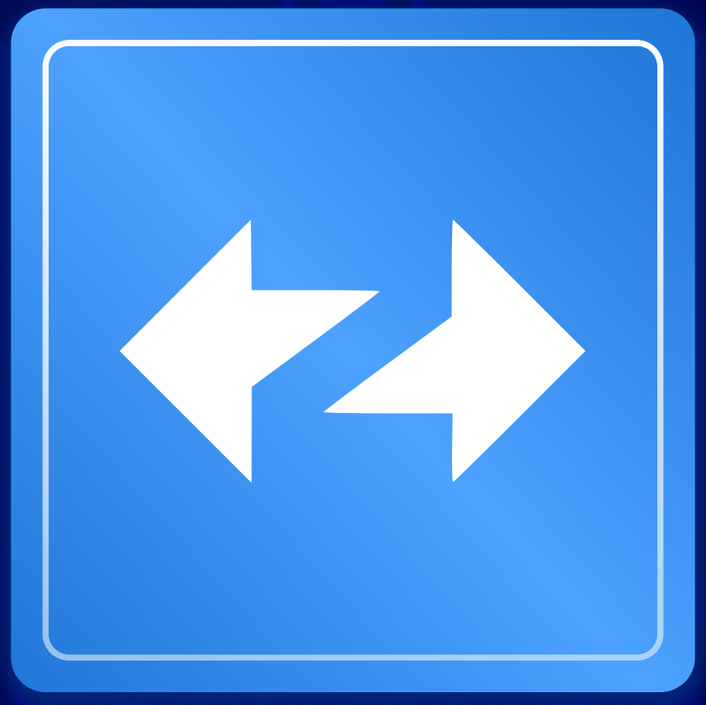


DELPHI CONSULTING

ZKsync

The Elastic Network Endgame

CONTENTS

Executive Summary

2024 will undoubtedly go down as the year crypto experienced unprecedented growth in institutional interest and demand.

Since the approval on January 10, **total cumulative net inflows** for the 11 Bitcoin Spot ETFs have exceeded $30B. Institutional adoption has rapidly gained momentum, with JP Morgan's Kinexys and BlackRock's tokenized money market funds leading the charge. On CNBC, Larry Fink aptly described tokenization as the next step in the technological revolution of financial markets, a sentiment echoed by 97% of institutional investors in a BNY Mellon survey.

The unrelenting demand for asset tokenization primarily stems from challenges in traditional financial markets – particularly the illiquidity of real world assets (RWAs) exacerbated by restricted access. Barriers to entry hindering progress are especially evident in the demand for computing infrastructure and private equity. Tokenization in crypto levels the playing field by enabling fractional ownership of any asset, making asset opportunities accessible to everyone. It reduces costs by eliminating intermediaries and enabling atomic settlements. Tokenization also supports 24/7 trading, fosters deep liquidity, and lowers entry barriers, making it a transformative force in modernizing financial markets. The opportunity is immense, with BCG and ADDX estimating the tokenized asset market could reach **$16 Trillion** by 2030, equal to **10% of the global GDP.**

Blockchain technology emerges as an equally disruptive solution in the banking sector, as the industry continues to grapple with increasing regulatory pressures, fraud, high operational costs, and the demand for faster, more secure services. Among the blockchain's emerging high-potential applications are faster and cheaper payments, instantaneous cross-border transactions, P2P transfers, efficient clearance & settlement, secure digital identity verification, and streamlined KYC.

Despite these two massive opportunities, there's still a long way to go before blockchains achieve institutional mass adoption, begging the question: what's holding it back?

The answer is twofold. First, blockchains are facing key challenges themselves: fragmentation of liquidity, users, and activity, has led to a significant deterioration in user experience, capital efficiency, and network integrity.

For instance, L2 scaling solutions now boast a total TVL of **$49.23B**, with the vast majority spread across 30 different networks each vying for market share. And while performant L1s make significant strides in improving scalability, they often make compromises when it comes to decentralization and security. The impact is felt not only by users but also by developers and enterprises, all of whom face an overwhelming set of questions about safety, composability, and use case suitability.

Secondly, public blockchains in their current form are unfit to meet the institutional demand for tokenization and banking needs. Popular blockchains like Bitcoin and Ethereum operate as public, permissionless ledgers. Anyone can participate, verify transactions, and access the public records. However, data privacy, controlled access, confidentiality, and conformity with regulations are all non-negotiables for institutions. This has created a dire need for highly customizable blockchain environments that can meet regulatory requirements and drive the mass adoption of tokenization and banking applications.

Enter ZKsync 3.0 - The Elastic Network

Introduced as a protocol update in June, ZKsync Era transformed from a single ZK rollup into the ***Elastic Network***. By reconfiguring the ZKsync L1 bridge contract into a shared router contract, the basis for an evolving network of interoperable ZK Chains was laid.

Utilizing the ZK stack, ZKsyncs' open-source codebase, anyone can build a modular ZK Chain and seamlessly integrate with the Elastic Network to be part of an ecosystem that benefits from:

- **Trustless and low-cost interoperability** with all other chains in the network by leveraging shared L1 contracts, middleware, and the same ZK proof system.
- **Revamped user experience** via native account abstraction, unified liquidity, smart wallet SDK, simplified onboarding through passkeys, and more.
- **Horizontal and vertical scalability** achieved by the shared prover system & parallelized ZK Chains.
- **Customizability** of modular ZK Chain architecture enabling **confidentiality with verifiability** via Validiums & ZK proofs while retaining **full control** over data availability, data privacy, user confidentiality, and accessibility.

- **Multi-layered Security** via tamper-proof ZK cryptography, formal verification, and SGX.

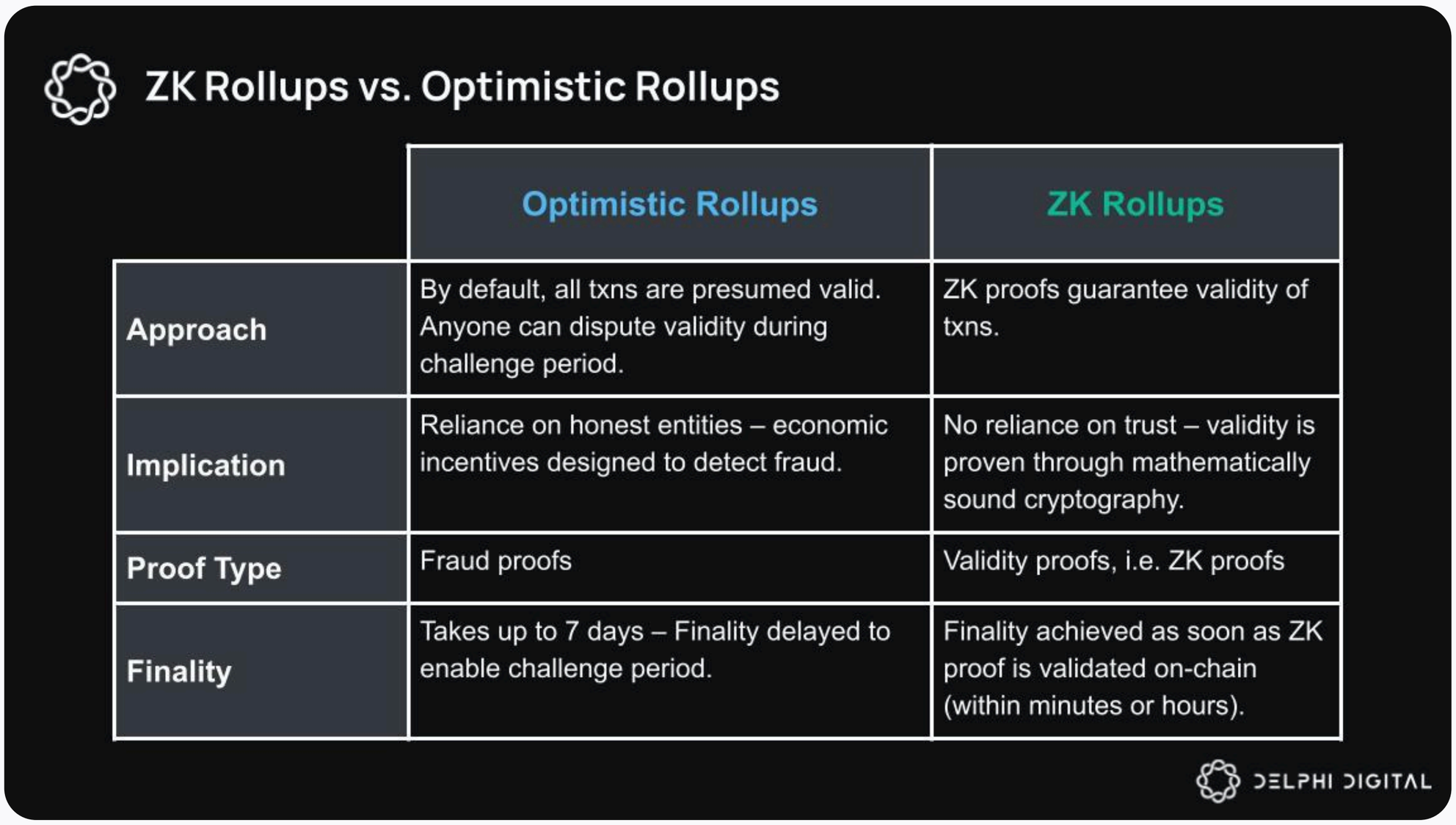
This design empowers enterprises to build their own proprietary sovereign ZK Chain tailored to regulatory compliance, streamlined business operations, and data confidentiality, all while taking advantage of the benefits that ZKsync has to offer.

Over 13 new ZK chains are set to join ZKsync becoming part of the Elastic Network, with a focus on diverse chains/applications, including tokenization and private permissioned blockchain environments tailored for enterprises

ZK Rollups vs. Optimistic Rollups

Before we dive into the technical details of ZKsync, let's quickly look at the differences between the two major rollup types.

There is a strong case to be made that **Zero Knowledge proofs** present the **mathematical key** to achieve hyperscalability and security, asserting the technical superiority of validity proofs over fraud proofs.



Optimistic rollups inherit their name from their "optimistic" approach to handling the off-chain transactions and computation. By default, Optimistic rollups assume that all transactions are valid. Because of this assumption, proofs for transaction bundles are not submitted to the Layer 1 in conjunction with the bundles. Instead, to safeguard against fraudulent or incorrect transactions being validated, Optimistic rollups use a fraud-proving scheme.

