briefly introduced from Section 2, we define ZKApps as a application which utilizes ZKPs and ZK Infrastructures to generate transactions that primarily aim to 1) preserve user privacy and/or 2) increase efficiency.

Focusing on the privacy aspect, applications which prefer not to store their transaction data (i.e., KYC procedures, gene testing, and confidential personal data) on public chains present compelling use cases. Leveraging ZKPs, these data can be safely stored in local database without revealed to the public, but can be verified (e.g., prove that Alice's blood type is B, prove that Bob is over 20 years old) globally. This approach is particularly advantageous for privacy-sensitive applications where accountability and transparency are also required. Projects working on this topic include zkPass, nuAuth, and BioSnark.

Bhutan, a small Asian country situated between India and China, is a case in point. The country has been utilizing ZKPs nation-wide to build their digital identity infrastructure in recent years. This approach makes it easier for the government to manage data while ensuring that it can be verified across borders without conflicting with other countries' data privacy regulations.

Interestingly, this use of ZKPs could be further implemented into **credit loan systems** and identity checking mechanisms, facilitating international cooperation and trust in shared digital services. For instance, USDT loans could utilize ZKPs to protect and verify off-chain credits. This approach could further facilitate the issuance of uncollateralized loans on chain using stablecoins. Such applications of ZKPs could revolutionize how credit is assessed and loans are issued, enhancing security and trust while expanding access to financial services.

There are still some underexplored fields, such as **GambleFi,** where this approach could be particularly beneficial. ZKPs enable fair and cheat-resistant gambling by cryptographically verifying outcomes and actions without exposing underlying data. An example can be creating betting pools where users' contributions and winnings are kept anonymous, but the total pool size and distribution are verifiable. These benefits can hopefully attract more users to GambleFi by fostering trust and offering a more private and scalable gambling experience.

The usage of ZKP is, of course, not limited to these examples. Beyond the mentioned use cases, ZKP can be introduced in social media to protect the anonymity of content creators, and top-ranked gamers who do not want to share their speedrun strategies may also welcome the adoption of this technology. As such, ongoing research explores how ZKP can offer more advanced services in various fields of our daily lives compared to existing methods, and more use cases will continue to be discovered in the future.

4. An Analysis: Why ZKApps Are the Next Trend

In this section, we provide a data-driven analysis of why the main trend in the ZK industry is shifting from infrastructure to applications. In Section 4.1, we explore why ZKApps are the next promising trend, based on the investment trends of 2024. And in Section 4.2, we examine how client demand for actual ZKApps has increased, using on-chain data as an evidence.

