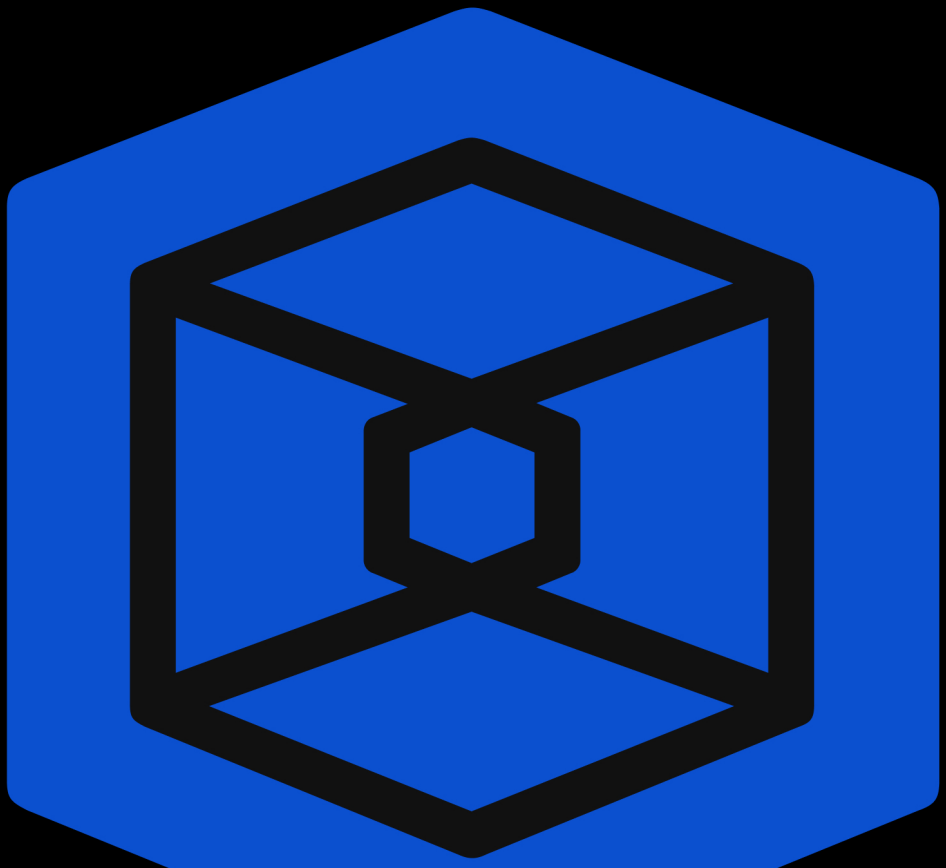
RESEARCH UNLOCKED

OCTOBER 2024



The Future of Tokenization

HOW ZKsync IS CHANGING THE GAME

RESEARCHED BY

THE BLOCK

IAN DEVENDORF, Author

QUICK TAKE

- **Tokenization is anticipated to reshape various industries, including finance, commodities, intellectual property, and real estate, by enabling more efficient, secure, and accessible markets, with a projected $16 trillion market by 2030 and endorsements from industry leaders like BlackRock's CEO Larry Fink.**

- **ZKsync's Elastic Chain offers a limitlessly scalable, multi-chain network that is well-suited to facilitating institutional-grade tokenization activities.**

- **By integrating customizable architecture, robust confidentiality measures, unified liquidity, and Ethereum-level security, the Elastic Chain's design supports the complex requirements of enterprises, enabling them to manage and scale their tokenization efforts across diverse asset classes while ensuring compliance and operational stability.**

TOKENIZATION

Tokenization is the process of converting rights to an asset into a digital token on a blockchain or other distributed ledger technology. This digital representation can symbolize ownership of real-world assets such as bonds, real estate, artwork, or commodities, as well as more abstract assets like voting rights or identity credentials. By digitizing these assets, tokenization creates new possibilities for fractional ownership, increased liquidity, and more efficient, transparent, and accessible transactions that can be executed quickly and securely across global markets.