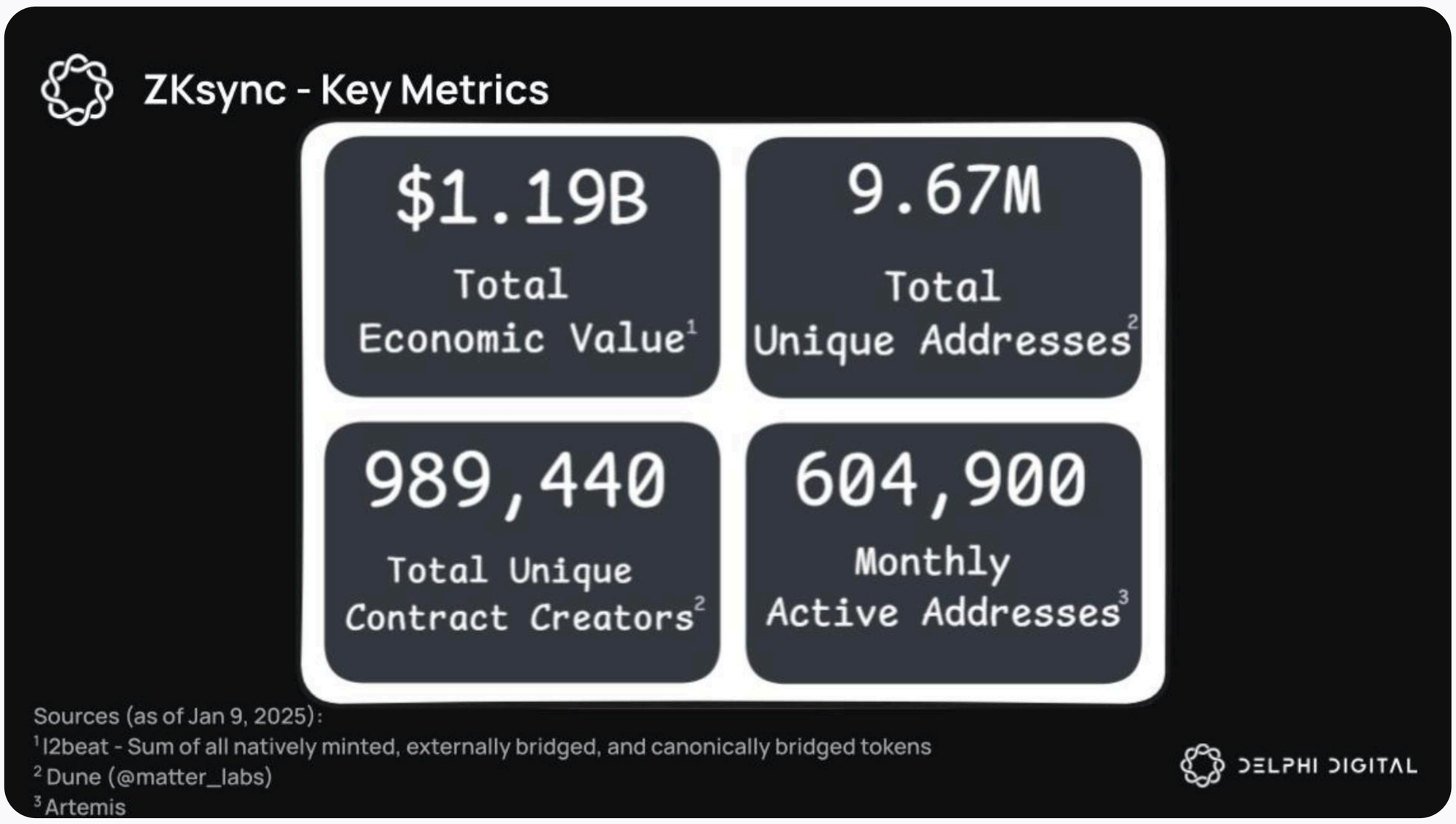
When a bundle of transactions is posted to the Ethereum L1, a challenge period commences before final verification takes place. During this time period, anyone can dispute the validity of the bundle by computing a **fraud proof**. If no valid challenges arise, the bundle is accepted on the Layer 1. However, if a fraud proof demonstrates the invalidity of a bundle, the entity that submitted it, known as the sequencer, is penalized. So, instead of being rewarded for a valid submission by receiving tokens, the sequencer loses part of their capital posted as collateral.

In contrast, zero-knowledge rollups, or short ZK rollups, operate differently by submitting validity proofs when sending compressed data bundles to Ethereum. At a higher level, this entails computing the transactions off-chain, compressing the transaction information into a data bundle, generating a **Zero Knowledge proof**, and posting it to Ethereum.

As a result, some ZK rollups only need to post state diffs to the L1, whereas Optimistic rollups must post information for every L2 transaction to the L1 to enable fraud proofs and make transaction challenges possible. This difference reduces the workload on the Ethereum network for ZK rollups, paving the way for improved scalability and lower costs.

ZKsync Era

ZKsync Era is a Layer 2 zkEVM leveraging Zero Knowledge Proofs designed to scale blockchains efficiently. Using the battle-tested ZKsync network, users enjoy low transaction costs, fast confirmation times, and the same level of security guarantees as the Ethereum network.



With over **$1.19B i**n total economic value (the sum of all natively minted, externally bridged, and canonically bridged tokens) ZKsync ranks first among all ZK rollups. Live on the mainnet since March 2023, ZKsync has served more than 9,670,000 unique addresses and gathered an active cohort of over 604,000 unique monthly active addresses (an individual person may be active on multiple addresses). Beyond its activity metrics, ZKsync stands out from other ZK rollups due to key nuances in its design.

Lifecycle of a Transaction on ZKsync

To highlight ZKsync's novel features and benefits, let's examine the lifecycle of a transaction on ZKsync.

1. **The ZKsync user signs and submits a transaction.**

The ZKsync sequencer receives submitted transactions, collects them, and orders them based on submission time.

2. **Sequencer leverages the zkEVM.**

While a sequencer running on Ethereum uses the EVM to execute code securely across all Ethereum nodes, ZKsync's sequencer employs the customized zkEVM instead.

This is the first important architectural nuance to Ethereum and other ZK rollups, because using this customized VM comes with notable advantages. In contrast to the EVM and other VMs, the ZKsync VM is specifically tailored to efficiently produce proofs of correct transaction execution. It uses custom bytecode designed to be provable in ZK. This drastically reduces friction, resulting in greater throughput. The zkEVM also handles storage and gas fees with customized metering, leading to lower costs for users.

Since ZKsync Era is an L2, the zkEVM inherits the flexibility to offer advanced functionalities earlier than the EVM. For example, ZKsync often supports new predeployed contracts before Ethereum does, such as precompiles for the secp256r1 curve. Predeployed contracts are able to perform actions that typically require higher security access and functionality, reducing computational load and improving gas affordability.

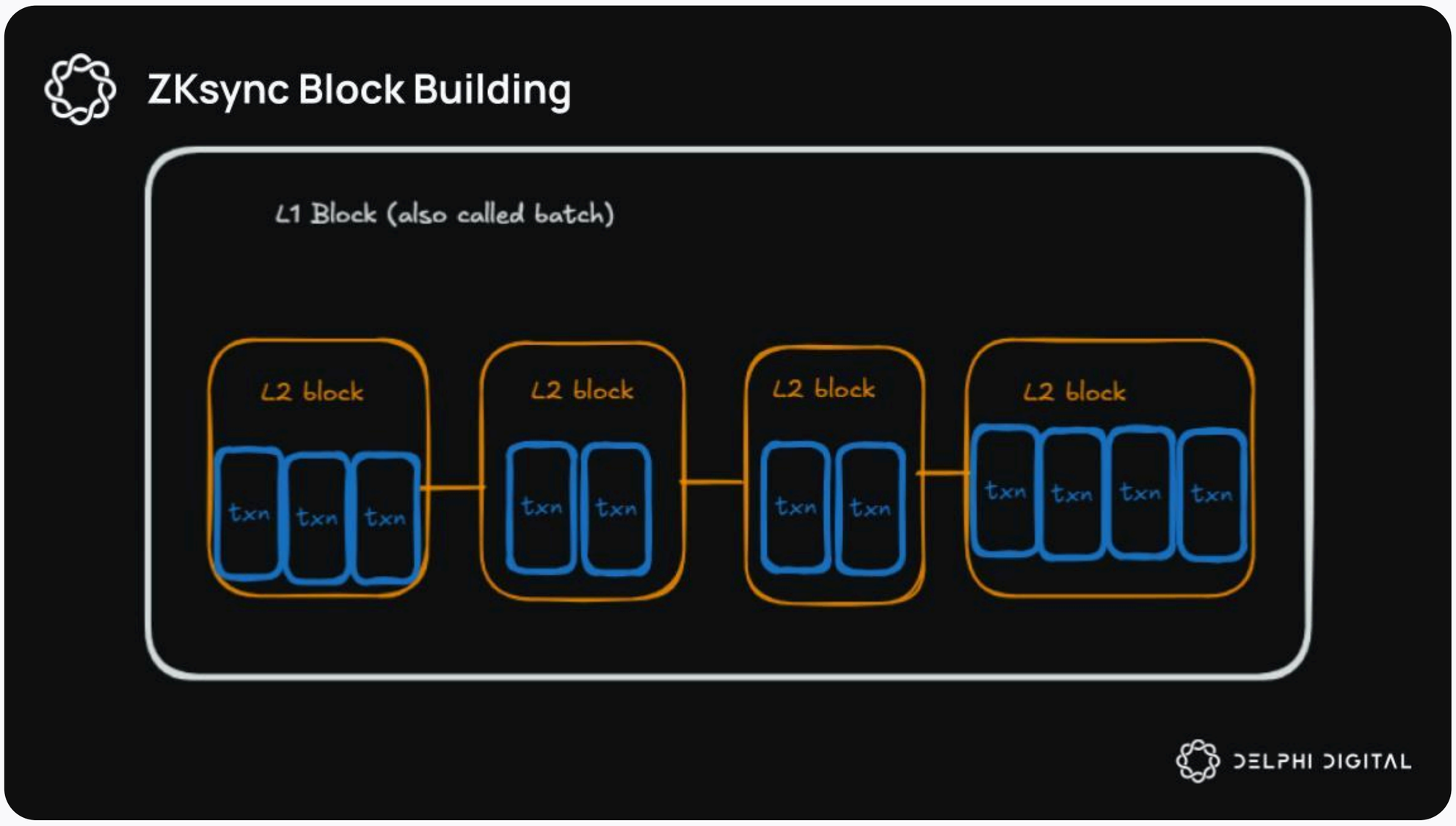
Overall, the zkEVM is a vital piece of custom infrastructure designed for specialized, efficient, secure, and scalable throughput resulting in improved time, cost, and operation efficiency. The zkEVM and its capabilities are the key drivers in keeping costs low for ZKsync users, the rollup, and the Ethereum L1.

3. **Soft Confirmations are produced**

The sequencer orders all submitted transactions bundling them into L2 blocks. Once a transaction is included in a L2 block on ZKsync, a soft confirmation is sent to the user. Since this typically happens within one second of the users submitting transactions, soft confirmations feel near synchronous.

4. Block Building

The L2 blocks are significantly smaller, containing fewer transactions, than the L1 blocks submitted to Ethereum. Due to their smaller size, L2 blocks are processed much faster, with ZKsync generating one every second. After producing a number of L2 blocks, they are chained together to form a single L1 block which is then submitted to the Ethereum L1.