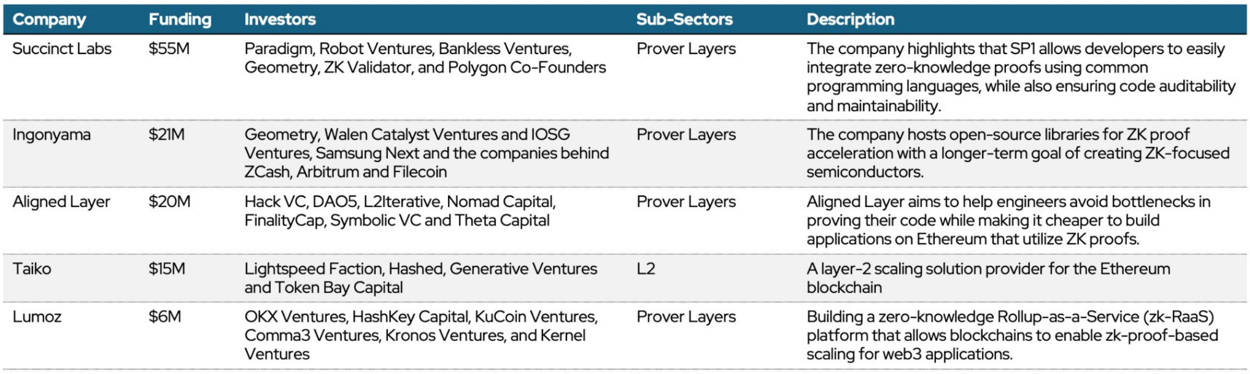
4.1. Investment Trends

When examining the investment history in the ZK industry, it's evident that most substantial investments have been directed toward ZK infrastructures (i.e., ZK L1/L2s, Hardware acceleration), including projects like zkSync, Starknet, Aleo, and Cysics. Cumulative investments towards this market have surpassed $1 billion, with many projects gearing up to launch products in the coming quarters. This trend continues into 2024, as evidenced by the robust performance of the top 5 ZK-related fundraising deals (Figure 2), four of which received investments exceeding $15 million. Notably, four out of the top 5 deals were related to **prover layers**, while one was related to L2 solutions.

Why is the prover layer receiving so much attention? As explained in Section 3, the prover layer is a critical component that supports the growing demand for ZKPs by enabling individuals with weak devices to participate in the ZKP generation and verification process. This increased demand for prover layers indicates a significant rise in the demand for ZKPs, suggesting that more people want to generate transactions from using ZK L1/L2s.

Figure 2: 2024 ZK investing trends

Source: Cointelegraph, The Block, Ocular VC



Company	Funding	Investors	Sub-Sectors	Description
Succinct Labs	$55M	Paradigm, Robot Ventures, Bankless Ventures, Geometry, ZK Validator, and Polygon Co-Founders	Prover Layers	The company highlights that SP1 allows developers to easily integrate zero-knowledge proofs using common programming languages, while also ensuring code auditability and maintainability.
Ingonyama	$21M	Geometry, Walen Catalyst Ventures and IOSG Ventures, Samsung Next and the companies behind ZCash, Arbitrum and Filecoin	Prover Layers	The company hosts open-source libraries for ZK proof acceleration with a longer-term goal of creating ZK-focused semiconductors.
Aligned Layer	$20M	Hack VC, DAO5, L2Iterative, Nomad Capital, FinalityCap, Symbolic VC and Theta Capital	Prover Layers	Aligned Layer aims to help engineers avoid bottlenecks in proving their code while making it cheaper to build applications on Ethereum that utilize ZK proofs.
Taiko	$15M	Lightspeed Faction, Hashed, Generative Ventures and Token Bay Capital	L2	A layer-2 scaling solution provider for the Ethereum blockchain
Lumoz	$6M	OKX Ventures, HashKey Capital, KuCoin Ventures, Comma3 Ventures, Kronos Ventures, and Kernel Ventures	Prover Layers	Building a zero-knowledge Rollup-as-a-Service (zk-RaaS) platform that allows blockchains to enable zk-proof-based scaling for web3 applications.

