BINANCE RESEARCH

The zkEVM world:
An Overview of zkSync

Moulik Nagesh
Shivam Sharma

Table of Contents

1 Key Takeaways

- Matter Labs, the team behind zkSync Lite (a first-generation Ethereum zk-rollup), launched the first public zkEVM solution, zkSync Era. The launch represents an important milestone for the adoption of zkEVM technology.
- zkSync Era has notable differences from its optimistic rollup counterparts (i.e., Arbitrum and Optimism). These differences relate to security, capital efficiency, and transaction costs.
- zkPorter is an interesting, upcoming innovation by Matter Labs and is an off-chain data availability solution that complements the zkSync Era rollup. zkPorter offers a significant upgrade in transaction speed and cost to current solutions.
- zkSync Era has attracted a significant amount of TVL and unique deposit addresses since their March mainnet, especially when compared to competitors.
- Some of this activity is likely in relation to a long-rumored airdrop for zkSync.
- StarkNet, Polygon zkEVM, Scroll, Taiko, and Linea are also working on (or have released) competing zkEVM solutions.

2 Introduction

The layer-2 ("L2") discussion has largely centered around two primary types of solutions: optimistic rollups and zero-knowledge rollups ("zk-rollups"). While optimistic rollups, like Optimism and Arbitrum, have dominated the Ethereum L2 landscape over the last year, **2023 has seen significant growth in their zero-knowledge counterparts**. Previously, one of the main drawbacks of zk-rollup solutions was their lack of support for the Ethereum Virtual Machine ("EVM") and hence the inability to execute related smart contracts. The development of zero-knowledge Ethereum Virtual Machines ("zkEVM") has changed this and been a particular catalyst for zk-rollup adoption, spurring them to new heights.

Matter Labs, the team behind zkSync Lite (a first-generation zk-based Ethereum L2), has been a notable presence in the space and **the mainnet launch of their zkEVM, zkSync Era, has been an important milestone**. This milestone has also been accompanied by increased activity on zkSync, signaling the importance of the zkSync product suite and zkEVM solutions in the current L2 landscape.

In this report, we have a look at Matter Labs' zk product suite, recent updates, and roadmap, the discussion around a potential airdrop, as well as a market comparison versus their competitors.

3 Key Products

zkSync Lite

zkSync Lite (previously known as zkSync 1.0) is a standard L2 zk-rollup solution that offers an early version of the zkSync network without extensive smart contract support. Particularly, zkSync Lite does not natively support the Ethereum Virtual Machine ("EVM"). **In its simplest form, zkSync Lite is a trustless protocol for scalable, low-cost payments on Ethereum.** Given the challenges of engineering an EVM-compatible zk-rollup solution, zkSync initially prioritized a phased launch, with zkSync Lite being the first stage to be released in June 2020.

At the time of launch, the product's main purpose was to act as a special prototype, focused on delivering early payment solutions utilizing zk-rollup architecture. A key advantage of zkSync Lite is attributed to its simplicity in performing swaps and transfers whilst enabling users to benefit from low transaction fees and high transaction efficiency. **Even though zkSync Lite lacked smart contract coverage, the initial zkSync product accumulated more than US$80M in total value locked[(1)] ("TVL") and is one of the largest L2 solutions operating in the Ethereum ecosystem**. However, it is worthwhile to note that a proportion of this TVL may not necessarily reflect activity on the network but rather users wanting to lock funds on the rollup due to the incentives of a future token airdrop. When accounting for daily transactions, zkSync Lite falls short of other L2 solutions, indicating that zkSync's first-stage product is potentially forgoing activity due to the lack of support for smart contracts.

zkSync Lite's incompatibility with EVM means that the product possesses a limited range of applications and utility outside of token swaps and transfers. Put in context, this is quite a significant limitation considering smart contracts are at the core of decentralized app ("dApp") development for any Ethereum-based technology. EVM as a computation engine was not inherently designed to support zk-circuits, with such a limitation allowing zkEVM to enter the picture. The next stage of the zkSync's product lifecycle aims to close this gap with zkSync Era superseding zkSync Lite.

zkSync Era

zkSync Era (previously known as zkSync 2.0) is Matter Labs' version of a zkEVM rollup. What exactly is a zkEVM? A zkEVM is a virtual machine that executes smart contracts in a way that is compatible with zk-proofs. **zkSync Era uses the zkEVM and is a special type of zk-rollup that enables every smart contract to be easily deployed and executed on the Ethereum Virtual Machine ("EVM"), with very limited code changes.**

Practically, what this means is that zkEVMs aspire to create a zk-rollup experience that feels as close to using the Ethereum base layer as possible. For developers, the **key benefit is that they can port EVM-compatible dApps over to zkSync Era and realize much lower gas fees and higher transaction throughput**, while also inheriting Ethereum's security and decentralization.

To get a more technical background on zkEVMs, please make sure to check our report zkEVM and the Future of Ethereum Scaling.

Key differences between zkSync Era and optimistic rollups

- Security: **optimistic rollups assume all transactions are valid** and then use a game-theoretic approach, where users are incentivized to call out fraudulent or invalid transactions via **fraud proofs**. **zkSync Era, like other zk-rollups, uses a different approach, whereby it produces validity proofs**, which confirm that there were no fraudulent transactions that they settled. In essence, this means that **zkSync Era relies purely on mathematics, whereas optimistic rollups rely upon game theory and incentivized actors to ensure certainty of their transactions,** i.e., zk-rollups can be said to have higher security than their optimistic counterparts – in at least some ways.

- Settlement and capital efficiency: due to the game theory mentioned above, **optimistic rollups necessitate a 7-day settlement period**. This also means that users cannot withdraw assets from the optimistic rollup immediately, but have to wait at least a week. **Liquidity providers ("LPs") can step in to help** this issue, but this creates a security risk, and does not work for institutions or whales, as LPs would charge fees for this service, which would weigh on margins for whales. **zkSync Era does not have this issue and provides settlement in hours, with a target to reduce it to minutes.**

- Transaction Costs: **optimistic rollups have to post more data onto the Ethereum layer-1 ("L1") when compared to zk-rollups**, which only have to post validity proofs. This is among the key reasons **why optimistic rollups are generally more expensive to use** when compared to zk-rollups. zkSync Era specifically has announced a further extension called **zkPorter**, which will reduce fees even further (more on this later).