1. **Growing Institutional Interest**: Major financial players are taking notice. According to a joint study by BNY Mellon and Celent, an overwhelming 97% of institutional investors agree that tokenization will revolutionize asset management.

2. **Massive Market Potential**: The market value for tokenized assets is projected to reach between $10 trillion and $16 trillion by 2030, according to estimates from Boston Consulting Group (BCG) and ADDX (2024).

3. **Endorsement from Financial Leaders**: BlackRock CEO Larry Fink, a prominent figure in the investment world, has described the recent approval of spot Bitcoin ETFs as merely "step one in the technological revolution in the financial markets." He further emphasized that "step two being the tokenization of every financial asset" is on the horizon.

4. **Application Beyond Finance**: While the financial sector stands to benefit greatly from tokenization, its applications extend far beyond. Tokenization is finding use cases in decentralized social platforms, loyalty programs, identity management and various other domains, demonstrating its versatility and wide-ranging impact.

Tokenization of real-world assets has already shown significant growth, as evidenced by figure 1. The graph below illustrates the dramatic increase in the total value of tokenized real-world assets which surged from near zero to over $11 billion in the five-year period ending July 2024. This upward trend underscores the growing adoption of tokenization and the increasing recognition of its benefits. The steep rise in value is anticipated to continue its momentum, fueled by a growing influx of institutional capital and increasing market confidence in the technology. Additionally, while financial assets have been particularly successful as tokenized products, the scope of tokenization is expected to expand across a broader range of asset classes.