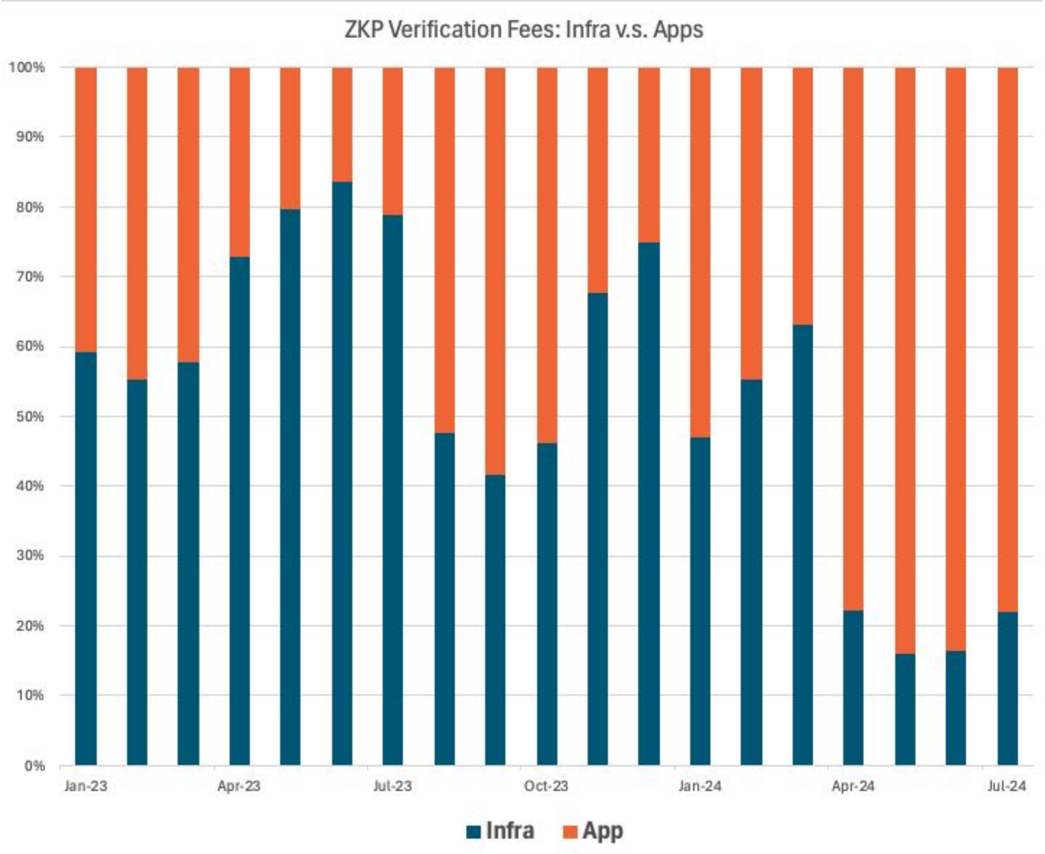
There are two possible interpretations for the increased demand for transactions on ZK L1/L2 chains. The first is that the demand for ZKApps has grown, leading to more transactions being submitted to the base ZK chain. The second is that the volume of transfers on ZK chains has significantly increased due to the mainnet launches of ZK L1/L2s over the past two years, resulting in a rise in number of transactions. Regardless of which interpretation is true, the outlook for ZKApps remains positive. In the former case, it signals that more people want to use ZKApps. In the latter case, it indicates that as more people use the base ZK chain and the ecosystem and infrastructure matures, an environment conducive to developing ZKApps is being established.

4.2. On-chain Data Analysis

Now, let's directly confirm the increased demand for ZKApps through an on-chain data analysis. One can observe that accumulated fees used in the ZKP verification process over the past 1.5 years, have exceeded $198 million, indicating a significant increase in demand for ZKPs compared to previous years. More importantly, most of the increase came from the growing demand for ZKApps. After breaking down the usage for ZKP verification fees into infrastructure and ZKApps, we found that the ZKApps' share, which was 40% in the past, has risen to 70-80% in 2024. This data serves as evidence that the recent surge in demand for ZKPs has primarily come from ZKApps.

Figure 3: ZKPs Verification Fees Dynamics

Source: dune.xyz@nebra, Ocular VC



5. Technical Advancements Making ZKApps Practical

So far, we have explored what ZKApps are, identified key use cases to pay attention to, and discussed why the main trend in the ZK industry appears to be shifting from infrastructures to applications. The viability of these ZKApps, of course, hinges on technological advancements that make them practical and feasible. Previously, we noted that the ZK infrastructure has matured sufficiently, and ZKApps that appropriately leverage this technology will become mainstream in the Blockchain/Web3 industry in the coming years. So, what specific advancements have made this possible, and what's more to come?

5.1. ZK Proving Systems

First thing to discuss about is the progress in ZK proving systems. Given the complexity involved, to those without technical background, it is often opaque which process employ what types of cryptographic technologies and how their improvements have enhanced the ZK proving system. Thus, in this section, we highlight notable advancements in ZK proving systems along with easy-to-understand metaphors. In short, these advancements have brought two major benefits: "**An increase in supported functionalities**" and "**Optimization of the computation process**".

For readers who want to check the full details about the life cycle of ZK proving system and advancements in each particular process, please refer to* ***Appendix*.