- Support for native account abstraction: one of the critical features required for mass adoption is a top-tier user interface. Native account abstraction is a major stepping stone to this goal. For example, **accounts on zkSync Era can pay transaction fees in any token rather than a specific token**. It also means that wallets can be customized to allow users to batch multiple transactions and just sign once, or to add two-factor authentication without seed phrases. It should be **noted that this feature is not only unavailable on competing optimistic rollups, but also unavailable for Polygon zkEVM.**

Figure 1: zk-rollups are generally cheaper than optimistic rollups (top 5 cheapest rollups below).

Logo	Name	Rollup type	Cost to send ETH (US$)	Cost to swap tokens (US$)
	Loopring	zk	0.06	0.48
	Polygon zkEVM	zk	0.07	0.28
zkSync	zkSync Lite	zk	0.09	0.22
	Arbitrum One	Optimistic	0.12	0.33
	Boba Network	Optimistic	0.20	0.36

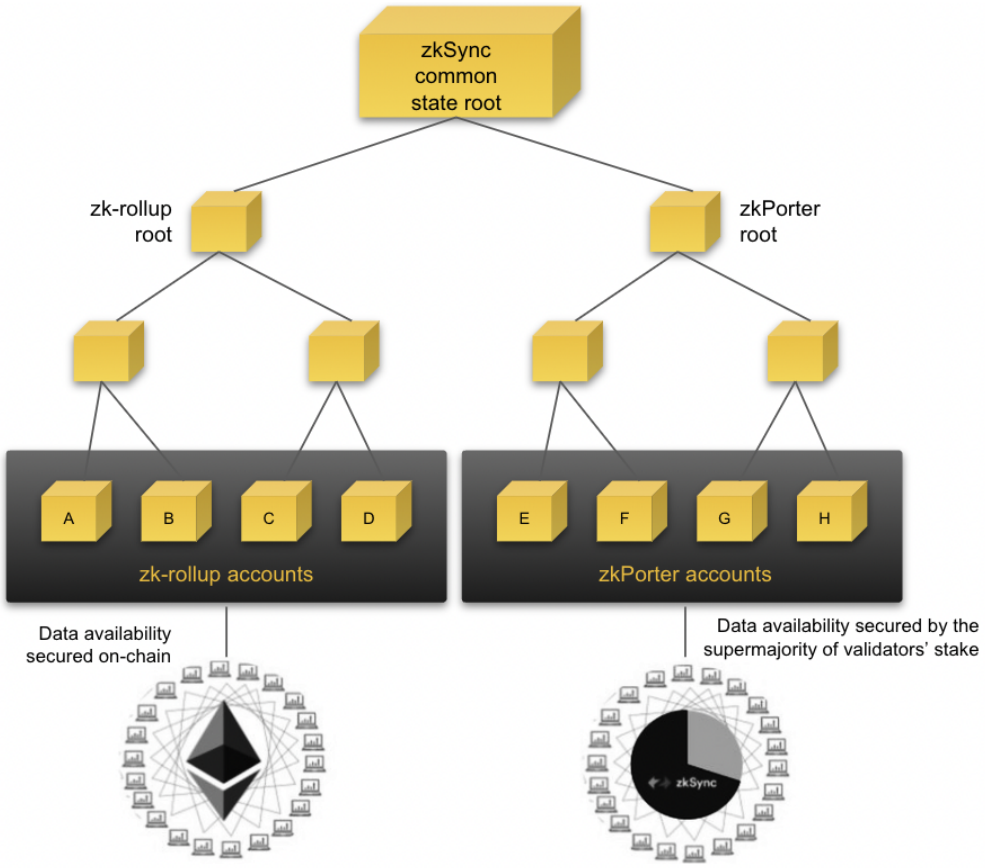
Source: l2fees.info, as of May 30, 2023

zkPorter

zkPorter is a system designed by Matter Labs to take zk-rollup scalability to the next level. **zkPorter is an off-chain data availability solution that will complement the zkSync Era rollup.** Both solutions will be **composable and interoperable,** i.e., accounts and smart contracts from both sides will be able to interact with each other.

To make the solution easier to explain, check out this diagram from Matter Labs:

Figure 2: A visual representation of how zkSync Era will work zkPorter.



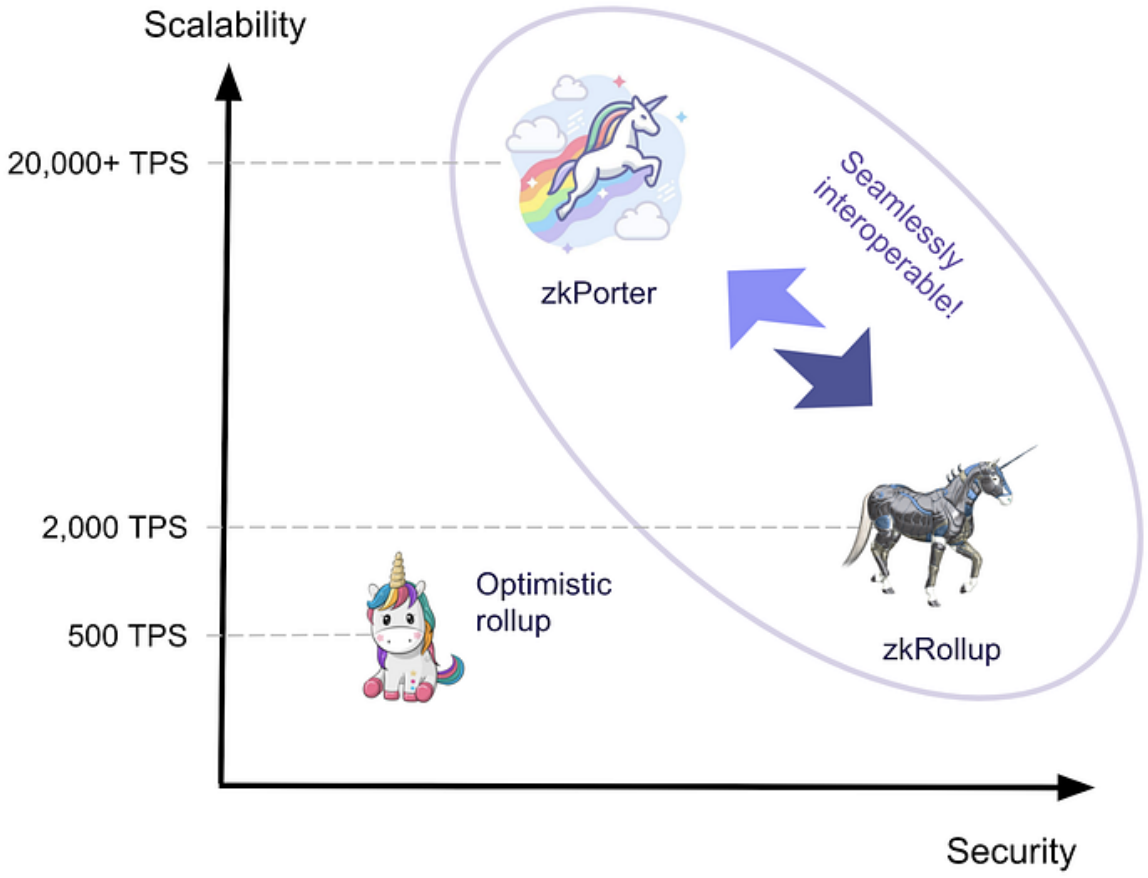
Source: blog.matter-labs.io, Binance Research

