GSR

January 2025

GSR Research

2025 Subsector Trends

www.gsr.io

Brian Rudick, Head of Research
Carlos Guzman, Research Analyst
Toe Bautista, Research Analyst

In a slightly different twist than a typical year-ahead report, we profile various crypto subsectors that we believe represent particularly large opportunities in 2025 and beyond.

Introduction

With the turn of the calendar, the cryptosphere is awash in year-ahead previews and predictions. Rather than offer more general thoughts on what may come, we present a slight twist, profiling six subsectors that we believe have particular promise for 2025 and beyond. Based rollups are one such subsector with the ability to solve Ethereum's state and liquidity fragmentation issues, enhance rollup security guarantees, and improve mainnet value capture. zkVMs are another, as they enable anyone to utilize zero knowledge proofs - already an incredibly powerful scaling and privacy paradigm - without requiring the immense time and expertise required to write lengthy custom arithmetic circuits. In a similar vein, trusted execution environments are increasingly being used within crypto to eschew the limitations of replicated execution and provide high compute use cases like AI with confidentiality, integrity, and verifiability. And rather than utilizing cryptography like zkVMs or hardware like TEEs, restaking extends trust beyond typical decentralized applications using economic incentives to ultimately unleash innovation. AI agents and frameworks are another gamechanging subsector that, while initially used to proliferate memecoins, are increasingly autonomous, with agentic agents perhaps one day the main user of blockchains. And lastly, Bitcoin L2s are on the verge of truly trustless scaling to unlock $2T of idle capital and leverage Bitcoin's leading security and decentralization. Finally, note that the digital assets industry is diverse and widely evolving, and as such, there are so many additional promising subsectors like fully homomorphic encryption, new execution environments, real world assets, decentralized physical infrastructure networks, and even memecoins, that we are unable to cover in a short preview. Nevertheless, we jump right into our subsector overviews.

Table of Contents

Based Rollups for a Unified Layer 2

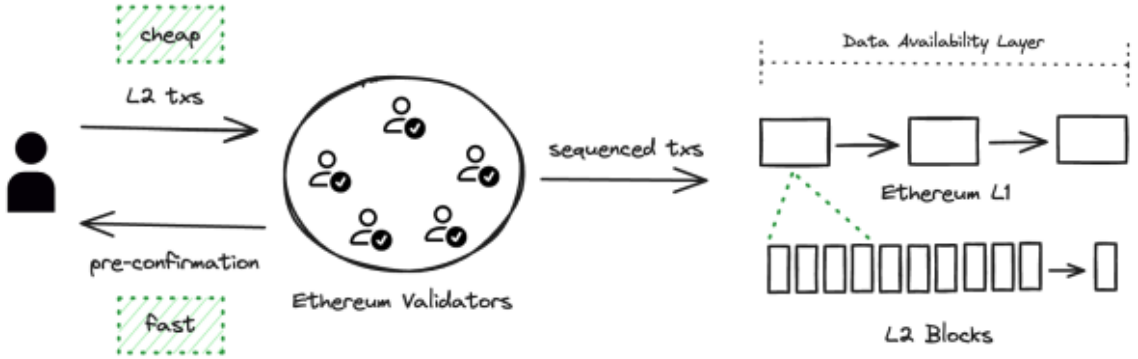
Conceived in 2013 by Vitalik Buterin and launched in mid-2015, Ethereum revolutionized blockchain technology and cryptocurrencies forever by enabling nodes to process general purpose code, known as smart contracts, to add programmability and arbitrary computation to the blockchain. While incredibly novel, Ethereum optimized for decentralization and security, a choice that has led to comparatively low throughput and periodic congestion/fee spikes during times of significant activity. To remedy this, Vitalik Buterin proposed his rollup-centric roadmap that executes transactions off-chain (ie. on rollups) before proving valid execution to Ethereum, thus pushing the bulk of the computational load off-chain. Such a setup significantly increases throughput as transaction validation is more efficient than re-executing the transactions themselves, and it further enables rollups to inherit many of the security properties of Ethereum mainnet itself. However, such a setup has also fragmented rollup state and liquidity.

First proposed by Justin Drake in early 2023, one solution that is gaining considerable momentum is based rollups and preconfirmations. Unlike typical rollups that rely on a single, centralized sequencer to choose which transactions are included in a block and in what order, based rollups use Ethereum mainnet validators to select and order transactions, essentially making Ethereum mainnet the shared sequencer for all based rollups and enabling atomic interoperability not only between the based rollup and mainnet, but also between the based rollups themselves. This, however, only solves part of the problem, as Ethereum's 12 second block time is incongruent with the shorter block times rollups aim to achieve. This is where preconfirmations come in, which allow an Ethereum validator to pledge ETH as a bond and promise to include an L2's transaction in the next Ethereum block, adding economic security behind based rollup transaction inclusion and creating a notion of finality that can be extremely fast, on the order of 100-200 milliseconds. And while based rollups do not order their own transactions and therefore lose the ability to extract MEV, there are reasons to believe their MEV opportunity will fall over time regardless. More importantly, based rollups inherit the liveness, censorship resistance, credible neutrality, and real-time settlement guarantees of Ethereum itself, and atomic composability should enable based rollups to garner more execution than would otherwise be the case.

Several teams are building based rollups or based rollup frameworks. While proofs of concept with limited functionality like Fuel v1 have existed for several years, Taiko arguably became the first fully programmable EVM-compatible based rollup when it launched on mainnet last year. They continue to iterate on their design and are working on Taiko Gwyneth, a booster rollup initiative to extend the concept of based rollups further. Spire is developing an open-source framework for deploying based rollups, which will hopefully enable many teams to easily deploy their own based rollups dedicated to their applications. The team at Rise is building a rollup that aims to achieve extreme high performance while benefiting from based sequencing. Nethermind is similarly building Surge as a high-performance based rollup. And Puffer and Espresso Systems are building infrastructure to support based rollups, enabling

pre-confirmations and block proposer auctions. On top of building infrastructure for based rollup pre-confirmations, Puffer is building its own based rollup called UniFi, which will leverage this infrastructure and dovetail with their broader suite of products that includes liquid restaking. We're excited to see the progress these teams make in 2025 toward enabling a unified Ethereum ecosystem.