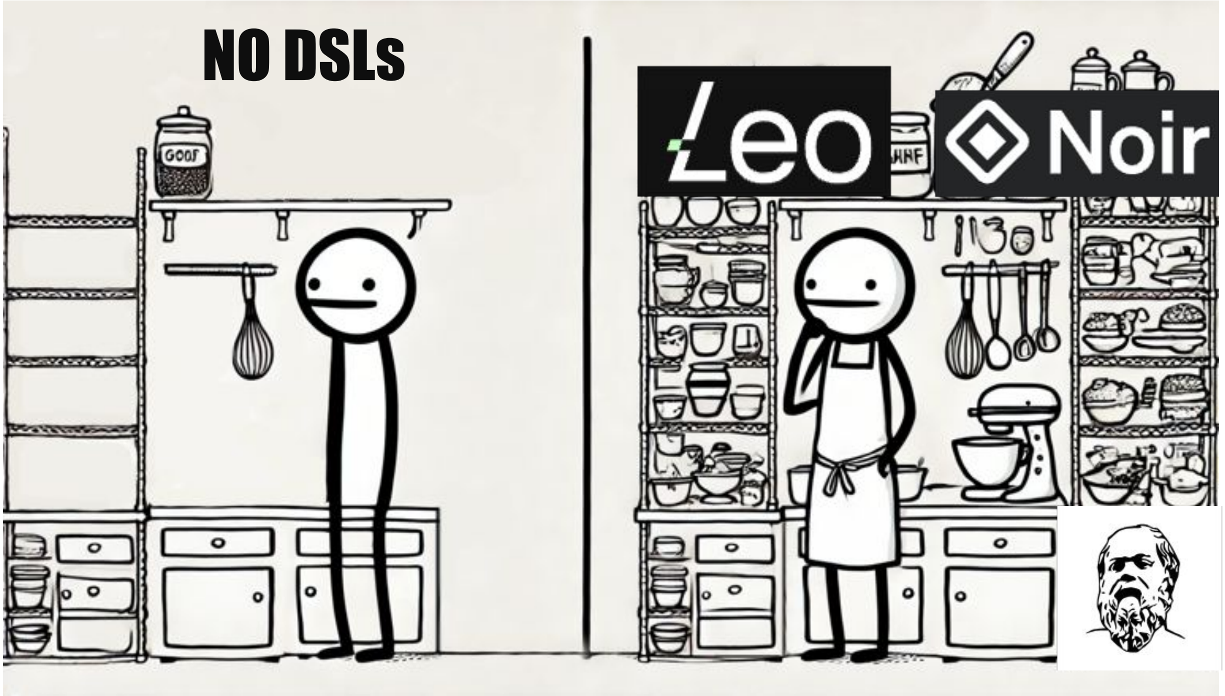
Supporting more functionalities: Domain-Specific Languages (DSLs)

Domain-specific languages (DSLs) in ZK proving systems are specialized programming languages designed to handle specific tasks within the ZK ecosystem. These languages enriches the creation of ZKPs by providing tailored syntax and functionalities that are optimized for ZK operations. DSLs like Leo, Zinc, Cairo, Noir, and ZoKrates are currently being researched and developed to **support more functionalities**, such as mutable variables, if-statements, and arrays.

This is analogous to a situation where Bob needs to prove Alice that he made a cake with a legitimate recipe, without revealing it. First thing Bob needs to do is make his recipe. The recipe should include all the high-level steps and ingredients needed to make the cake (e.g., make a batter with ingredients, then bake it). It will be great if Bob can use more trendy ingredients and cooking skills in his recipe (Figure 4)!

Figure 4: DSLs support more functionality for ZKPs

Source: DALL E, Presto Research



Optimizing the computation process: Arithmetization, Proof System (IOP+FCS)

After writing a program with DSL, it undergoes process such as Arithmetization and Proof System (consists of Interactive Oracle Proof (IOP), and Functional Commitment Scheme (FCS)) to be converted into ZKPs. The common challenge in these processes is to **minimize the computational overhead**, in order to make the ZKP generation and verification process accessible to more people.