Essentially, **zkPorter allows data availability to be stored off-chain rather than on the Ethereum L1**. The data is secured by "**Guardians**"[(2)], who will sign blocks to confirm data availability and be **governed via Proof-of-Stake** ("PoS"), i.e., the Guardians will stake their zkSync tokens (which is not yet announced) and any failure or misbehavior will lead to slashing. Matter Labs clarify that this PoS system is more secure than that observed in other sidechains, because **zkSync Guardians are essentially powerless, and cannot steal funds**.

Benefits and drawbacks of the zkPorter solution

+ Exponential scalability: according to Matter Labs, zk-rollups, including **zkSync Era can handle up to 2,000 transactions per second ("TPS") at peak capacity. This compares to 20,000+ TPS for zkPorter.** The reason for this is that the majority of rollup fees are due to the costs of publishing data on the Ethereum L1. zkPorter, on the other hand, can perform thousands of transactions on any contract that is deployed on it, and only has to post a single update to Ethereum.

Figure 3: zkPorter can theoretically offer a significant scalability boost compared to other solutions.



Source: blog.matter-labs.io

+ User choice: Users can **choose to transact on either the zk-rollup or via zkPorter based on their preferences for security and the trade-offs they are willing to make.** Any users who want the entire data availability on-chain can stay completely on the rollup side. Still, those that are fee-sensitive or conducting trivial transactions can choose to use zkPorter.

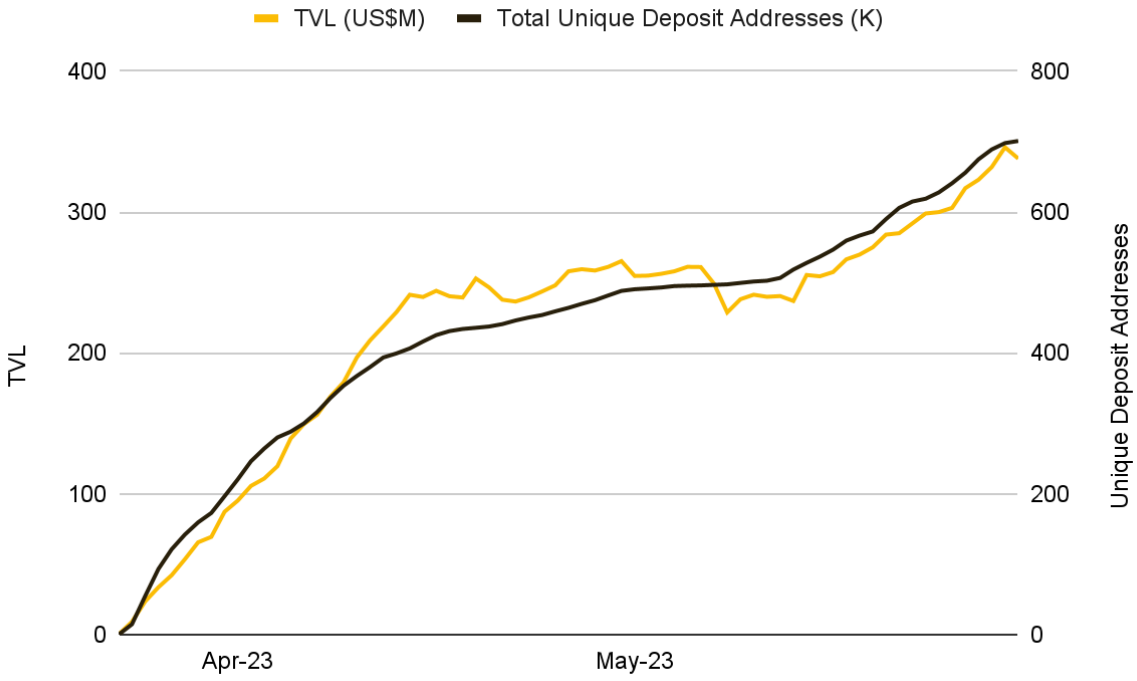
- Potential for centralization: when **utilizing zkPorter, the user will rely upon its internal consensus mechanism, which is PoS using the zkSync token** as described above. This is likely to be significantly less secure or decentralized when compared to using Ethereum for data availability (as you would be if you chose to use the zk-rollup side) – at least in the beginning.

4 Recent Developments & Roadmap

Recent Developments

The major recent development for Matter Labs was the launch of the zkSync Era Mainnet on March 24, 2023[3]. Since launch, zkSync Era has been quite successful in attracting TVL and users to its platform, as we can see below in Figure 4. In fact, their **performance is particularly impressive when compared to the competing Polygon zkEVM solution, which has around US$28M in TVL and ~24K unique depositors**[4].

Figure 4: Since launch, zkSync Era has attracted over US$350M in TVL and over 700K unique depositors.