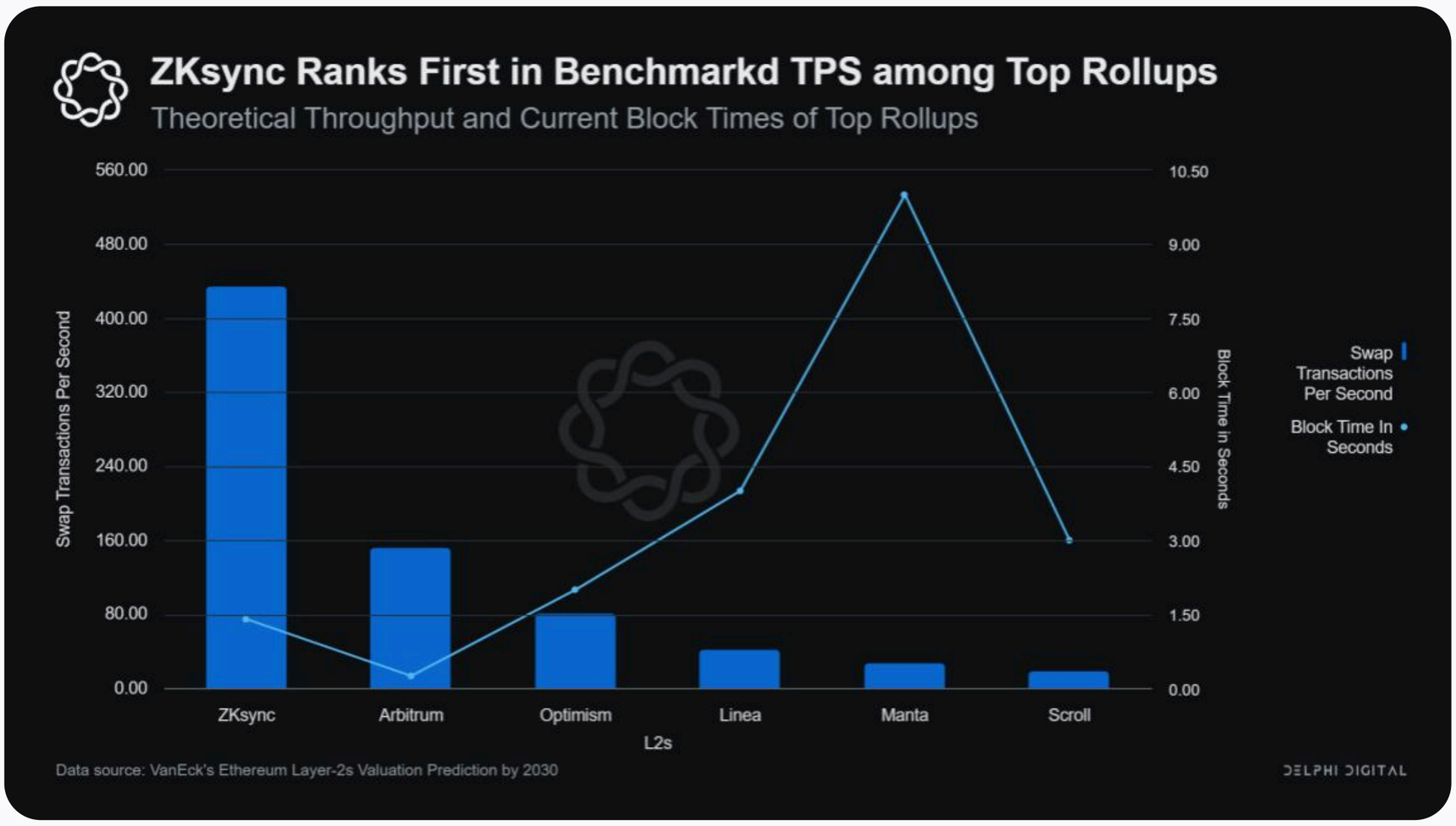


5. Data is sent to the L1

Another important nuance is the fact that data is sent to the Ethereum L1 before a ZK proof for the validity of the block is submitted. This initial data only outlines the planned changes to ZKsync's network state, allowing Ethereum nodes to prepare for the upcoming ZKsync state difference. By doing so, storage needs can be estimated in advance optimizing the subsequent data submission – a small but meaningful execution difference.

6. ZK proofs are submitted

To prove the validity of all blocks and its transactions submitted to Ethereum, a prover is needed. For ZKsync, its custom proving system called the Boojum proof system serves as the prover and generates ZK proofs. In April, VanEck benchmarked throughput for leading rollups, including both top ZK rollups and top optimistic rollups. ZKsync led the theoretical throughput results at **434 TPS** while having the second lowest block time.



Notably, the Boojum proof system **wraps the ZK proof** before submitting it, adding another layer of performance to the system. Similar to zipped files, this wrapped proof compresses its contents making the ZK proof considerably smaller and cheaper to verify on the L1. As a result, the costs incurred by ZKsync are lower and thus drive down costs for each transaction and the users themselves. Ultimately, **the more transactions are included in a bundle** and verified with a ZK proof, **the smaller the verification costs per transaction.**

That's because ZKsync pays proofing costs per ZK proof submitted to Ethereum. Since each ZK proof validates one bundle of transactions, the verification costs per transaction goes down the more transactions are included in a bundle, achieving efficient economies of scale – often referred to as **amortization of costs.**

Effect of Cost Amortization via Batching

For illustrative purposes only, the calculations assume an arbitrary proof cost of $10 to demonstrate the effect of cost amortization.

TXN count in a bundle	Cost per TXN
50	$0.20
200	$0.05
1000	$0.01
4000	$0.0025

DELPHI DIGITAL

7. Finality

Finality is the last step in the transaction lifecycle. To better grasp the concept of finality for ZKsync, we can think of finality in two different steps: L2 soft confirmation and L1 finality.

Once the ZK proof is submitted to the Ethereum L1 to validate the transaction bundle, the batch is scrutinized by a final verification step. This final step includes an intentional delay of 3 hours. This delay acts as a safety measure. After passing final verification, the batch is settled on Ethereum and added to Ethereum's blockchain, achieving L1 finality. At this point, the transactions in the batch are irreversible unless Ethereum’s network state is challenged. This is the reason why ZKsync inherits Ethereum’s security guarantees.

To enhance the user experience, transactions on the ZKsync L2 are instantly confirmed via L2 soft confirmation as soon as the sequencer includes a transaction in a L2 block. These instant confirmations result in immediate asset availability. Meaning, tokens become transferable immediately upon L2 soft confirmation and can be used instantly.

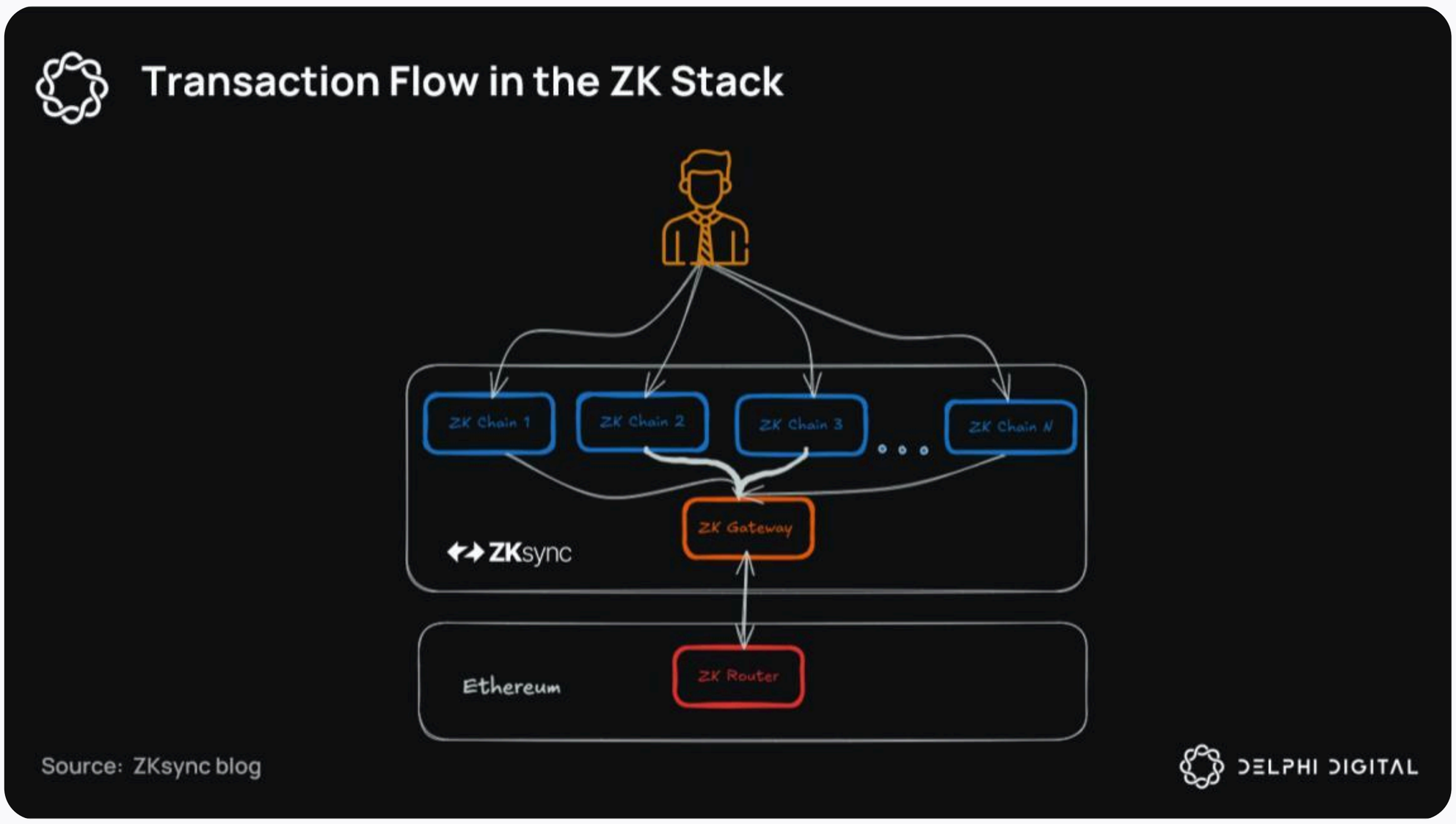
Note: ZKsync’s codebase, the **ZK stack**, is open-source and available to anyone.

The Elastic Network

ZKsync has transitioned from being a single rollup to strategically positioning itself as a versatile network capable of leading across multiple sectors, including institutional tokenization, permissioned private blockchain solutions, gaming, and consumer applications. Its architectural advantages stood out for impressive scalability and cost reductions, but this transformation was catalyzed by the ZKsync 3.0 protocol upgrade in June. By reconfiguring the ZKsync L1 bridge contract into a shared router contract, the basis for an evolving network of interoperable ZK Chains was laid - introducing the **Elastic Network**.

To understand how the Elastic Network achieves hyperscalability, enhanced UX & security, confidentiality with verifiability, and trustless interoperability, let's peel back each of its layers.

The secret to all of the above is found in its architecture with three pillars supporting the framework of the elastic network: the **ZK Router**, the **ZK Gateway**, and the **ZK Chains**.



1. ZK Router

The ZK Router consists of a set of different smart contracts deployed on Ethereum and builds the foundation of the Elastic Network. Assuming core responsibilities, it facilitates key interactions, manages the network state, executes new chain registrations, and most importantly, ensures that liquidity is shared across the Elastic Network.

2. ZK Gateway

The ZK Gateway serves as the middleware between Ethereum and the ZK Chains. Guaranteeing seamless interoperability, this pillar accelerates finality for low latency cross-chain transfers. Additionally, the ZK Gateway batches proofs and state data from all ZK Chains to optimize interactions with Ethereum, enhancing cost efficiency and overall performance.

3. ZK Chains

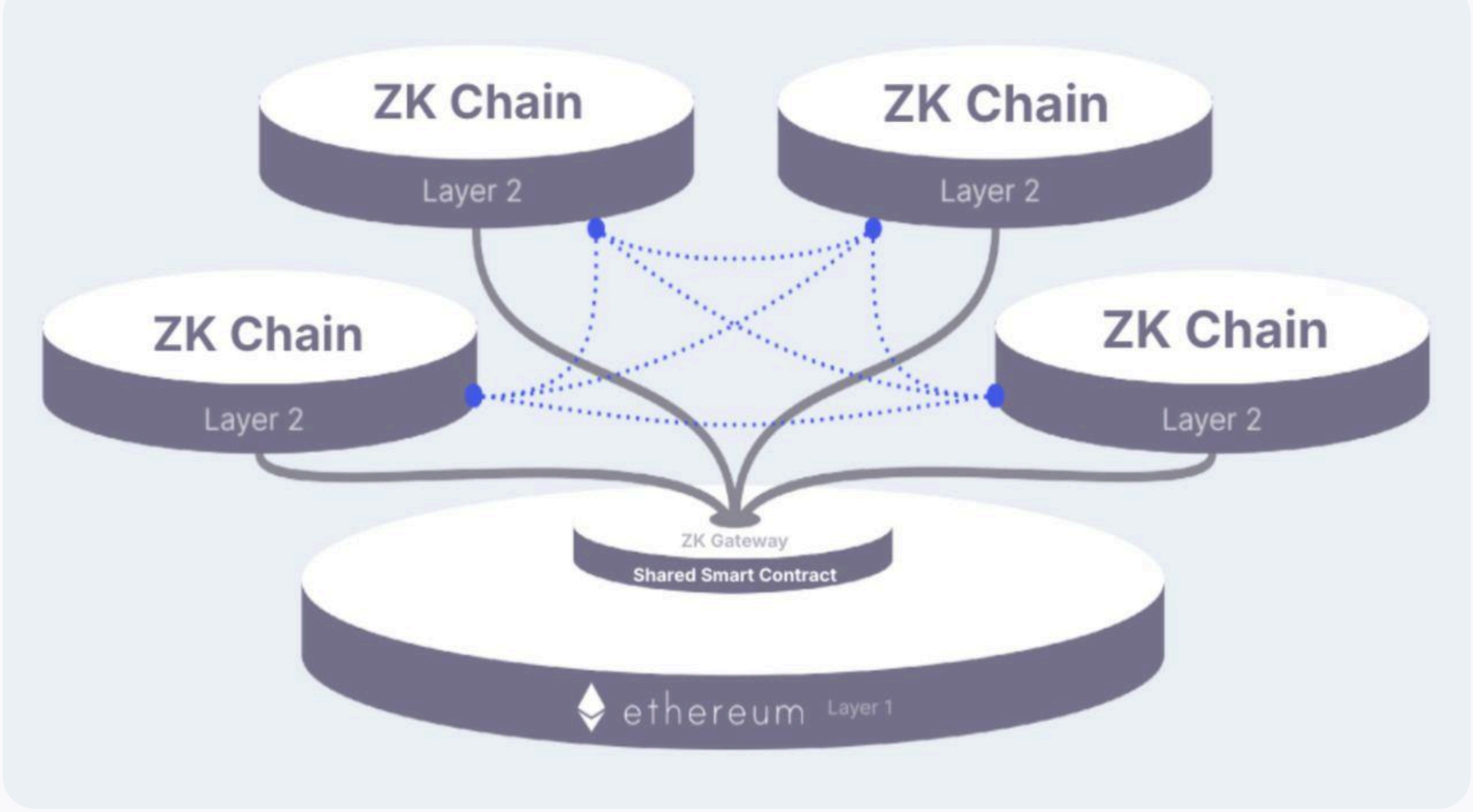
ZK Chains are the last pillar of the framework and complete the main architecture elements. At a high level, ZK Chains consists of parallel-running instances of the zkEVM achieving consensus and finality on the Ethereum L1 by operating on a shared bridge contract.