Among the efforts to reduce computational overhead, the most intuitively understandable is the **reduction of field size in the Proof Systems**. Here, the field size refers to the size of the mathematical field used in the ZKP generation process. In easy words, it represents the total number of possible values that can be used to create secret codes; larger field sizes make it harder for someone to guess the code but take longer to generate. Famous cryptographic proof systems like Groth16, Plonk, and Halo2, which even those unfamiliar with ZKPs might have heard of, use a field size of 256 bits. However, with advancements in technology, recent proof systems like Goldilocks and Plonky3 use field sizes of 31 to 64 bits without sacrificing security. The state-of-the-art proof system, Binius, has significantly increased computational speed by using only 1 bit (zeros and ones) as its field size.

5.2. Decentralized Proving Infrastructures

The second technological advancement to discuss is the development of decentralized proving infrastructures. While the advancements in ZK proving systems optimized and simplified the proof generation and verification process by reducing the amount of computation required, decentralized proving infrastructures **allowed individuals to outsource intense computational power for generating ZKPs**.

Currently, there are two primary methods for implementing decentralized proving infrastructure in the ZK industry. The first method involves a ZK-based chain building its own **in-house prover layer**, and the second one is to operate an **outsourced prover layer** that can handle ZKP generation requests from various chains and applications.

In-house Prover Layer

For In-house prover layer method, the ZKP generation entities (i.e., the provers) are subordinate to specific chains. The biggest bottleneck of an in-house prover layer is the bootstrapping process: Since it is economically infeasible for chain developers to equip themselves with ZK proving devices to provide a seamless prover layer for all network users (this approach also negatively impacts the network's safety and liveness), typically they deploy protocols that attract individuals or groups with computational power to participate in the prover layer by offering rewards in the form of native tokens.

A representative example of a project operating an in-house prover layer is Aleo, a ZK Layer 1 blockchain. Similar to PoW in Bitcoin, Aleo requires provers to generate ZKPs that meet a certain threshold (i.e., "Proof Target") for each block. If the sum of the accumulated proofs exceeds the "Coinbase Target", the coinbase reward (Aleo token) is shared among the provers pro-rata based on their contributions. This proof-of-mining protocol can incentivize the development of faster software and hardware for ZKPs & decentralizing the prover ecosystem due to widespread distribution of prover rewards.

Outsourced Prover Layer

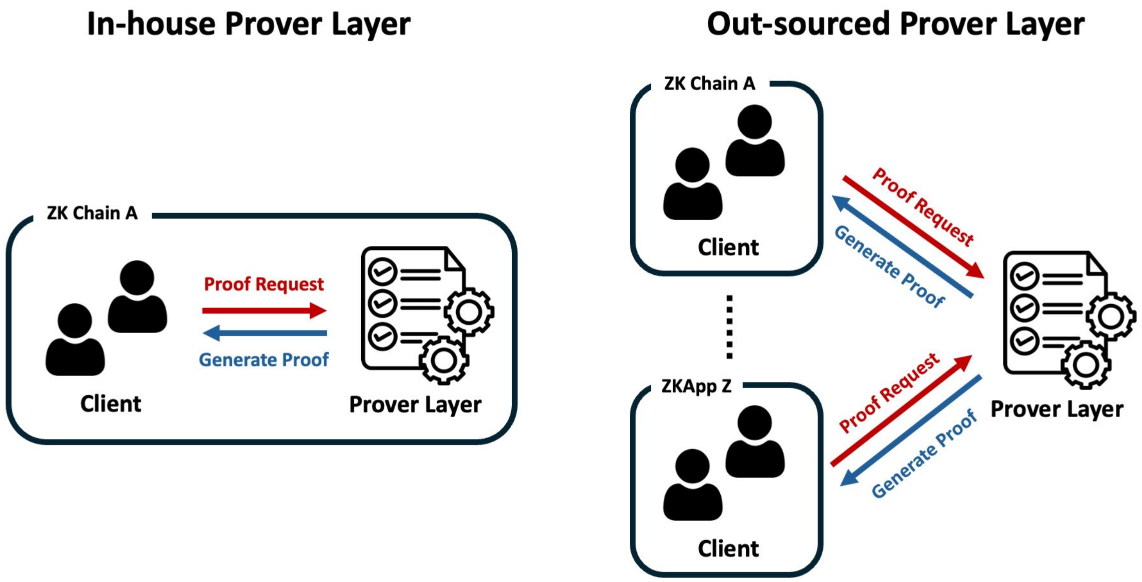
On the other hand, outsourced prover layers are located outside of the blockchain; and provides computational power upon request from various ZK-based chains and ZKApps. You can think of modular blockchains like Celestia, but with ZKP generation function. These outsourced prover layers are usually operated in a form of "prover market": where clients submit their transactions requiring ZKP generation, while provers bid to offer their proving services, including their capacity and cost to generate ZKPs.