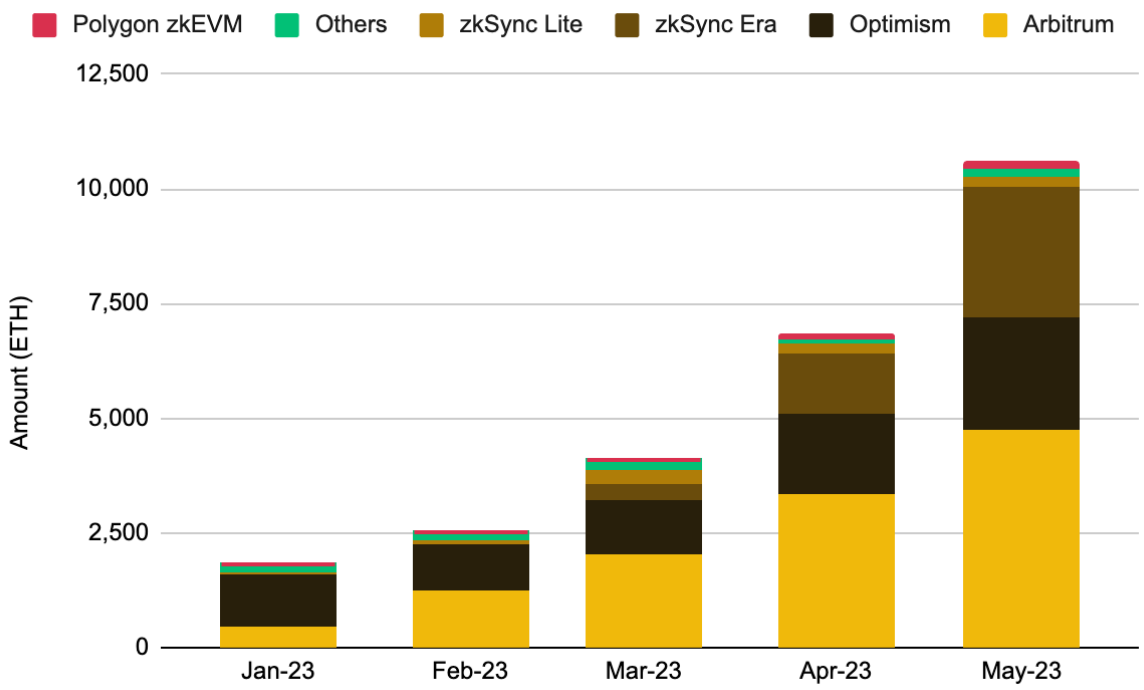


Source: Dune Analytics (@makaineko), Binance Research, as of May 30, 2023

This increase in user activity has also made itself evident in other metrics. Below, we look at **data publishing fees on Ethereum** – remember, L2s have to publish data or send proofs of computation up to the Ethereum L1 in order to finalize their transactions. Looking at Figure 5, we can see that while Optimism and Arbitrum have led the way throughout 2023, May has been an impressive month for zkSync Era. For the **first time ever, zkSync Era surpassed Optimism and was the second-largest fee-payer to Ethereum** for data publishing. Considering Optimism's top position so far this year, this is a positive sign for

zkSync Era and further indicates the level of interest that this protocol has generated with users.

Figure 5: With 2.85K ETH in data fees and a 118.8% increase MoM in May, zkSync Era surpassed Optimism to secure second place.



Source: The Block, Binance Research, as of May 31, 2023

We should also consider the fact that it is **likely that activity on zkSync Era may have been driven by rumors of a potential airdrop**, which have been circulating for many months (more on this below). As such, users may be more likely to engage with zkSync in different ways in order to potentially qualify for an airdrop, especially when compared to competitors like Polygon zkEVM, who already have the $MATIC token. Nevertheless, **the surge in data fees for zkSync undoubtedly represents a key milestone for the project and for the underlying adoption of zk-based technology in the L2 ecosystem**.

Expected Roadmap

While the team is yet to release an official update to their roadmap, we did have the chance to listen to Anthony Rose, Head of Engineering at Matter Labs, in a recent podcast appearance[5] discuss what is next for zkSync Era.

Generally speaking, Anthony was focused on the basic principles of how to make their product faster, cheaper, and more secure. However, the key question that their team is working on is "**how do we decentralize?**". Anthony further added that their plan is to start with **decentralizing the sequencer, followed by the prover** (also mentioned in their

ethos). The sequencer and prover[6] are two crucial components of the infrastructure that makes up zkSync Era and are currently run by Matter Labs[7].

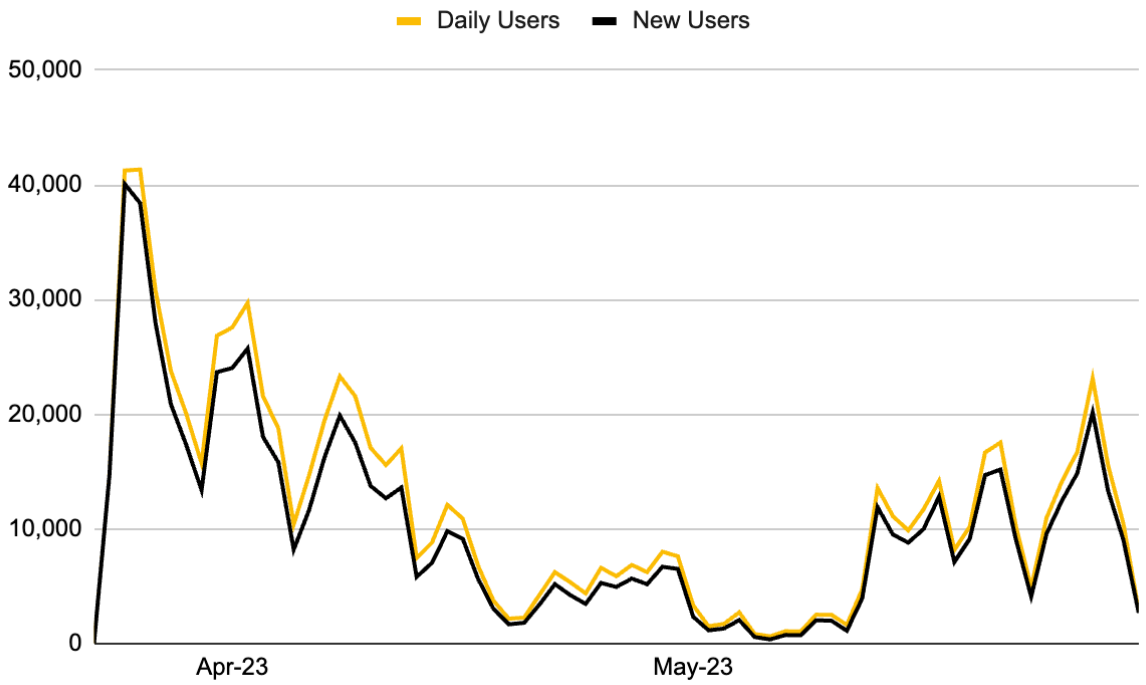
In addition to this, **zkPorter is yet to be launched and is something that should be expected in the near future**, having originally been set to launch alongside the zkSync Era mainnet.