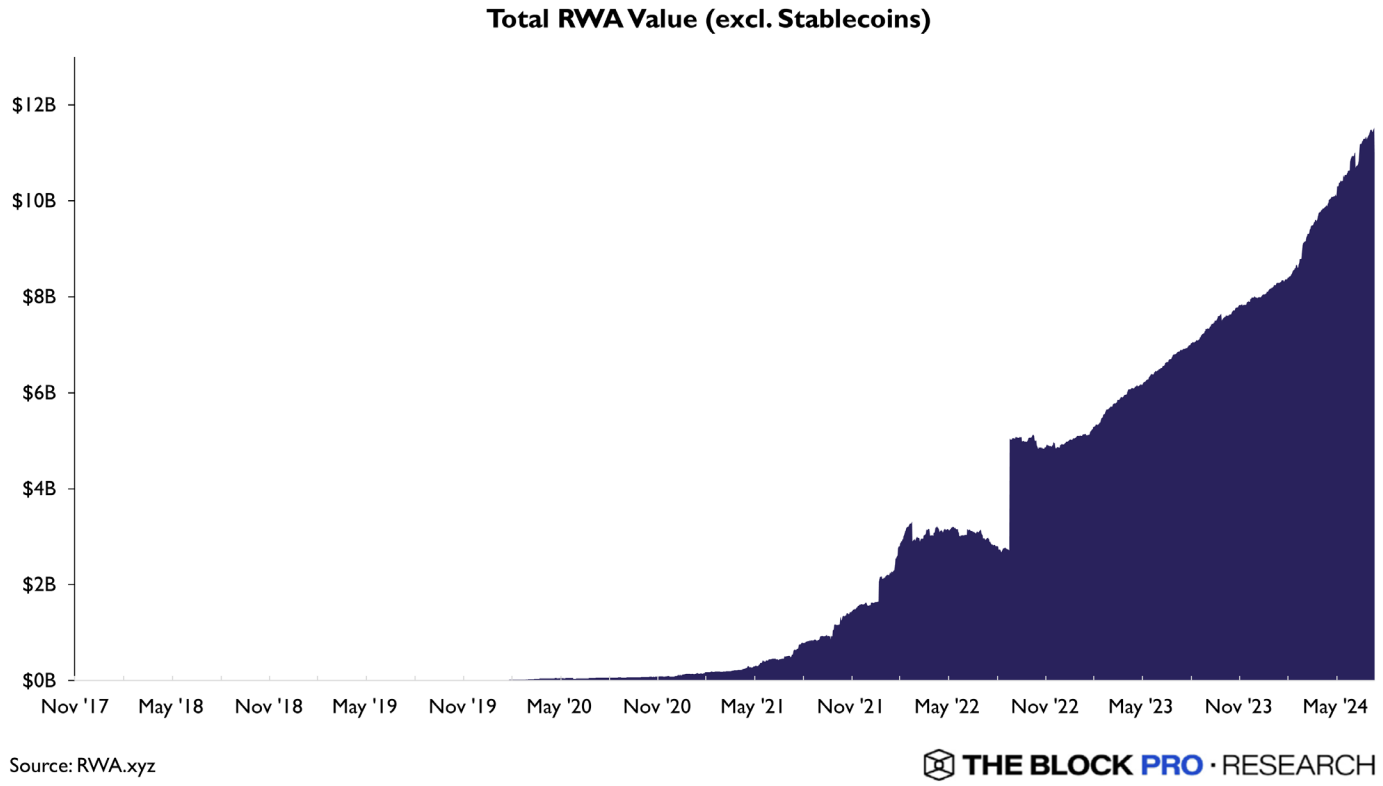


Figure 1: Total RWA value excluding stablecoins ($ in billions)

While tokenization has already gained traction, full on-chain issuance and value transfer has yet to surface in a material way. As the industry begins to recognize its potential benefits and becomes more comfortable with the technology, tokenization will likely progress to this more streamlined and secure model of asset management. Consider U.S Treasuries as an example. In the current model of tokenization, a digital token might represent ownership of a T-bill, but the underlying security remains in off-chain custody. With full on-chain issuance, the entire T-bill - from issuance to trading to redemption - would exist natively on a blockchain. This shift to full on-chain processes offers several advantages including:

- **Disintermediation**: By eliminating the need for custodians, clearinghouses, and other middlemen, costs decrease while security improves.

- **Minimized counterparty risk**: Direct peer-to-peer transactions on a transparent and immutable ledger reduce the need for hedging against counterparty default.

- **Increased efficiency**: Automated smart contracts can handle complex processes like interest payments and redemptions immediately without manual intervention.

- **Improved liquidity**: Easier transfer of ownership and robust interoperability can lead to more active secondary markets.

- **Real-time settlement**: Transactions can be settled almost instantaneously, reducing settlement risk.

ZK TECH

As tokenization expands across various sectors and asset classes, concerns around privacy, security, and scalability have come to the forefront. This is where zero-knowledge (ZK) technology enters the picture.

A Zero-Knowledge Proof (ZKP) is a cryptographic method that allows one party to prove to another that a statement is true without revealing any additional information beyond the validity of the statement itself. In this way, ZKPs ensure privacy and security by enabling verification without exposing sensitive data or underlying details. For example, ZKPs can be used to prove that a user has sufficient funds in a digital wallet without revealing the exact balance, confirm someone's identity without disclosing personal information like a name or address (QuarkID), or demonstrate that a party is over a certain age without revealing their exact birthdate or age, ensuring that only the necessary criteria are verified while keeping all other details private.

Zero-Knowledge Proofs have also been leveraged to help scale Ethereum Mainnet. ZKPs are used in Layer 2 scaling solutions, such as ZKsync, which bundle many transactions into a single proof that is then verified on the Ethereum Mainnet, as shown in Figure 2. This approach significantly reduces the amount of transactions that need to be processed on-chain, thereby increasing transaction throughput and reducing costs. By validating large batches of transactions with a single ZKP, ZK rollups maintain the security and decentralization of the Ethereum network while greatly improving its scalability.