Individually, ZK Chains function as fully customizable, independent blockchains leveraging the ZK stack. The modular framework allows anyone to deploy and configure a customized ZK Chain. Despite operating completely independently and developers retaining control, ZK Chains are interconnected through the ZK Gateway and ZK Router.

Benefits of ZK Chains

Before highlighting a few interesting enterprises building ZK Chains, let's pinpoint why a large number of companies, governments, teams, and institutions have decided to do so. **From an institutional and developer perspective**, ZK Chains using the ZK stack have the following **distinct benefits**:

1. **Seamless Interoperability**



One of the main advantages is the seamless interoperability between ZK chains. While the ZK Gateway facilitates communication, protocol-native interoperability (systems of smart contracts, shown as orange lines above) connect ZK Chains by verifying transactions across the Elastic Network via Merkle proofs. Simply put, these are trustless connectors enabling cost-effective cross-chain function calls. They serve as the cornerstone that unlocks trustless and seamless interoperability between ZK Chains.

Moreover, transactions across the network are processed uniformly, maintaining absolute integrity, because all ZK Chains share the same proof system. Since ZK proof cryptography is tamper-proof, proofs can only be generated for valid transactions. This allows any ZK Chain to cross-verify proofs submitted to shared contracts, guaranteeing that each chain can safely trust its state.

Since ZK chains share the same bridge contract, liquidity in the Elastic Network is shared and not fragmented across all chains. This interoperability enables the transfer of assets directly between ZK Chains, without having to rely on their own liquidity like third party bridges and without the need to initiate calls on the destination chain.

Key advantages are:

- Native protocol messaging & simplified asset transfers
- No new trust assumptions or requirements of third party actors
- Security derived directly from proof being validated by Ethereum

As a result of the seamless interoperability, asset transfers and function calls are supported by robust security, capital efficiency, and low latency - with soft confirmations taking approximately 1s.

2. Horizontal Scalability & Cost Reduction

Generally speaking, horizontal scalability is achieved by running ZK Chains in parallel while aggregating proofs.

To start, the ZK Gateway combines multiple ZK proofs into a single proof-of-proofs that is settled to the Ethereum L1. The benefits of this proof composition are twofold: enhancing amortization of costs while unlocking greater scalability capabilities.

Secondly, recursive ZK proofs verify other ZK proofs within its circuit, giving the Elastic Network its growth elasticity. As usage grows, capacity can be increased by adding new ZK Chains without negatively impacting performance, ZK verifiability, or decentralization. This unlocks horizontal scalability as multiple ZK Chains can be run in parallel for the same purpose.

Thirdly, instead of recording each update to the network state, the ZK Gateway compresses multiple updates into a single one and only records differences between the old and new network state. This state diff compression reduces data size, requires less storage space, and as always, reduces costs associated with interactions with the Ethereum L1.

3. Enhanced User Experience

Due to the interoperability and composability of ZK Chains, users interact with the Elastic Network ecosystem as if it were a single, unified blockchain. Unique to the Elastic Network:

Only one address, account, and signature are needed to transact with any smart contract in the network – no cumbersome multi-step approvals or signatures required. Automation via native Account Abstraction eliminates the need for users to initiate destination chain calls manually, reducing complexity and lowering fees of bridging transactions to levels comparable with single-chain transactions. And with paymaster accounts supporting gasless meta-transactions, fees can be fully subsidized making interactions free for the user. Ultimately, creating a sleek, unique, and improved UX by allowing the seamless movement of users and crypto assets across all ZK Chains.

Onboarding is equally simplified. Users can simply create an account with a single tap via FaceID or by using Passkeys, a joint initiative by Apple, Google, and Microsoft to improve and streamline authentication. Instead of being forced to store compromisable seed phrases, passkeys create a unique user signature that proves possession of a passkey without sharing the passkey with anyone. The ZK stack also supports Apple's Secure Enclave, Webauthn, and Android Keychain to sign transactions, enhancing operations to be more user-friendly and secure – a significant stride towards a streamlined, web2-like UX.

4. Multi-Layered Security

Unlike other existing solutions, ZK Chains achieve a high level of security by having multiple security layers.

Firstly, instead of relying on game theory like Optimistic rollups, ZK Chains are purely trusting in mathematically correct ZK proofs – meaning zero honesty assumptions are made. On top of inheriting Ethereum’s security guarantees, security is further enhanced for all chains in the elastic network by using Intel Software Guard Extensions (SGX). SGX stands as the leading confidential computing technology in production, preserving data privacy and control through the creation of trusted execution environments (TEEs). ZKsync Era and the ZK stack leverage TEEs to build a multi-prover system in the future, allowing both ZK proofs and TEEs to validate the integrity of transaction batches. Incorporating TEEs into the network is an effective hedge mitigating the risk of potential bugs in ZK proofs, which could otherwise create serious protocol vulnerabilities.

Next, cross-chain forced transactions allow users to bypass censorship on one ZK Chain by submitting their transaction through another ZK Chain. This is much cheaper than forcing transaction inclusion on Ethereum. By enabling this feature, the network becomes more censorship-resistant and affordable for a wider range of users. Thus, greater security guarantees are unlocked.

Moreover, ZK Chains leverage ZKsync's technology stack - which has been in production since March 2023 and underwent security audits, protocol upgrades, and steady development improvements. To date, the team has spent over $10 million on security audits and bug bounty contests. Institutions and enterprises deciding to build on the Elastic Network do not have to take on unnecessary risk by trusting a new network and can instead rely on the seasoned ZKsync code.

Nevertheless, human-conducted audits can miss important edge cases or subtle bugs in complex code. To strengthen security assurance of the zk-verifer, the network takes advantage of formal verification. The zk-verifier is responsible for ensuring that ZK Chain transactions are processed as intended by checking the correctness of ZK proofs – bugs in the verifier could make the Elastic Network vulnerable to attacks. By leveraging formal verification, a mathematical approach to proving correctness of code, the risk of bugs related to the zk-verifier can be reduced providing a higher level of assurance than other ZK rollups.

Lastly, ZKsyncs source code is EVM-compatible, meaning the largest cohort of applications and experienced developers in web3 can redeploy on ZKsync and other ZK Chains without refactoring any code. The risk of missing potential bugs is minimized, aiding in the prevention of exploits.

5. Customization & Confidentiality

The modular design of ZK Chains provides enterprises with the flexibility to tailor their blockchain architecture to specific needs, offering choices such as:

- Chain Type: Rollup or Validium
- Data Availability (DA): Ethereum, Third party, or Own storage solution
- Gas Token: ETH or Custom Token
- Transaction Sequencing: Centralized, Decentralized, or Shared
- Accessibility: Permissionless or Permissioned
- Consensus and Nodes: Centralized vs. Decentralized

For privacy-focused use cases, enterprises can opt for the validium design. Unlike ZK rollups, validiums enhance scalability by relying on off-chain DA and computation. Although transaction data remains off-chain, the ZK proof is still verified on Ethereum to validate state changes, enabling confidentiality with verifiability. This unlocks the ability to choose your own data storage solution, such as on-premise or cloud solution, and retains control over sensitive information enabling private networks that maintain interoperability with other ZK Chains.

Additionally, institutions whose services require KYC or KYT for regulatory compliance can opt for permissioned access. This entails gating access to a specific ZK Chain through a whitelisting process.

From an institutional perspective, this modularity is arguably the most significant benefit. It enables the implementation of privacy features to keep sensitive information confidential, meet different compliance standards, gate access, and adhere to regulatory requirements – imperative features for the banking and tokenization sectors.

Enterprises joining the Elastic Network

The aforementioned distinct advantages of ZK Chains position the Elastic Network well to meet the needs of advanced institutional tokenization and banks seeking private and permissioned blockchain solutions.

The notion that the Elastic Network offers solutions eliminating bottlenecks that have plagued the tokenization and banking sector is already starting to gain traction. ZKsync Era, the ecosystem's first chain, will soon be joined by over 13 new ZK Chains. A few standout enterprises pushing the boundaries by leveraging the ZK Stack:

Deutsche Bank: Asset Tokenization and Fund Management Platform

Deutsche Bank has partnered with Memento Blockchain to develop an interoperable platform for asset tokenization and fund management on a ZK Chain.

As a solution, the German financial giant is utilizing the advanced features of the ZK Stack to simplify the deployment and operation of tokenized investment products, reducing the complexity and costs associated with fund issuance and distribution. The initiative aims to address the regulatory challenges of using public blockchains in financial sectors, enhancing transaction efficiency while incorporating robust KYC and AML measures to ensure compliance with industry regulations.

Buenos Aires Government: Self-Sovereign Digital Identity Protocol

Tokenization use cases extend beyond financial applications, as showcased by the self-sovereign digital identity initiative in Argentina’s capital. The overarching goal was to create a digital trust framework to reduce costs, streamline operations, improve interoperability, and most importantly give citizens sovereignty over personal information.

Buenos Aires is revolutionizing digital identity for its 3.6 million residents and beyond through QuarkID, a decentralized identity open-source protocol powered by ZKsync. Integrated into the city’s miBa platform, the QuarkID wallet allows citizens of Buenos Aires to access their digital identity and manage personal data, such as birth certificates, marriage records, and proof of income. By leveraging ZK proofs, the system validates documents without requiring citizens to trust public services with sensitive information, ensuring privacy and security.