Airdrop Discussion

One of the consistent topics of discussion when it comes to zkSync has been that of a potential airdrop. With most competitors, including Optimism, Arbitrum, dYdY, Loopring, and more, having launched tokens, it has long been rumored that a zkSync token is in the making. The topic becomes particularly relevant when thinking about the team's focus on decentralizing the protocol.

While nothing concrete has been announced at this point, and team members have generally deflected the question when asked on podcasts or on Twitter, there is one angle worth considering. The **zkPorter protocol is designed to run its own consensus mechanism via PoS – this necessitates validators or Guardians to have staked tokens that might be slashed** in case of misbehavior. While this does not confirm a token, it does indeed add some more weight to the rumors of a potential token airdrop.

Figure 6: Both daily and new users on zkSync Era have been ramping up through May.

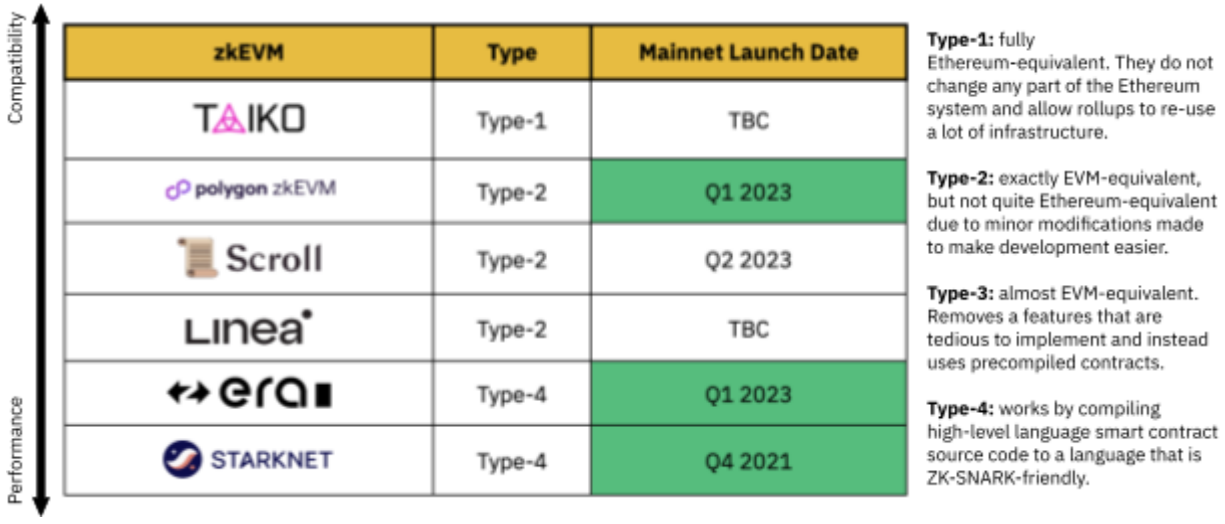


Source: Dune Analytics (@makaineko), Binance Research, as of May 30, 2023

5 Layer-2 Landscape & Comparison

With the emergence of zk-rollup solutions, it isn't surprising to see a number of competing projects that have their own perspectives and applications in this space. Considering the focus of zkSync's roadmap and product suite, we will be reviewing other leading projects in the market that also utilize zkEVM technology. Even though the underlying goals of zkEVM projects are similar to the extent of processing transactions and driving scalability on the Ethereum mainnet, it is possible to classify each project as a distinct category based on how they are prioritizing compatibility and performance.

Figure 7: Type categorizations of zkEVM projects with their compatibility and performance trade-offs.



Source: Vitalik Buterin, Project teams

The table in Figure 7 comprises prominent zkEVM projects from the current L2 market. "Type" is an important taxonomy based on Vitalik's zkEVM classifications and is used to distinguish between different zkEVM solutions. While possessing a certain type does not unambiguously render a project to be more or less successful, it does tell us at what point a project exists on the performance and compatibility trade-off space. For example, Taiko, a type-1 project, is more compatible with existing Ethereum infrastructure in comparison to Starknet, a type-4 project, which is less compatible but possesses faster prover times.

It is also worth noting that with the exception of zkSync Era, Polygon zkEVM, and StarkNet, all other zkEVM projects are yet to launch their mainnets. While the race to launch the first zkEVM solution may prove to be inconsequential, the release of the zkSync Era mainnet was considered a major technical milestone as it became the first public and

permissionless zkEVM for use amongst both users and developers. Given that we are in such a nascent stage of zkEVM adoption, we have seen rising activity on zkEVM development, with a number of projects progressing in their quest to try and capture market share. What's more, exploration of the different type classifications by the competing players is certainly helpful in fuelling innovation in a space where there may be little to separate zk-rollup-powered projects that possess similar underlying mission statements.

For a deep dive into zkEVMs and their type classifications, please make sure to check our report zkEVM and the Future of Ethereum Scaling.

Figure 8: Key metric comparisons of different zkEVMs that are live on mainnet today. For the purpose of the below table, we have considered the products zkSync Lite and zkSync Era separately.

zkEVM	TVL (US$M)	Daily TPS
era	350.5	7.93
zkSync lite	81.0	1.08
STARKNET	60.2	2.27
polygon zkEVM	28.0	0.26