Representative examples of projects currently operating outsourced prover layers include =nil, and Gevulot. =nil maintains an order book for each circuit with buy orders from users and sell orders from provers. The price discovery for generating a proof is managed through this orderbook mechanism. Gevulot operates in a PoS manner: it requires provers to deposit a stake and complete proof of workload tasks to join. Apart from the bidding system, the proof generation jobs are randomly allocated using a verifiable random function (VRF) to ensure fairness.

Nevertheless, outsourced prover layer method also have major concern, which is the difficulty of preserving end-to-end-privacy since the transaction data included in the proof request is submitted to provers while unsealed. To address this issue, projects like Marlin and zkPass leverage enclaves (a secure, isolated execution environment that protect data integrity) to ensure there is no privacy leakage in the process of ZKP generation.

Figure 5: Overview of Decentralized Proving Infrastructures

Source: Presto Research



Presto Research

Conclusion

So far, we have examined the overall adoption landscape of the ZK industry, the benefits that ZKApps can bring us, the evidence for why the main trend in the ZK industry is shifting from infrastructure to ZKApps, and the technological advancements that will support the rise of ZKApps. The development of cryptographic proof systems and decentralized proving infrastructure has paved the way for ZKApps to be used more swiftly and affordably, bringing zero-knowledge technology closer to everyday life.

The Blockchain/Web3 industry often faces criticism for developing overhyped technologies aimed more at attracting investors with little consideration given to actual market demand. To overcome this criticism, developers must advance technology in ways that genuinely improve our lives; however, it is equally important for us, the users, to continually assess which fields this technology can be effectively applied to. We hope this article provides readers with a broad understanding of ZKP and ZKApps, and intrigue more DYORs towards this industry.

In the upcoming Presto Research & Ocular VC collaboration series, we will go over a list of cutting-edge ZK-related projects (i.e., privacy roll-ups, client-side proving, privacy-preserving prover layers) both on the infrastructure and application sides, that are set to launch based on technological advancements we have mentioned in this article. Stay tuned!

About Presto

Presto is a Singapore-based algorithmic trading and financial services firm founded in 2014. Presto focuses on delivering exceptional value for clients through rigorous research-driven approach to investment and trade execution. With more than a 100 million trade executions in a day, Presto is a leading financial services firm in both digital assets and traditional finance markets.

Find out more at https://www.prestolabs.io.
Follow Presto for more content: X, LinkedIn

About Ocular

Ocular is a Singapore-based investment fund focused on the rising asset class of crypto and web3. With tech venture capital and data science background, our team is deeply rooted in the crypto community. Ocular Fund is managed by Openspace, a leading Southeast Asia venture capital firm with over US$850m in committed capital.

Find out more at https://www.ocular.vc.
Follow Ocular for more content: X, LinkedIn