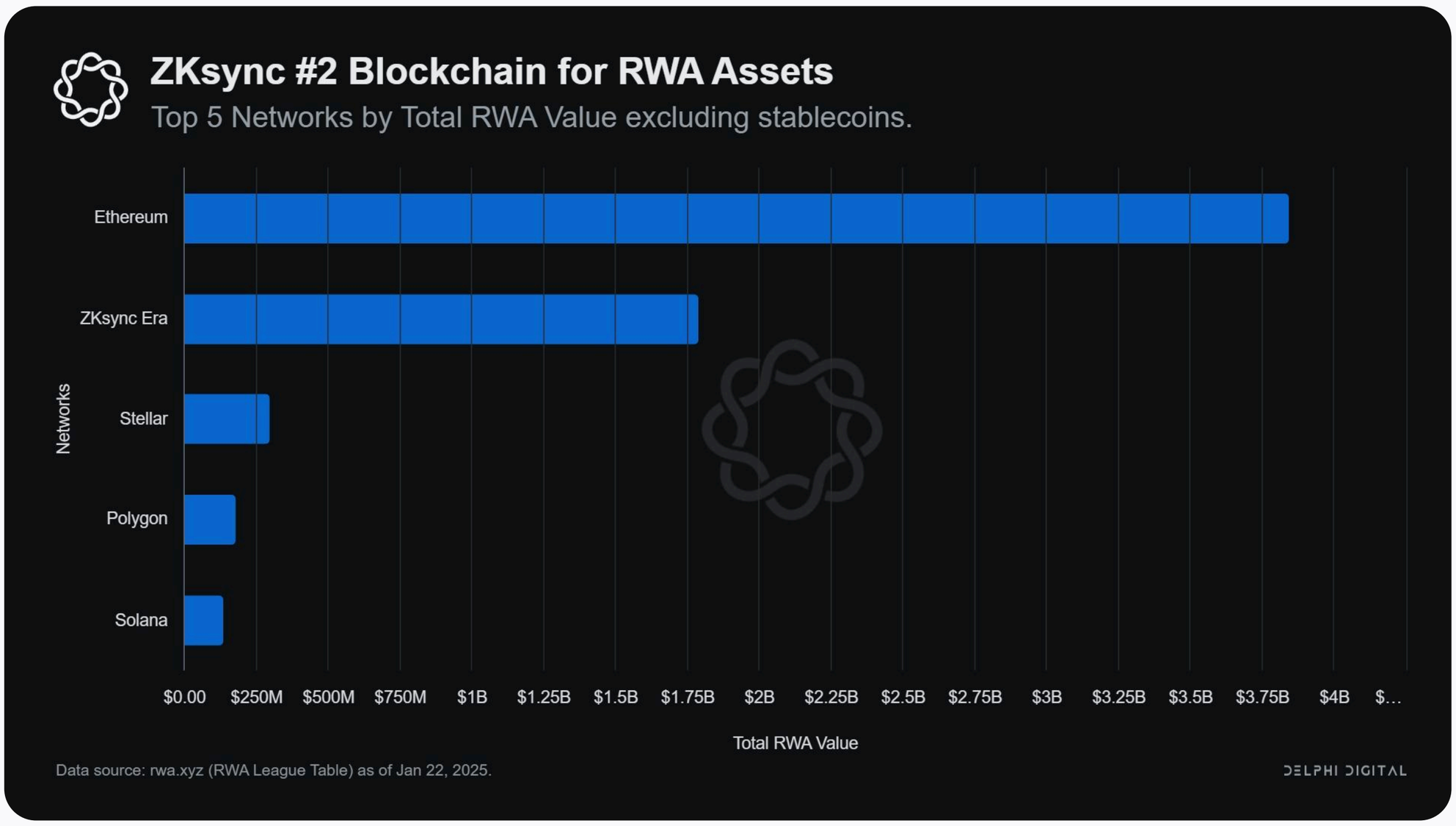
Recognized as a Digital Public Good, QuarkID, complies with international data protection standards set by the United Nations, and is now expanding across LATAM. Future plans include migrating to its own ZK Chain to enhance confidentiality, scalability and security, empowering millions more to take control of their digital identities.

Tradable: Onchain Private Credit Market

Tradable is a high-profile joint venture between Victory Park Capital, a private credit fund with $9B in originations, and Spring Labs, a blockchain data security firm, aiming to stand at the forefront of the private credit evolution. With a total RWA onchain value of $16.62B (excluding stablecoins), private credit presents the most sought-after tokenization commanding over 70% of the total RWA market share.

Built on top of ZKsync Era, Tradable provides institutional-grade private credit exposure onchain. This enables leading asset managers to securely and compliantly tokenize assets, unlocking access to diverse private credit opportunities. And by streamlining syndications on-chain, Tradable reduces costs and lowers barriers of entry traditionally associated with private credit transactions, opening the door to a broader investor base.

“Tradable seamlessly bridges the on-chain / off-chain divide, while abstracting away all the complexity of adopting web3 technology,” said Alex Cordover, CEO of Tradable. “By leveraging blockchain rails, we’re enabling the supply side to provide any arbitrary institutional grade asset, starting with best-in-class private credit opportunities, to any number of demand side investors, whether on-chain or not.”



In January 2025, Tradable achieved a major milestone by tokenizing $1.7B of assets across almost 30 institutional-grade private credit positions in collaboration with Victory Park Capital, Janus Henderson, and ParaFi Capital. This places Tradable as the now third-largest RWA asset platform globally and solidifies ZKsync as the number 2 network by Total RWA Value trailing only Ethereum.

Abstract: ZK Infrastructure for Web3 Gaming

Igloo, the parent company of the popular NFT brand Pudgy Penguins, raised over $11m in July to develop the Abstract Chain, a new consumer-focused L2 blockchain.

With the ZK Stack as the technical backbone, Abstract is building ZK infrastructure for Web3 gaming simplifying the development of decentralized apps. The overarching goal lies in powering consumer-facing applications at scale while maintaining low fees and rapid transactions times. This is achieved by leveraging the validium design and a self-managed DA as customization options within the ZK stack. By creating a fully private and permissioned blockchain, Abstract Chain facilitates fast proving, guarantees high TPS, and enables scalability to support millions of potential users. Currently live on testnet, Abstract is scheduled to transition to mainnet in January 2025.

GRVT Exchange: Self-Custodial Central Derivatives Exchange

The implosion of FTX and uncovered fraud scandal was a turning point for web3, leading to a significant trader migration to decentralized exchanges allowing self-custody. Although decentralized exchanges have made great strides towards being competitive with centralized exchanges, weaknesses still exist. Namely scalable, low latency trading and liquidity provision. Compared to their decentralized counterparts, centralized trading engines achieve lower latency and higher performance by leveraging centralized high-speed order matching systems. Additionally, decentralized exchanges typically struggle to provide deep liquidity for trading pairs and users experience higher slippage, inherent drawbacks stemming from current AMM implementations.

GRVT is a hybrid derivatives exchange blending the CeFi and DeFi world aiming to solve the aforementioned drawbacks and stands as the first regulated DEX offering a secure and compliant UX. Coupling an off-chain orderbook with onchain trade settlement, GRVT aims to leverage the strengths of each design to achieve deep liquidity while enabling high security and self-custody features. Built as a validium ZK Chain, this hybrid exchange preserves data privacy while enjoying the scalability and interoperability benefits of being part of the Elastic Network.

GRVT also takes advantage of the ZK stacks' native account abstraction features to enable zero-gas trading. The GRVT Mainnet Alpha went live on December 20, 2024, fostering a user base of over 30,000 KYC'd users.

Treasure: Decentralized Game Console

Previously integrated on top of Arbitrum, Treasure is a gaming ecosystem working on creating a decentralized game console. Beyond game development, the Treasure team are protocol builders developing a decentralized infrastructure tech stack aimed at replacing traditional gaming companies. The protocol functions as a DAO, governed by users staking the native token MAGIC.

To reduce transaction fees, leverage a fully interoperable account system, and create a network of app-specific Infinity Chain L3s, Treasure migrated from Arbitrum to Treasure Chain, its own rollup powered by the ZK stack.

The modular ZK stack is the framework underpinning the end-to-end interoperable ecosystem of decentralized gaming infrastructure with the overarching goal of fostering a community-owned gaming platform.The mainnet of the Treasure Chain launched on December 12, 2024, migrating over 15 games and $200m+ in assets to the Elastic Network. Key features span an universal account across all games & apps, sponsored transactions, an integrated DEX for onchain economies, and tooling for developers.

Lens: Decentralized Social Media

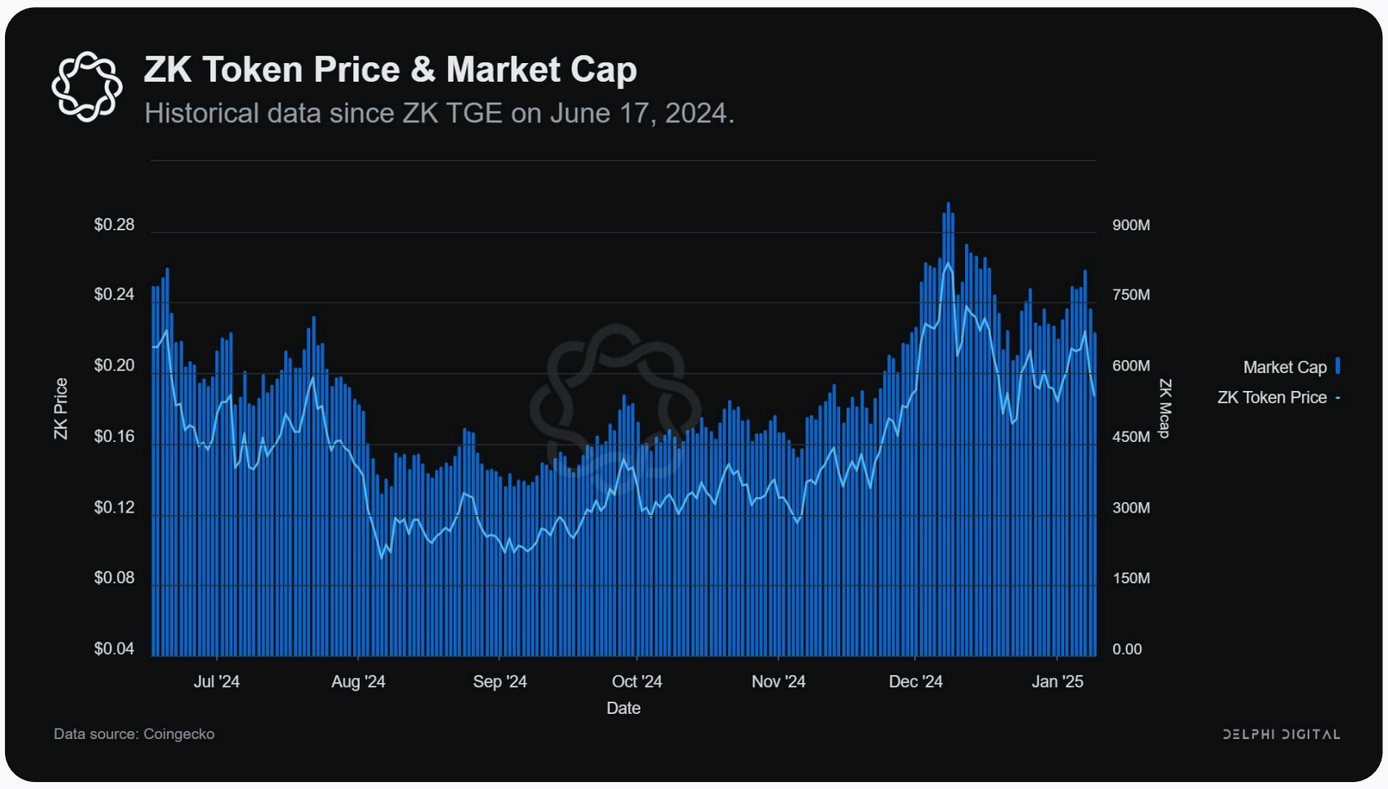
At a high level, Lens is an open social media network enabling users to own their content and connections. Supporting over 545,00 social media profiles, Lens allows developers to build applications on the protocol leveraging its infrastructure and audience. Currently, Lens' ecosystem consists of 15 core applications aimed at enhancing the social media experience. For instance Yup, a decentralized social platform, allows users to cross-post between Twitter, Lens, Farcaster, and Bluesky. In March 2024, Lens announced the intention to migrate to a ZK Chain and become part of the Elastic Network ecosystem. The choice to build on their own custom ZK Chain was made to upgrade their user experience comparable to Web2 platforms.

"To lay a scalable foundation for the future of social spaces, we chose to develop the next generation of Lens on what we believe is the most robust and future-proof technology — ZKsync's ZK Stack."

Powered by this ZK Stack, Lens aims to provide a UX on par with web2 social networks while granting users the benefits of data & content ownership, portability, platform choice, and secure transactions. All published content, including texts, images, and video URLs, is stored in a separate database. Linked to the publication through a web address, content can be hosted on external platforms.