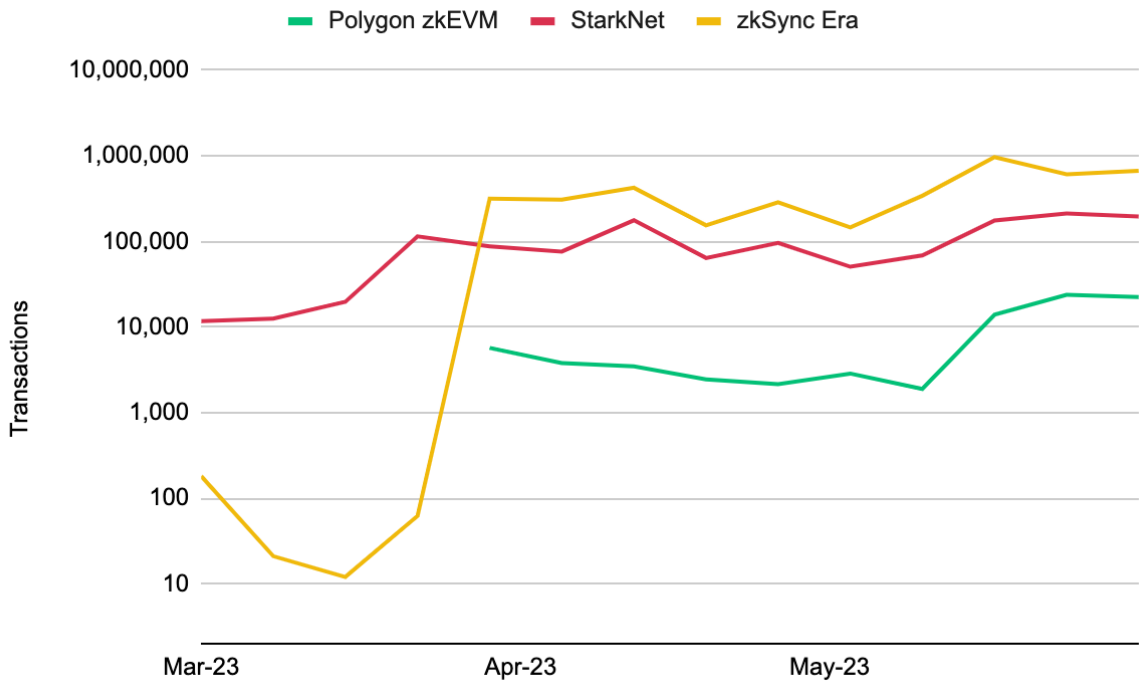
Source: L2Beat, Dune Analytics (@Marcov), Binance Research, as of May 31, 2023

It is clear that zkSync has a substantial lead over both StarkNet and Polygon zkEVM when analyzing TVL, with the latter falling behind by more than 20 times in magnitude. zkSync and StarkNet are showing sustained growth in comparison to polygon zkEVM, something which is likely being driven by the potential of a token airdrop in the future. Therefore, it would be important for the zkEVM projects to maintain organic growth even after the consummation of such token incentives.

Even though we have seen a rise in zkSync and StarkNet TVL over time, transactions and network activity haven't seen the same levels of sustained growth. As seen earlier in Figure 4, this is especially true for zkSync Era since its mainnet deployment back in March. This indicates that users are actively bridging funds into the ecosystem but tend not to continue transacting on the rollup, and instead leave their funds to sit idle. This isn't surprising, given that incentives from qualifying for a potential airdrop tend to only exist in the short term. L2s without a token will generally find it harder to sustain long-term network activity due to a lack of transaction-related incentives. This may further be driven by the fact that zkEVMs are still in a nascent phase of their lifecycle. For example, rollups are currently working with

smaller-scale liquidity, and there are a lower number of tried and tested DApps available with sufficient utility.

Figure 9: Daily transactions of mainnet zkEVM projects over time. The below visualization is based on a logarithmic scale.



Source: Artemis, Binance Research, as of May 31, 2023

StarkNet

StarkWare's **StarkNet is a general-purpose zk-rollup chain that utilizes its own language in Cairo** instead of engaging with EVM compatibility. Warp is a Solidity to Cairo transpiler, which is currently in progress, that would make for easier onboarding into the StarkNet ecosystem. However, Cairo is considered to have tooling, open-source libraries, and security practices that lag behind Solidity, putting StarkNet at a disadvantage in comparison to other players, such as zkSync's zkEVM. This may act as a barrier to entry for developers, given that they may be required to learn a new language.

Generally, it is common for L2 solutions to have fees paid in $ETH. Contrary to this, **StarkNet has instead opted to use their native STARK token for gas fees**. While this may be disadvantageous to Ethereum, it is beneficial to StarkNet as such an approach moves value from L1 to L2.

A key difference between StarkNet and zkSync is technical in nature. zkSync is designed on a zk-SNARK-based system, which is a cryptographic technique that verifies data without having to reveal the data. In comparison, StarkNet utilizes zk-STARKs, which is a slightly

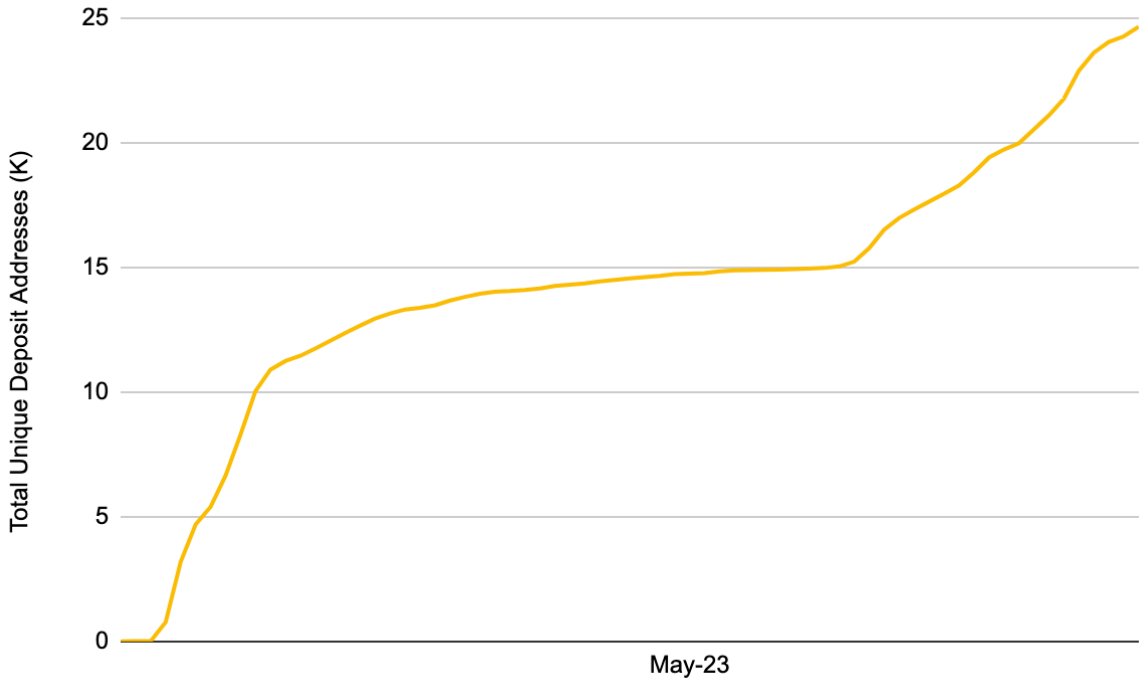
different variant of zk-proofs whereby the computation can be batched and occur off-chain prior to confirming the validity on-chain. This results in StarkNet benefiting from increased scalability when considering computational speed, although StarkNet's underlying characteristics do limit its generalizability.