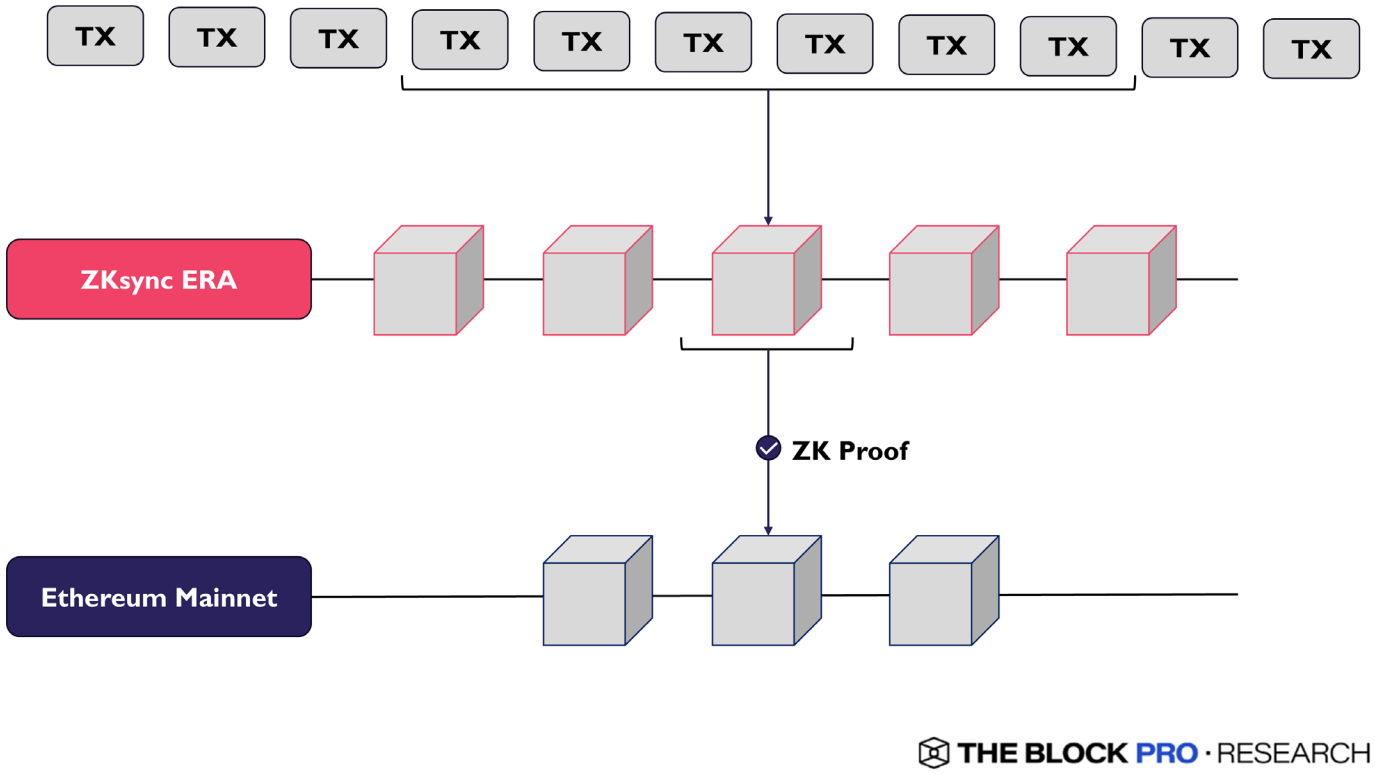


Figure 2: High-level schematic of a ZK rollup

Building on this concept, ZKsync created The Elastic Chain, an architecture designed to extend the capabilities of ZK rollups. The Elastic Chain is composed of interconnected ZK Chains that operate in parallel, that are secured by Ethereum, and can scale horizontally by adding new chains as demand grows. It can also enable enterprises, such as banks, to trustlessly communicate while maintaining confidentiality, as illustrated in Figure 3.