Authors

Jaehyun Ha, Research Analyst : X, LinkedIn
Yi-wei Lin, Analyst : X, LinkedIn

Required Disclosures

Any expression of opinion (which may be subject to change without notice) is personal to the author and the author makes no guarantee of any sort regarding accuracy or completeness of any information or analysis supplied. The views and opinions expressed herein are those of the author(s) and do not necessarily reflect the views of Presto Labs or its affiliates. This material by itself, is not and should not be construed as an offer or a solicitation to deal in any investment product or to enter into any legal relations. This material is for informational purposes only and is only intended for sophisticated investors, and is not intended to provide accounting, legal, or tax advice, or investment recommendations, or an official statement of Presto Labs or its affiliates. Presto Labs, its affiliates and its employees make no representation and assume no liability to the accuracy or completeness of the information provided. Presto Labs, its affiliates and its employees also do not warrant that such information and publications are accurate, up to date or applicable to the circumstances of any particular case. Certain statements in this document provide predictions and there is no guarantee that such predictions are currently accurate or will ultimately be realized. Prior results that are presented here are not guaranteed and prior results do not guarantee future performance. Recipients should consult their advisors before making any investment decision. Presto Labs or its affiliates may have financial interests in, or relationships with, some of the assets, entities and/or publications discussed or otherwise referenced in the materials. Certain links that may be provided in the materials are provided for convenience and do not imply Presto Labs' endorsement, or approval of any third-party websites or their content. Any use, review, retransmission, distribution, or reproduction of these materials, in whole or in part, is strictly prohibited in any form without the express written approval of Presto Labs. Presto Research and related logos are trademarks of Presto Labs, or its affiliates.

Appendix: Lifecycle of The ZK Proving System

Step 1: Writing a program

Purpose: Define the problem or computation to be proved in zero-knowledge.

Explanation: The first step in the life cycle of the ZK proving system is, of course, writing a program. This step involves writing the actual program or algorithm that you want to prove knowledge of. The program encapsulates the logic and operations required to solve a particular problem or verify a particular statement. Here, the problem can be very simple, like X+1 = 2, or very complex, like verifying that a large dataset satisfies certain properties (e.g., all entries are correctly encrypted and meet specific criteria).

Technical Advancements: Previously, the primary focus of research in the ZK industry was on generating fast, efficient, and secure proofs from ZK circuits (which will be explained in Step 4 and Step 5). However, with significant advancements in cryptographic proof systems, there is now active research into developing Domain-Specific Languages (DSLs) that support converting wider high-level concepts into ZK circuits. Efforts are being made to support more terminologies used in traditional computer science, such as mutable variables, primitive types, if-statements, and arrays, into ZK circuits. DSLs like Leo, Zinc, Cairo, Noir, and ZoKrates are currently being researched and developed to support these functionalities and more.

Metaphor: Let’s explain this entire process with a metaphor: where Bob needs to prove to Alice that he made a cake with a legitimate recipe. First thing he needs to do is make a recipe. The recipe should include all the high-level steps and ingredients needed to make the cake (e.g., make a batter with ingredients, then bake it). It will be great if Bob can use more trendy ingredients and cooking skills in his recipe!

Step 2: Arithmetization

Purpose: Convert the program into arithmetic circuits that can be analyzed mathematically.

Explanation: Arithmetization is the process of transforming the high-level program into an arithmetic circuit. An arithmetic circuit is a mathematical representation of the program using basic arithmetic operations (i.e., addition and multiplication). This conversion allows the program to be expressed in a form that can be further manipulated and verified.

Technical Advancements: Optimizing the arithmetization process is crucial for reducing computational overhead, and making ZKPs practical for real-world applications. R1CS (Rank-1 Constraint Systems), and AIR (Algebraic Intermediate Representation) are the representative arithmetization techniques used in ZK proving systems today. R1CS, mostly used in SNARKs, uses quadratic constraints and is well-suited for circuit computations, requiring gadgets for complex operations. AIR, frequently used in STARKs, represents computations with an execution trace matrix and allows polynomial constraints of varying degrees, making it suitable for machine computations. Furthermore, research on improved arithmetization techniques, such as Succinct R1CS, log-space circuits, and CCS (Customizable Constraint Systems) aimed at reducing constraint size and the number of operations, has continued until recently.

Metaphor: If writing a program can be compared to writing a new recipe, arithmetization can be thinked as converting the recipe into a series of steps involving basic operations like mixing, baking, battering, and measuring ingredients. Instead of just listing the steps, Bob can break down each action into fundamental operations (e.g., mix 180g of egg and 90g of sugar, bake the batter in the oven for 30 mins at 180°C (356°F)). It is important for Bob to optimize this break-down process, in order to utilize the whole kitchen and prevent from performing redundant actions.