For more detailed comparisons on zk-SNARKs and zk-STARKs, please make sure to check our report zkEVM and the Future of Ethereum Scaling.

Polygon zkEVM

Polygon zkEVM is a zk-rollup solution that originated from Polygon's prior work in exploring Ethereum scaling solutions and their acquisitions of zk-related projects in Hermez and Mir. Polygon's rationale for pursuing zk-based blockchain solutions is derived from shortcomings in the design of their Proof-of-Stake ("PoS") sidechain, particularly in Polygon PoS being able to fully leverage Ethereum's security. Polygon zkEVM was launched on March 28, 2023, a few days after zkSync Era launched their mainnet. While both projects have seen an influx of users, zkSync Era has had a much larger level of adoption, with zkSync boasting a significantly higher TVL.

Figure 10: Polygon zkEVM has seen unique addresses grow, albeit at a much slower rate than zkSync Era.



Source: Dune Analytics (@Marcov), Binance Research, as of May 31, 2023

Aside from the fact that both Polygon zkEVM and zkSync Era are open-sourced zkEVM chains, they also have a few comparable similarities. For example, **both chains support account abstraction processes and have also prioritized data availability solutions** as

part of their product roadmap. While zkSync Era will integrate with zkPorter, Polygon is very closely linked to Avail as their own data availability solution (formerly Polygon Avail).

However, Polygon zkEVM and zkSync Era do have inherent differences, with the main distinction being that **Polygon zkEVM is EVM-equivalent, whereas zkSync Era is EMV-compatible.** EVM-equivalent rollups are generally considered to possess less friction than EVM-compatible rollups[8]. Being EVM compatible, zkSync Era leverages an LLVM-based compiler that works with popular EVM languages such as Solidity, Vyper, and Yul. On the other hand, Polygon zkEVM enables the migration of Solidity natively and does not require any re-writing of code or additional tooling.

Polygon zkEVM is further different in that it combines the best of zkSTARKS and zkSNARKS to benefit from improved latency, scalability, and lower costs. Polygon zkEVM has also integrated a range of solutions in their product suite, namely:

- Polygon Miden (a STARK-based rollup)
- Polygon Nightfall (a privacy-focused rollup)
- Polygon Zero (a zk-rollup with recursive proof generation)
- Polygon ID (a web3 identity solution that utilizes zk technology).

With a growing product suite, it is important to mention that Polygon zkEVM does have the potential to tap into its wider ecosystem of resources from the Polygon PoS side. Polygon PoS has more daily active addresses than any other L2, something that Polygon zkEVM may benefit from if network effects were to be realized.

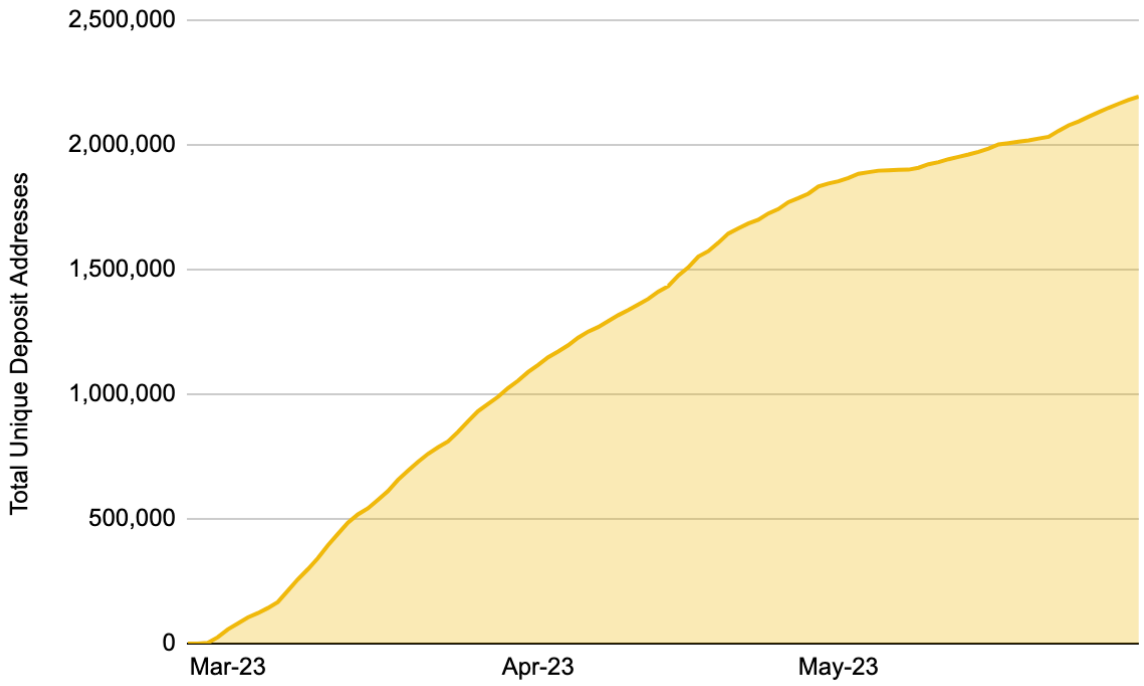
Scroll

Scroll is another zkEVM solution that recently launched their Alpha testnet on February 27, 2023[9]. In their Pre-Alpha testnet, Scroll had impressively amassed over 15.4M transactions, a trend that seems to be continuing on Scroll's Alpha testnet, with the total number of unique depositors increasing over time, as depicted in Figure 11 below.

Separate from the zkSync solution, Scroll is built with a design that prioritizes the use of Solidity without the need for any additional compilers in between. Based on their current status and development trajectory, Scroll may be classified as a type-2 zkEVM solution. This renders Scroll to be relatively similar to the Polygon zkEVM in that both projects are bytecode-level solutions.

As a result of Scroll's use of ZCash's Halo2 code[10], one major differentiating factor for Scroll is that it allows protocols to leverage zkSNARKs' reduced proof sizes and faster proof verification without the need for a trusted setup.

Figure 11: Scroll zkEVM is seeing a steady increase in network users, with over 2M unique deposit addresses on their Alpha testnet.