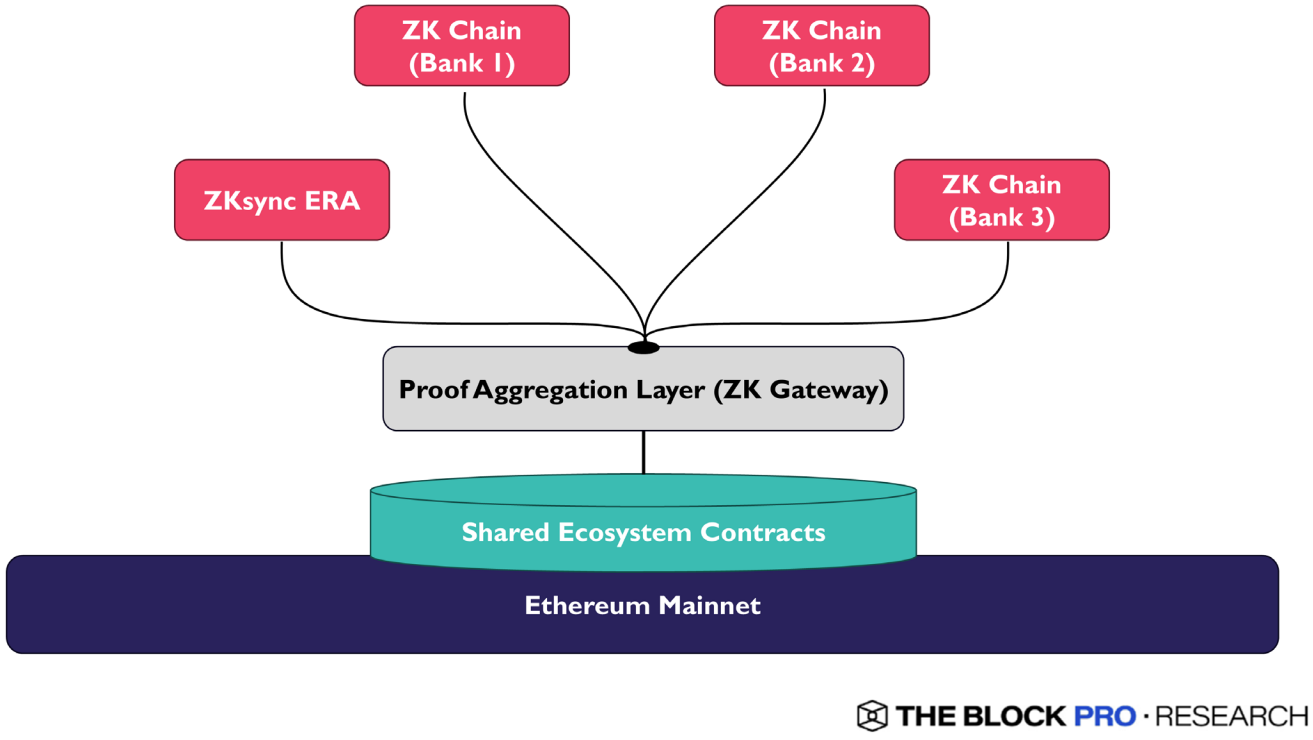


Figure 3: Diagram of The Elastic Chain's architecture

The Elastic Chain's design addresses many of the challenges associated with asset tokenization, enabling enterprises to capitalize on this technology and confidently transition to an entirely on-chain issuance and value transfer model.

- **Scalability**: Many enterprises require scalable infrastructure such as financial institutions that process massive amounts of transactions daily, ranging from small payments to large-scale asset transfers. For these institutions to adopt on-chain solutions, blockchain platforms must be capable of handling this transaction volume without incurring significant increases in latency or costs as network activity expands. The Elastic Chain achieves scalability by using a flexible architecture that

allows new ZK Chains to be added dynamically as demand increases. Each ZK Chain can operate in parallel, distributing the workload across multiple chains. This approach ensures that as more transactions are processed, the network can expand horizontally, maintaining optimal performance without bottlenecks or slowdowns.