Leveraging the ZK Stack, transactions created on the Lens protocol are either self-funded transactions or sponsored transactions. If a transaction is configured to be sponsored, users are not required to sign the transaction and all associated costs are covered by the integrated Lens API - creating a gasless and signless UX. The Lens ZK Chain is also built supporting custom gas tokens, allowing users and developers to pay gas fees in currencies such as USDC and ZK tokens.

ZK Token Utility & Governance

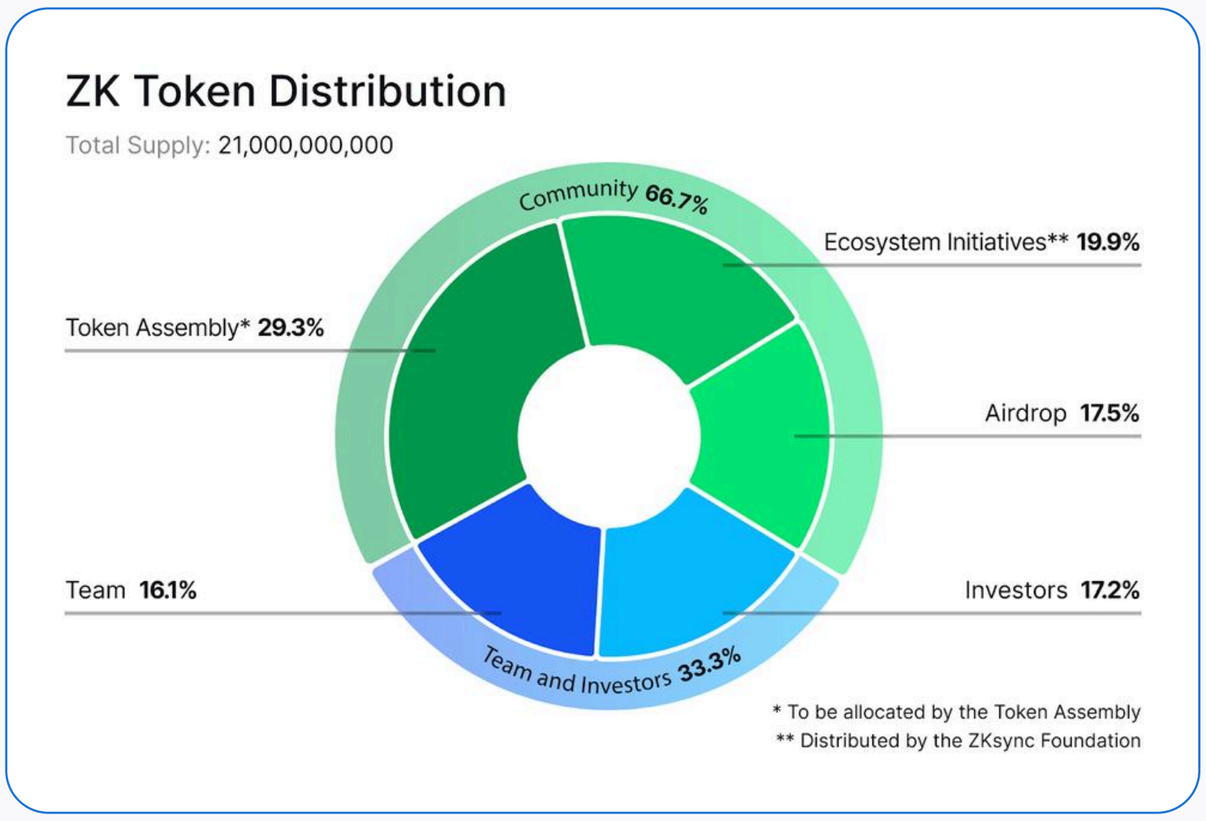


As of January 9, 2024, the ZK token trades at a price of $0.187 with a circulating market cap of ~$687.2M. While the circulating supply is 3,675,000,000, the total supply of ZK tokens is 21,000,000,000 resulting in a fully diluted valuation of $3.927B at the current ZK price.

Utility Design & Tokenomics

In June 2024, the native token, ZK, for ZKsync Era was introduced to decentralize the ecosystem's governance by granting token holders the rights to propose and vote on protocol upgrades.

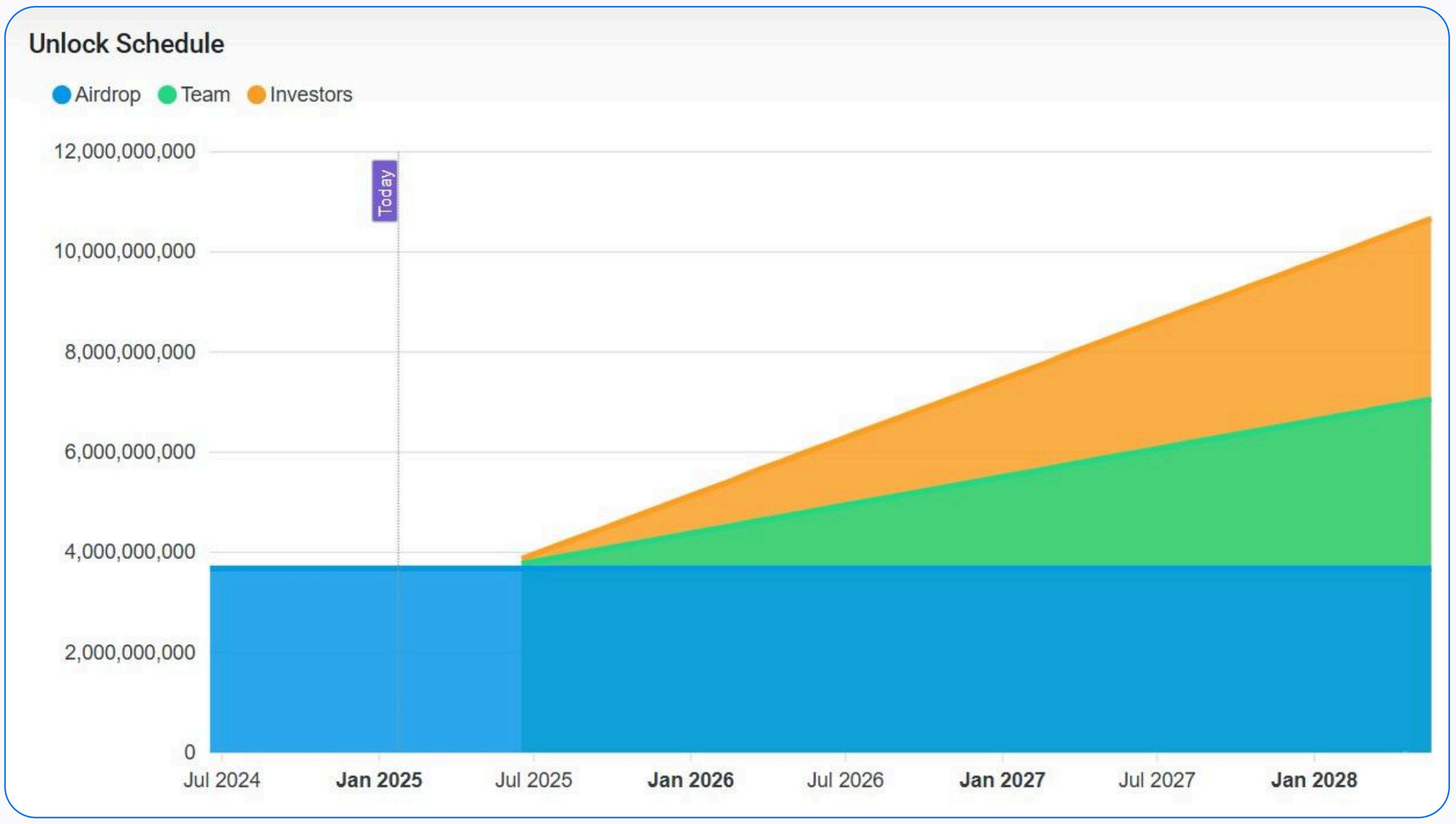
Beyond its main utility function as a governance token, ZK can also be used to pay for network fees on ZKsync and any ZK Chain. Additionally, to participate as a validator in the decentralized validation process of the Elastic Network, ZK tokens will be required. Additional utility functions could be introduced soon. For example the Gateway could be using the ZK token as the base token. This would mean that all chains connected to it would be paying in ZK for proof aggregation and interoperability. Other tokenomics designs could also replicate the Optimism Superchain model where sequencer revenue is shared with the protocol or governance could vote on additional fees for the Gateway.



source: https://blog.zknation.io/zk-token/

Currently, the total token supply for ZK is 21,000,000,000. At a high level, the token distribution can be categorized into a team & investor allocation, equal to ⅓, and a community allocation, ⅔ of the total ZK token supply.

Of the ⅓ allocated to investors and team members, 16.1% were distributed to the Matter Labs team, and 17.2% were dispersed to investors. Both allocations are subject to a 4 year unlock period (June 2024 - June 2028) with a one year cliff. Meaning, June 2025, 3.66% of the total supply will unlock from the team and investor distribution. Afterwards, the token allocations are vested monthly until June 2028, with a maximum monthly unlock of 0.82% of total supply.



None of the community allocations are subject to a vesting period. The airdropped tokens, equal to 17.5% of total ZK token supply, were unlocked immediately after the airdrop. The remainder of the community allocation, made up of the ecosystem incentives and token assembly, is distributed over time and managed by the ZKsync foundation and ZK Nation governance process.

Intro to ZKsync's Governance

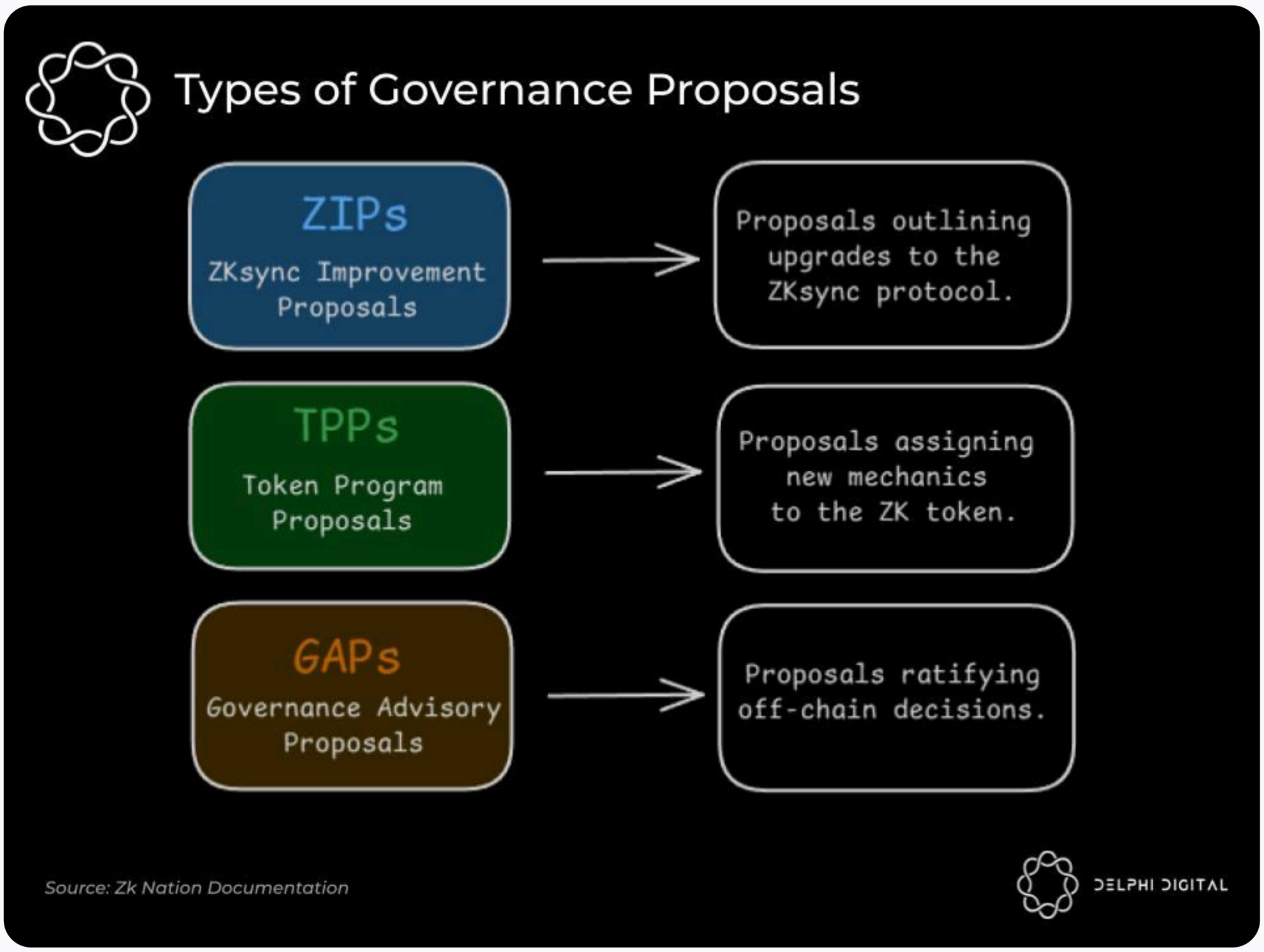
Each ZK token holds one vote in the ZKsync governance system that will soon encapsulate the Elastic Network ecosystem. With the intention to remove financial barriers and increase governance participation, a delegation mechanism was implemented allowing individuals without ZK tokens to hold voting power.