Step 3: Constraint Satisfaction Problem (CSP)

Purpose: Represent the arithmetic circuit as a set of polynomial equations.

Explanation: The arithmetic circuit is then transformed into a Constraint Satisfaction Problem (CSP). This involves expressing the circuit as a set of polynomial equations that must be satisfied. Each gate and wire in the circuit corresponds to a constraint, and solving these constraints verifies the computation.

Metaphor: Bob converts the detailed steps of his cake recipe into a checklist. Each item on the checklist is a condition that must be met for the recipe to be successfully completed—such as, “Is the oven preheated to 180°C (356°F)?”. Now proving the claim “Bob knows legitimate recipe” is converted to a question “Did Bob checked all the lists in the checklist?”.

Step 4: Compatible Interactive Oracle Proof (IOP)

Purpose: Create an interactive protocol where the prover convinces the verifier of the validity of the statement (i.e., knowing the correct polynomial) without revealing the entire polynomial.

Explanation: An IOP involves multiple rounds of interaction between a prover and a verifier. During these interactions, the verifier can query specific values of the proof without seeing the entire proof. The prover sends the proof to an oracle, and the verifier can query the oracle to verify specific parts of the proof by checking if certain values are correct.

Technical Advancements: Marlin, Plonk, and Sonic are the most widely known examples of IOPs. A recently devised state-of-the-art IOP system is HyperPlonk. HyperPlonk improves upon Plonk by adapting it to the boolean hypercube and utilizing multilinear polynomial commitments, which brings several key advantages. Unlike Plonk, which requires a large FFT for proof generation, HyperPlonk eliminates this need, thereby simplifying and accelerating the process. Additionally, HyperPlonk supports custom gates of much higher degree without increasing the prover’s running time, enhancing its capability to handle complex computations efficiently. This adaptation not only retains Plonk’s flexibility but also significantly speeds up the prover’s running time.

Metaphor: Bob tries to convince Alice that he has baked a cake according to his specific recipe, without showing the entire cake. Alice cannot see the entire cake, but she can ask Bob to cut a slice and show a specific layer. Bob cuts a slice at Alice's chosen spot and shows it to Alice. Then Alice can taste or inspect that slice to determine whether the layer is correct according to the recipe, without needing to see the entire cake. This is akin to the oracle access in IOP, where the verifier queries specific parts of the proof.

Step 5: Crypto Compiler (Functional Commitment Scheme)

Purpose: Convert the interactive proof, which operates under idealized assumptions, into a practical non-interactive proof that can be easily verified and ensure the commitment of the inputs.

Explanation: The final step involves using a Crypto Compiler to transform the interactive protocol into a practical non-interactive proof by removing the idealized assumptions of the original proof system. This typically involves generating a commitment scheme, where the prover commits to certain values and proves their knowledge without further interaction. The commitment scheme ensures that the prover cannot change their inputs after committing to them.

Technical Advancements: The commitment scheme is the most actively researched field in ZK proving systems - aiming to optimize the proof generation process (e.g., reduce field sizes, optimize CPU utilization, reduce proving & verifying time). Schemes like Bulletproofs, KZG, and FRI are names that anyone with even a slight interest in ZK would have heard of. Among the newly developed commitment schemes, Binius is the most noteworthy project. Binius is a protocol designed to generate efficient cryptographic proofs by operating over binary fields instead of larger field sizes (31~256 bits) used in traditional SNARKs and STARKs. This method can reduce computational resource requirements since it allows faster arithmetic operation directly on bits (zeroes and ones). Additionally, new commitment schemes such as Basefold and Zeromorph have been proposed to reduce computation overhead.

Metaphor: Bob seals his cake recipe and all the steps he followed in an envelope. Then Bob presents the sealed envelope to Alice along with a certificate sticker from a trusted baking judge who verifies that the recipe inside was followed correctly. Alice doesn't need to open the envelope; she just checks the certificate and trusts it.