- **Customization**: The ability to customize blockchain features is essential for enterprises because it allows them to tailor their tokenization strategies to precisely fit a specific use case. Different types of assets, whether they are securities, real estate, or commodities, have unique requirements in terms of issuance, trading, and settlement. Customization enables enterprises to meet these varied requirements, ensuring that the tokenization process is efficient, compliant, and secure. The Elastic Chain supports this need for flexibility through its modular ZK Chain design. ZK Stack, the modular development framework used to build ZK Chains, allows developers to select or implement custom blockchain components; this enables customization and flexibility while maintaining core standards for network security and interoperability. For example, enterprises can choose from various architecture elements, including chain type (Rollup, Validium), gas token (ETH, custom), EVM optimization (EVM equivalence (ready by end of 2024), performance), transaction sequencing (centralized, decentralized*), data availability (Ethereum, third-party, on-premises), data visibility (private, public), accessibility (permissionless, permissioned), number of nodes (one, n+*), and consensus mechanism (centralized, Proof of Authority*).

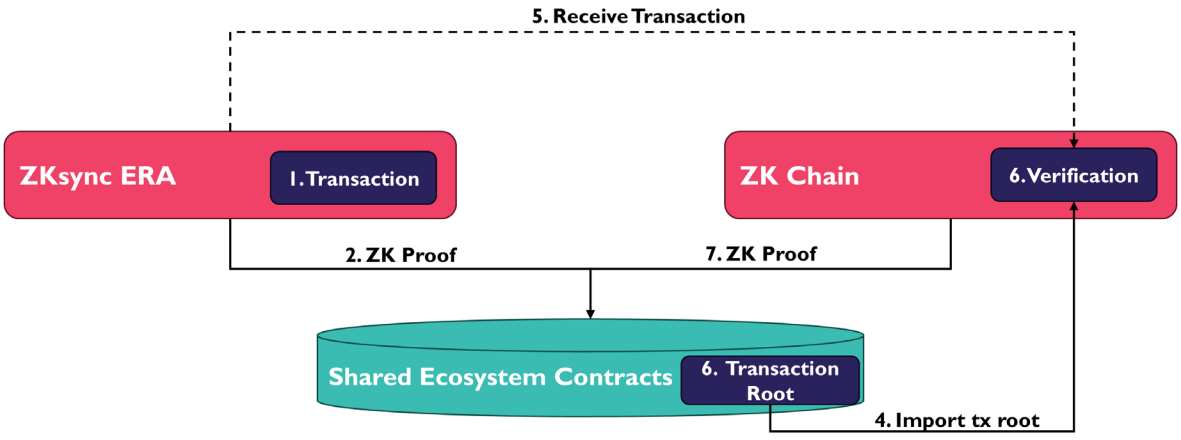
- **Confidentiality**: Confidentiality is important for enterprises, as it ensures the protection of sensitive data, maintains client trust, and supports compliance with regulatory requirements. Different use cases require varying levels of privacy; for example, sensitive corporate transactions may demand stricter confidentiality measures than more routine transactions. By tailoring privacy levels to specific needs, enterprises can prevent unauthorized access and data breaches, preserving the integrity of financial operations while meeting regulatory standards. Enterprises operating a ZK Chain can choose to keep transaction data off public networks, instead storing it on secure cloud servers, private infrastructure, or another third party data availability layer. This strategy allows for granular control over data visibility, with the ability to grant access to specific parties, such as regulators, when necessary. Additionally, ZK Chains post zero-knowledge proofs to Ethereum for verification, updating the chain's state without revealing participants' identities or transaction details. These proofs prevent unauthorized parties from accessing sensitive information.