Therefore, token holders must first delegate their voting rights to a ZKsync address to exercise voting power, which can be their own or that of a third party. Addresses who are delegated voting power are referred to as delegates and inherit the right to vote on governance proposals. Notably, delegating voting power to a third party does not alter ZK token ownership but only transfers the right to vote. Token holders also retain the flexibility to re-delegate and revoke their delegation at any time.

While all delegates receive voting power, a minimum threshold must be met to submit a proposal for an onchain governance vote. Currently set at **0.1%** of the total token supply equal to 21,000,000 ZK tokens, this threshold amounts to **$4,410,000** based on current ZK prices. However, delegates who do not meet this threshold can seek eligible delegates to sponsor and submit the proposal on their behalf.

To enjoy legal protections, delegates can choose to become members of the ZKsync Association, an ownerless, non-profit organization. According to ZKsync, delegates cannot be legally held liable for decisions made in connection with proposals.

In total, there are three types of governance proposals tailored to specific actions in the ecosystem:

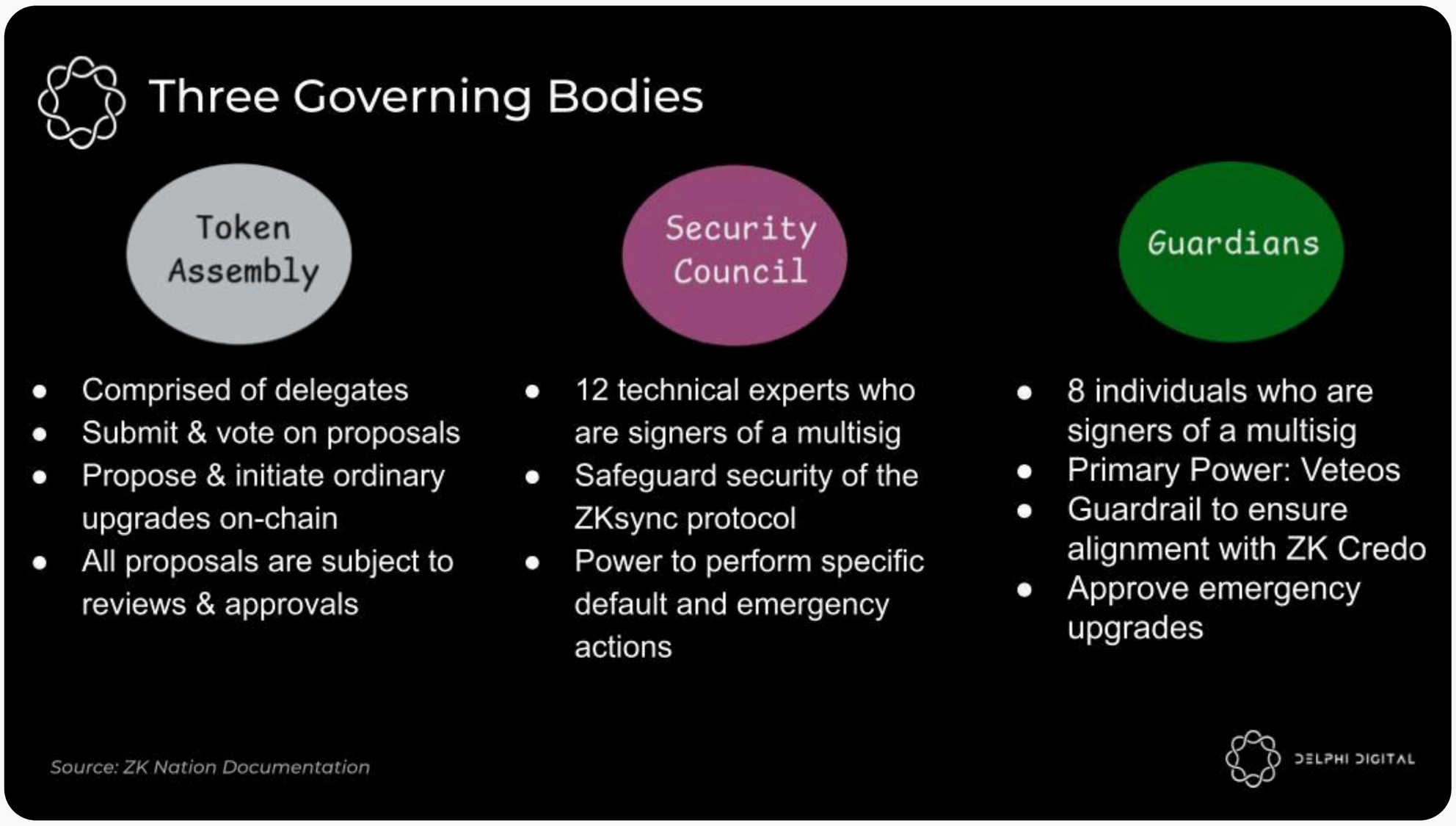


Three Body Governance

The design philosophy behind ZKsync's governance system is based on the values and principles of the ZK Credo. These include trustlessness, security, reliability, censorship-resistance, privacy, hyperscalability, accessibility, and sovereignty.

To prevent a rogue or adversarial government body abusing its power, the ZK governance system consists of 3 governing entities implementing separation of powers, checks, and balances: the Token Assembly, the Security Council, and the ZK Guardians.

Each body assumes different responsibilities with pre-defined abilities and constraints:

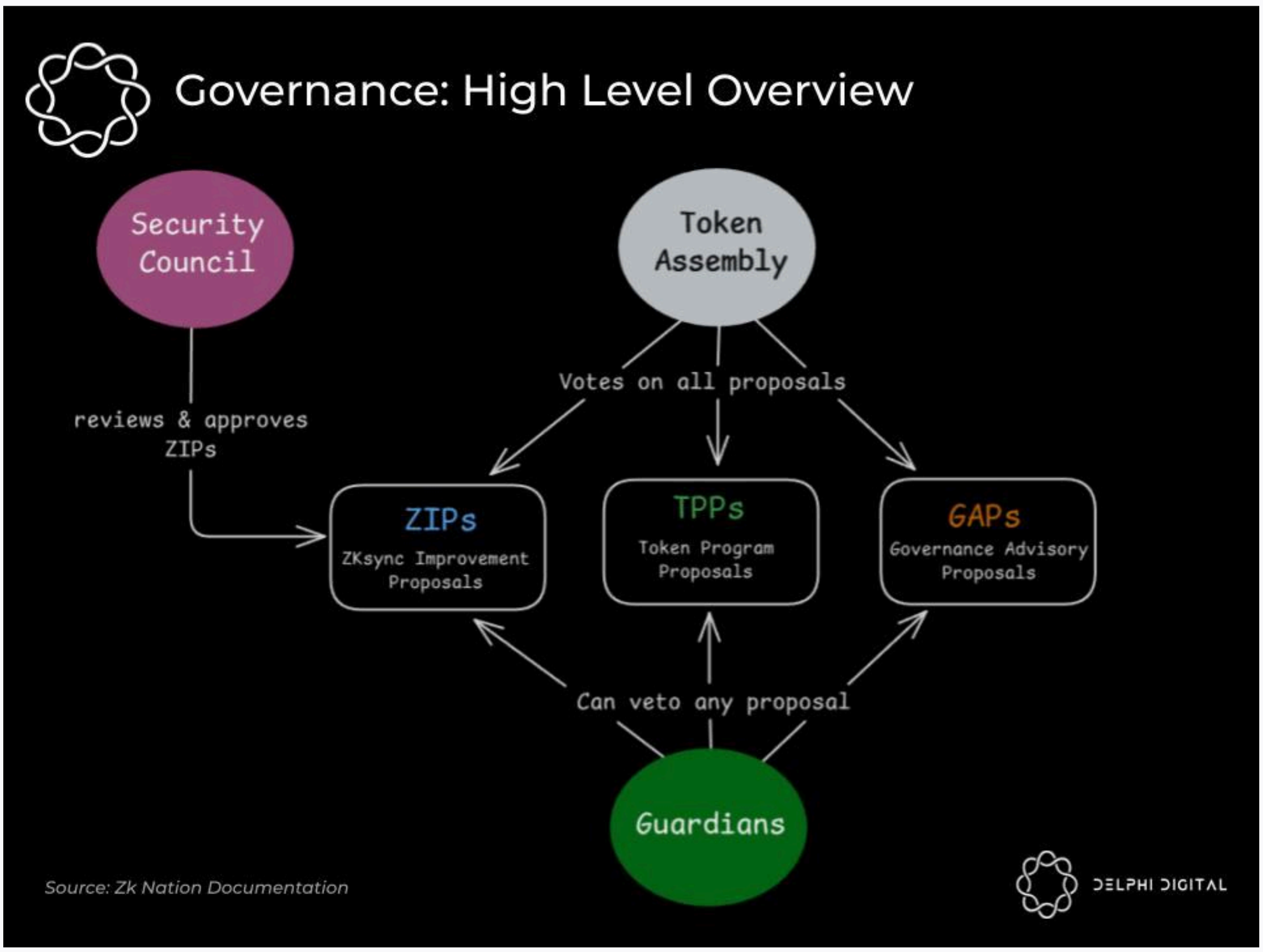


While the Token Assembly consists of token holders who delegate their voting power and delegates, the Security Council and Guardians are structured using smart contracts and legal entities. Both entities are legally bound to rules specified in charter documents aligning ethos and actions to be in the best interest of the ZKsync community.

The power of the Security Council to perform default and emergency actions include the ability to review and approve active proposals as well as the power to freeze the protocol and submit critical upgrades in the case of an emergency. However, the Security Council is also subject to several constraints. The Security Council cannot unilaterally submit & approve protocols and emergency upgrades require the approval of the Guardians and the ZKsync Foundation. Moreover, legal obligations of members are dictated by contractual agreements and bylaws and members can be removed or replaced following a onchain vote.

The Guardians include 8 individuals. Serving as signers to the guardian multisig, guardians have the ability to veto all governance proposals. They also inherit the ability to approve emergency proposals. Similar to the Security Council, membership is bound to legal obligations governed by bylaws and any guardian can be removed or replaced following an onchain vote.

At a high level, the relationship between each governing body and the types of proposals is structured as follows:



To conclude, there is no single entity or individual that retains the power to unilaterally propose and approve proposals. As a result, the ZK governance process is resilient via its built-in safeguards, autonomously enforced onchain, and mitigates the risks associated with typical governance models.