Source: Dune Analytics (@hashed_official), Binance Research, as of May 31, 2023

Fundamentally, and in the long-term, **Scroll is aiming to be the first zkEVM solution that is fully Ethereum equivalent** – i.e., an EVM-equivalent environment that does not change any part of the Ethereum system. Ethereum equivalence can be considered as a step above EVM-equivalence, meaning that any Ethereum-based application would be able to run perfectly without the need for additional tooling or modifications.

Taiko

Taiko is one of the newest players to emerge that recently launched its Alpha-2 testnet on March 22, 2023[11], having been founded as early as 2022. Yet this does not pose a disadvantage to the project as the team behind Taiko is vastly experienced, with their founders having worked on Loopring, one of the first zk-rollup solutions on Ethereum. **Similar to Scroll, Taiko is aiming to develop a fully Ethereum-equivalent solution and consequently build to gain a type-1 classification**.

What makes Taiko unique is that the protocol is specifically designed to reduce the time required for proof generation, something that is considered a disadvantage when zkSNARKS are involved. This is because Taiko only requires full zk-proofs to be generated for cross-layer transactions.

The exact date for Taiko's mainnet launch is not exactly confirmed, but it is envisioned to occur in early 2024.

Linea

ConsenSys, a leading blockchain software company, who have already launched a multitude of successful crypto products, are responsible for Linea and its unique zkEVM stack. ConsenSys announced the Linea testnet to the wider public on March 27, 2023[12]. Linea is the outcome of years of research conducted by the ConsenSys team, culminating in Linea's ability to circumvent gaps with zkSNARK technology. **With Linea's ability to generate zkSNARK proofs at a faster pace and not requiring a trusted setup**[13], the zkEVM solution is generating impressive traction without being deployed on mainnet, having already secured key partnerships with projects such as Lens Protocol, Celer Network and Cashmere.

6 Closing Thoughts

Many different teams are working on Ethereum's scalability – both from an optimistic and zero-knowledge perspective. While optimistic rollups have dominated in the last year, the launch of the first public zkEVM solution has set the foundation for users to begin utilizing DApps in a zk-rollup environment. zkSync Era represents an important milestone for the industry and for the adoption of zero-knowledge technology.

As with any emerging technology, the risk of unforeseen bugs and technical issues will always be present, yet zkSync Era has been relatively meticulous in its prioritization of security during the initial stages. Unfortunately, such prioritization yields a trade-off against decentralization in the interim, with teams trying to maintain control over sequencers and upgradability for the purpose of sustaining adequate performance and security standards. In the long run, we expect this to change as governance structures mature and confidence in the protocol grows.

It is also worthwhile to mention that the first few zkEVMs to publicly launch have generally possessed a lower EVM equivalence, namely type-3 and type-4, as per Vitalik's taxonomy. While less equivalent solutions do have advantages in prover performance and in their ability to harness non-EVM features, there are still a number of zkEVM projects yet to launch that are contesting for deeper EVM equivalence, such as Scroll, Taiko, and Linea. EVM as a computation engine is likely to face ongoing upgrades in the future, meaning that zkEVMs with more native compatibility may be well poised to adapt to such changes. Though more equivalence may not necessarily be fruitful during the adoption phase, it would be important for zkEVMs to pragmatically explore different options as the technology evolves.

With a product suite that includes zkSync Lite, zkSync Era, and zkPorter (and with more compatible solutions potentially in the works), zkSync has certainly done well in this area.

zkSync Era has, so far, outperformed in terms of metrics when compared to Polygon zkEVM (to which it went head-to-head at launch). The zkPorter protocol is particularly interesting and a potentially game-changing innovation in terms of what it provides from a speed and cost perspective.

Ultimately, we expect the landscape to be very different as more mainnet deployments from competing zkEVM players occur. We look forward to seeing how it turns out and how the year of the zkEVM evolves.

References

1. https://l2beat.com/scaling/projects/zksync-lite
2. https://blog.matter-labs.io/zkporter-a-breakthrough-in-l2-scaling-ed5e48842fbf
3. https://blog.matter-labs.io/gm-zkevm-171b12a26b36
4. https://dune.com/Marcov/polygon-zkevm
5. https://twitter.com/zksync/status/1659265233175695360?s=20
6. https://blog.matter-labs.io/milestone-3-zksync-end-to-end-prover-is-now-live-on-testnet-9ee4fdc1874f
7. https://zksync.io/security
8. https://vitalik.ca/general/2022/08/04/zkevm.html
9. https://scroll.io/blog/alphaTestnet
10. https://scroll.io/blog/proofGeneration
11. https://taiko.mirror.xyz/A6G6TNN-CXDAhl42k_bNHg_20fyGcT0xH-LBBSOPNzU
12. https://linea.mirror.xyz/6G30hwV2wPs_wPv0VEgHYaIdghMkIQaad-OI_0br1hM
13. https://eprint.iacr.org/2022/1633.pdf

Latest Binance Research Reports

Institutional Custody in Crypto

A detailed study of the institutional custody landscape.

BRC-20 Tokens: A Primer

A close look at the BRC-20 market, including their origins, market outlook, effects on Bitcoin's metrics, and much more.

Data Insights: Lending

A data-driven analysis of the growing DeFi lending market.

Monthly Market Insights - May 2023

A summary of the most important market developments, interesting charts, and upcoming events.

About Binance Research

Binance Research is the research arm of Binance, the world's leading cryptocurrency exchange. The team is committed to delivering objective, independent, and comprehensive analysis and aims to be the thought leader in the crypto space. Our analysts publish insightful thought pieces regularly on topics related but not limited to, the crypto ecosystem, blockchain technologies, and the latest market themes.

Shivam Sharma

Macro Researcher

Shivam is currently working for Binance as Macro Researcher. Prior to joining Binance, he worked as an Investment Banking Associate / Analyst at Bank of America on the Debt Capital Markets desk, specializing in European Financial Institutions. Shivam holds a BSc in Economics from the London School of Economics & Political Science ("LSE") and has been involved in the cryptocurrency space since 2017.

Moulik Nagesh

Macro Researcher

Moulik is currently working for Binance as Macro Researcher. Prior to joining Binance, he has experience working in cross-functional roles for Web3 and Silicon Valley based tech companies. He also possesses co-founder level experience at start-ups. Moulik holds a BSc in Economics from the London School of Economics & Political Science ("LSE") and has been involved in the cryptocurrency space since 2017.

Resources

Read more here

Share your feedback here