- **Security**: A critical consideration for institutions adopting tokenization is the integrity and reliability of the underlying technology. The stakes of bringing real-world assets on-chain are exceptionally high, as a single breach could result in substantial financial losses, erosion of client trust, and severe regulatory consequences. The Elastic Chain enhances its security by anchoring to Ethereum and submitting zero-knowledge proofs to mainnet for validation. This means that to tamper with a transaction on the Elastic Chain, an attacker would need to compromise Ethereum's entire, highly secure network, which is protected by over 1 million validators. With ZK proofs linking it

* = features coming in 2025

to Ethereum, even a ZK Chain operating with a single node can ensure decentralized protection without needing its own large validator base. Additionally, ZKsync supports EVM-compatible source code which has been rigorously tested for vulnerabilities, allowing applications to be ported with minimal refactoring, thereby reducing the risk of bugs and exploits.

- **Interoperability**: Robust interoperability is crucial for an on-chain platform to support tokenization because it ensures that tokenized assets can move seamlessly across different networks, maximizing their liquidity, usability, and market reach. Financial institutions benefit from built-in interoperability standards, which reduce the need for middlemen and minimize continuous integration maintenance. In addition, stronger interoperability could unlock new use cases, such as intra-day repo agreements or real-time cross-border settlement. To operationalize this, ZK Chains can access a shared pool of users and liquidity by connecting through common ecosystem smart contracts on Ethereum mainnet and utilizing verifiable ZK proofs for trustless communication. The shared smart contracts are on Ethereum's Layer 1, where the original assets are locked. These smart contracts verify Merkle proofs of transactions occurring on other ZK Chains, ensuring that every cross-chain transaction is legitimate. This process is shown in Figure 4. By locking the asset in the shared ecosystem smart contracts, the system guarantees that the asset's value is preserved while allowing it to be represented and transferred across different chains within the network. Since all ZK Chains are powered by the same ZK ecosystem, each chain can verify ZK proofs submitted to the shared smart contract, enabling seamless interaction and unified liquidity. This native interoperability is expected to be in production by the end of 2024.



THE BLOCK PRO · RESEARCH

Figure 4: Schematic of a bridge that connects ZK Chains

As tokenization continues to gain momentum, scalable and flexible infrastructure is needed to support the diverse range of assets moving on-chain. The Elastic Chain emerges as a strong candidate for enterprises looking to engage in tokenization activities. A number of established financial institutions have already begun using ZKsync's technology to facilitate their shift towards on-chain finance.

- Tradeable, in collaboration with Victory Park Capital, is leveraging ZKsync technology to tokenize $500 million+ of private credit assets.

- Fidelity International, Sygnum, and Chainlink have partnered to tokenize $50 million of Fidelity's $6.9 billion money market fund on ZKsync Era.

- Deutsche Bank is developing an interoperable asset tokenization and fund management platform on a ZK Chain, in collaboration with Memento Blockchain

- The Buenos Aires government is rolling out a new decentralized digital identity protocol powered by QuarkID which anchors decentralized identifiers (DID's) on ZKsync Era. QuarkID is now officially Open-Source as well as officially recognized as a Digital Public Good (DPG) following the Sustainable Development Goals (SDG) from the United Nations. The solution will later migrate to its own ZK Chain for the enhanced confidentiality, security, scalability, and compliance benefits.

The ZK Stack's combination of customization, scalability, and interoperability positions the Elastic Chain as a comprehensive platform for institutional-grade tokenization. In particular, these features make it a catalyst for the transition towards fully on-chain issuance and value transfer. While the benefits of this new model of tokenization are clear, the three key blockers that challenge its broader adoption are lack of regulatory clarity, technological robustness, and enterprise readiness. The Elastic Chain's architecture directly addresses the lack of technological robustness by providing a scalable, customizable, secure, and interoperable platform. Additionally, the Elastic Chain can act as a bridge to advance enterprise readiness by offering a flexible environment that allows institutions to gradually adopt blockchain technology while maintaining compatibility with their existing systems and processes as they transition towards full blockchain integration. Finally, the Elastic Chain equips enterprises to adapt quickly to evolving regulations, enabling them to capitalize on regulatory clarity as it emerges.