Business Model & Revenue Framework

Fee Mechanism

Each blockchain has revenue streams and expenses, including overhead, that must be covered using an economically sound and sophisticated fee structure.

On Ethereum, total fees paid combine a fixed base fee for each operation and an optional priority fee. The base fee is predetermined, while the priority fee, or validator tip, can be adjusted by users to potentially speed up transaction confirmation. Broadly speaking, the total transaction cost is the sum of these two fee types and users exert some control over transaction speed through their willingness to pay higher fees.

Since ZKsync is a rollup built on top of Ethereum, the fee mechanism must take the fluctuations of L1 gas prices into account and is designed with several nuances. Moreover, ZKsync must account for the costs incurred to commit batches to the L1, validate ZK proofs, finalize the network state, and process communication with the L1. Additionally, paymasters enable various account types to reduce transaction costs arbitrarily, which is another crucial aspect that ZKsync's fee mechanism must accommodate.

To overcome these obstacles, ZKsync **maximizes transaction inclusion** per batch, leverages a predefined **maximum gas price**, and **issues refunds**.

First, to amortize batch overhead expenses, ZKsync maximizes transaction inclusion per batch. Batch overhead, expenses associated with proving each batch, include both L1 costs and L2 costs. L1 costs entail proof verification and batch processing on the Ethereum L1 while L2 costs stem from paying for proving circuits. The total overhead depends on time constraints, memory usage, data limitations, and transaction slot capacity before each batch is sealed. Since the exact batch overhead expenses for each transaction cannot be determined before execution, ZKsync charges the maximum gas price upfront. Subsequently, after the transaction is completed, users receive a refund equal to the difference between the maximum cost and the actual cost incurred.

zkEVM Economics

The zkEVM economic framework can be separated into L1 costs and L2 revenue. L1 costs are the sum of batch expenses and withdrawals to the L1, while batch expenses make up the majority of incurred costs.

Moreover, costs associated with batches are threefold coming from

1) committing the batch to the L1,

2) submitting the batch to the L1 after generating the ZK proof, and

3) executing transaction processing of batches (L2 > L1 communication).

To turn a profit, the zkEVM covers these costs and generates revenue by charging users a transaction fee for L2 transactions. ZKsyncs' transaction fees are substantially lower than Ethereum's fees and the median monthly fee is the second lowest compared to other top ZK rollups.

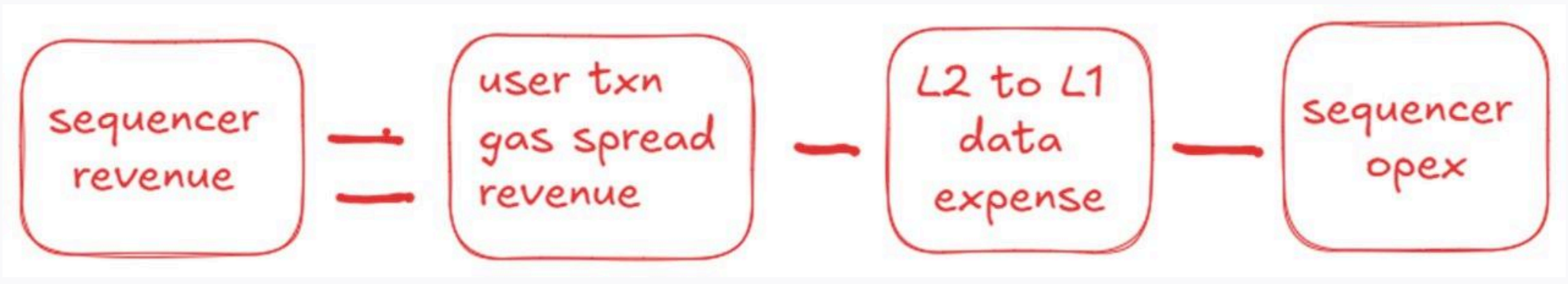
Median Monthly Fees across Top ZK Rollups

Rank	Network	Median Monthly Fee
1	Starknet	$0.006
2	**ZKsync**	**$0.015**
3	Linea	$0.021
4	Scroll	$0.047
5	Polygon zkEVM	$0.067
	Ethereum	**$3.40**

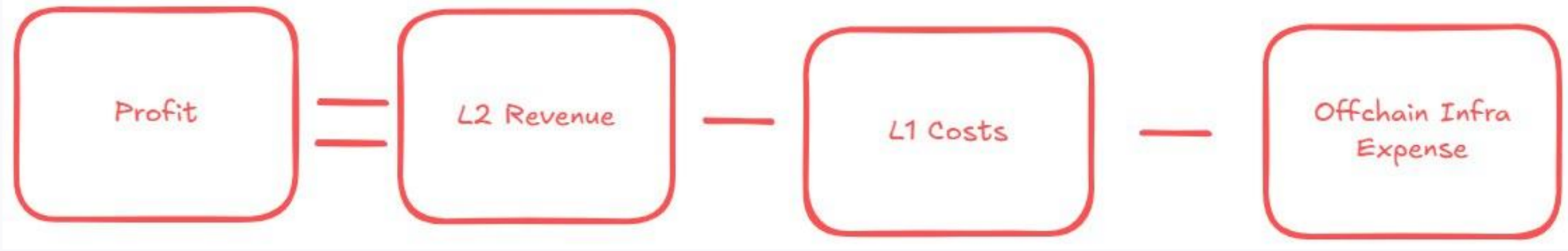
Data as of Oct 14, 2024
Source: growthepie (for L2s) and Token Terminal (for ETH)

DELPHI DIGITAL

The L2 revenue, or L2 transaction fee, includes the sequencer revenue and is calculated as follows:



Typically, the sequencer is also used to capture MEV, which generates additional revenue but can drastically increase transaction costs for users. As a result, MEV extraction is hostile to users in most cases. Unlike many other rollup sequencers, the ZKsync sequencer does not capture any MEV, forfeiting a significant revenue stream in favor of providing a much better user experience. Since running off-chain computation of transactions incurs infrastructure costs, the complete profit equation looks like this:



Elastic Network & ZK Token - Cryptoeconomic Framework

ZK Gateway Validation

There are distinct advantages economically incentivizing ZK Chains to use the ZK Gateway laying the foundation for its business model. The ZK Gateway will be operated by a set of decentralized and trustless validators removing the reliance on a single entity to maintain the mechanisms responsible for computing proofs to validate transactions. In short, the network of decentralized validators will secure the Elastic Network and be responsible for its reliability.

Participation in the decentralized validation process may be token-gated and require the staking of an ERC-20 token, such as the ZK token. To create economic incentives for participation, validators will earn fees for:

1. Facilitating cross-chain bridging,
2. Recursive ZK proof aggregation, and
3. Publishing and recompressing data to the DA layer.

The validator revenue for validators managing the ZK Gateway grows with the addition of each new ZK Chain joining the network. Most importantly, settlement costs on the ZK Gateway are significantly cheaper than settling directly on Ethereum. Combined with the seamless interoperability in the Elastic Network, ZK Chains have a strong incentive for participation.

Decentralized Sequencing

Sequencing on the Elastic Network can be decentralized, allowing all validators to stake tokens and gain the right to order transactions and build blocks. Transitioning to this decentralized sequencing model would enable greater value accrual, with kickbacks – such as sequencing fees, including MEV – distributed back to stakers. These fees could be captured through mechanisms like bidding auctions.

Decentralized Proving

ZKsync has the definitive goal to decentralize its prover network over 4 phases. Currently in phase 3, live proving is being tested. A small subset of proofs is generated and sent to the Ethereum L1. Successfully providing correct proofs on a regular cadence, with outputs ending on the L1, will conclude phase 3 and lead to the full integration of new trusted provers into the proving network (phase 4).

Once the decentralized proving network is established, there will be opportunities to expand it across ZK Chains. In this scenario, ZK Chains that opt into decentralized proving may pay part of their proving costs in ZK tokens to the provers.

Access Fee

To join the Elastic Network, ZK Chains may be required to pay access fees in ZK tokens. These fees would be programmatically charged to those entering the ecosystem and could be collected as a percentage of the profit generated by the ZK Chains. In practice, after covering costs for services like the ZK Gateway, interoperability validation, and decentralized sequencing, ZK Chains would then pay this access fee from their remaining profits.

It is important to note that all of the above information is subject to change, as no mechanism is currently integrated or finalized for implementation.

Conclusion

Indisputably, 2024 has seen unprecedented institutional interest and accelerating demand for tokenized assets and private blockchains. Yet, widespread adoption remains hindered by persistent challenges.

The Elastic Network is stepping up to systematically address these by introducing a network of ZK Chains that enables:

- Trustless and low-cost interoperability
- Enhanced privacy & confidentiality with verifiability
- Improved, web2-like UX
- Horizontal scalability
- Advanced, multi-layered security, and
- Distinct modularity

While benefitting from a unified system and shared infrastructure, each ZK Chain retains full control over data availability, data privacy, user confidentiality, and accessibility. By tailoring its design, architecture, and functionality to align with the profound needs of enterprises and users, the Elastic Network is well-positioned to focus on two key areas: tokenization and permissioned blockchain environments for enterprises. With ZKsync leading the charge and major institutions like Deutsche Bank, Tradable, and the government of Buenos Aires building on the Elastic Network, the network has laid the foundation to support exponential growth, assuming strong demand for and adoption of ZK Chains in the future.

Roadmap 2025

ZKsync recently published their *2025 Roadmap: Turning Vision into Action*. Key objectives include:

1. **Simplify Developer Experience**
   - Bytecode EVM equivalence
   - LLVM tooling
   - VS Code debugger
2. **Enable Web2-Like UX**
   - Performance: 10,000 TPS @ $0.0001.
   - Security: Stage 1. Decentralized sequencing and proving.
   - UI: Powerful smart wallet SDK for web and mobile.
   - Privacy: Private validium.
3. **Interconnect Public and Private ZK Chains**
   - Native interop with fast cross-chain transfers and method calls

For readers interested in a deeper dive into what lies ahead, we encourage you to explore the full roadmap here.

Matter Labs

Founded in 2018, Matter Labs is the engineering team behind ZKsync Era, the ZK stack, and the Elastic Network. Backed by the Ethereum Foundation and top investors like a16z, Dragonfly Capital, and Hashed, Matter Labs holds the belief that ZK cryptography is the most viable technology to drive mainstream and institutional adoption of blockchains. Providing blockchain scaling and privacy with succinctly verifiable ZK computation, everything the team builds is open source.

Matter Labs

Alex Gluchowski, Co-Founder & CEO

Alex, Co-Founder and CEO of Matter Labs, has been with the firm since the very beginning leading the development of ZKsync and the ZK stack. He holds a master's degree in computer science from TU Berlin (2011), where he wrote his thesis on energy efficiency in mobile positioning systems.

Alex's entrepreneurial background includes founding PaulCamper, now Europe's largest RV-sharing marketplace, and Somuchmore GmbH, a holistic wellness platform, which he grew from 3 to 80 employees before being acquired by Rocket Internet. He also served as CTO at both companies.Prior to that, Alex was the CTO at ExpoGlobus and Head of Software Engineering at Clarity AG leading an engineering team of 20.

Anthony Rose, CTO

Anthony Rose joined Matter Labs in 2022 as Head of Engineering, quickly advancing to SVP of Technology in 2023 and CTO in 2024. After earning his master's degree from the University of Surrey in 2009, Anthony completed his PhD in Elementary Particle Physics at the University of Sussex in the UK.

He brings a wealth of experience from top-tier companies like SpaceX and Uber, where he held roles as Senior Software Engineering Manager and Data Science Manager, respectively.

Meghan Hughes, CMO

Working as the VP of Marketing for the Solana Foundation from 2022 until September 2024, Meghan was poached by Matter Labs to take on the role of CMO. Along with her extensive experience at the Solana Foundation, Meghan previously served as VP of Marketing at 6D.ai, which was acquired by Niantic in 2020. She continued at Niantic as Platform and Developer Marketing Lead before moving to Stripe, where she became the Head of Developer Marketing, leading PMM and developer marketing for Stripe Apps.