Based Sequencing



Source: Puffer Finance, GSR.

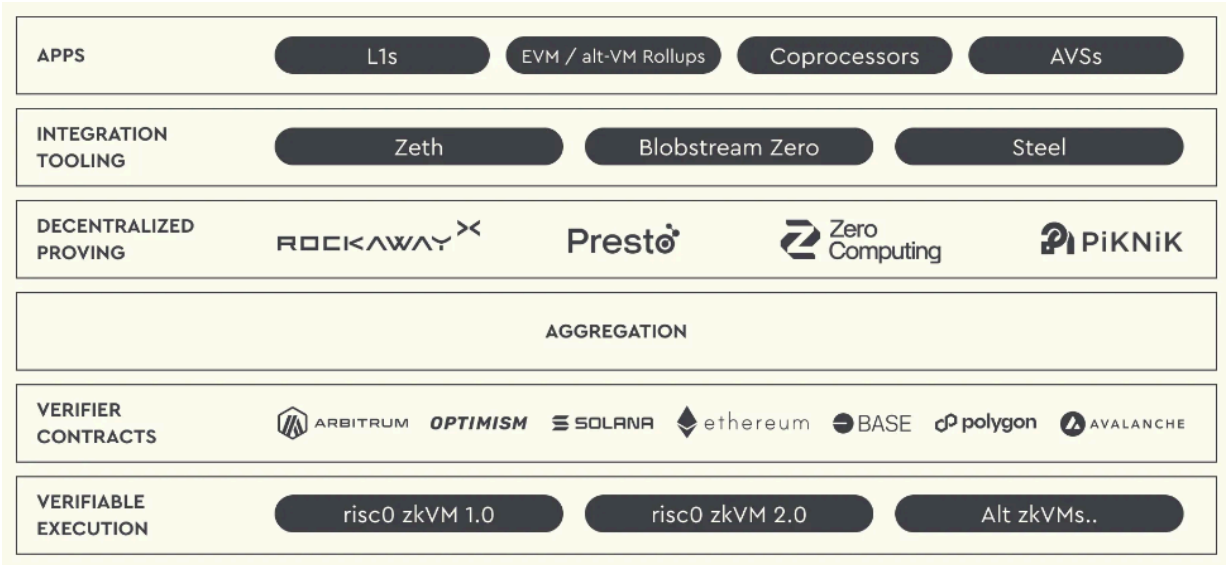
zkVMs: Bringing Zero Knowledge Proofs to All

With its main use cases in privacy and scaling, and applications ranging from finance to identity, compliance, governance, healthcare, gaming and more, zero knowledge proofs (ZKPs) allow for one to prove that a statement is true without revealing any other information. And while zero knowledge proofs have quickly moved from the theoretical to the practical, improving on key areas like prover time, proof size, verification time, and the trusted setup, the use of the technology has been out of reach for many given the immense time and expertise required to write lengthy custom arithmetic circuits in domain specific languages. However, zero knowledge virtual machines (zkVMs) have now progressed to allow developers to simply program in a high-level language like Rust and for the zkVM to prove the execution of the code, enabling a new paradigm in verifiable computation (technically, Rust code is compiled to RISC-V ISA bytecode and the zkVM proves the execution of RISC-V given the program and program inputs). Moreover, zkVM solutions like Risc Zero and Succinct are building decentralized prover networks so developers can outsource proof generation for low pricing/latency and high liveness/censorship resistance guarantees. And while the usage of zkVMs was historically inhibited by speed and cost considerations, zkVMs have improved immensely here to where zkVMs are now becoming the preferred zero knowledge solution for many/most use cases. As

one example, optimistic rollups can now convert to zero knowledge rollups using zkVM technology to benefit from faster withdrawals, lower trust assumptions, and greater interoperability, while zero knowledge rollups, currently in the form of zkEVMs that may be hundreds of thousands of lines of code that are difficult to audit or upgrade with Ethereum forks, can also utilize zkVMs to drastically enhance flexibility, auditability, and upgradability.

The zkVM space has grown quickly in the last couple of years with an increasing number of teams building competing products. RISC Zero pioneered the approach as the first team to productionize a RISC-V based zkVM. They've since used their zkVM to build solutions like their Bonsai proving service and a zk-provable Ethereum client called Zeth, and are now focused on Boundless, an integrated proving layer. The team at Succinct built their own open-source RISC-V zkVM called SP1, adding precompiles to enable further extensibility and performance. They've recently outlined a design for the Succinct Network, a decentralized prover network that will leverage SP1. Nexus is similarly building a prover network and a new version of their zkVM leveraging innovations from a16z's open-source Jolt zkVM and the Hypernova proof system. Taking a different approach, the Lita Foundation team have built their zkM, Valida, using a custom ISA different from RISC-V while still enabling developers to write in C or Rust leveraging the bespoke Valida compiler toolchain. Lita believes that this will result in significant performance gains for Valida compared to other zkVMs. Most recently, Axiom announced that they were building a new zkVM in collaboration with Scroll called OpenVM, with the goal of building a highly performant, extensible and maintainable open-source zkVM. Verifiable compute has been a core ingredient enabling crypto's trustlessness, we're excited to see zkVMs scale verifiable compute further in 2025.

Risc Zero's Boundless Zero Knowledge Stack



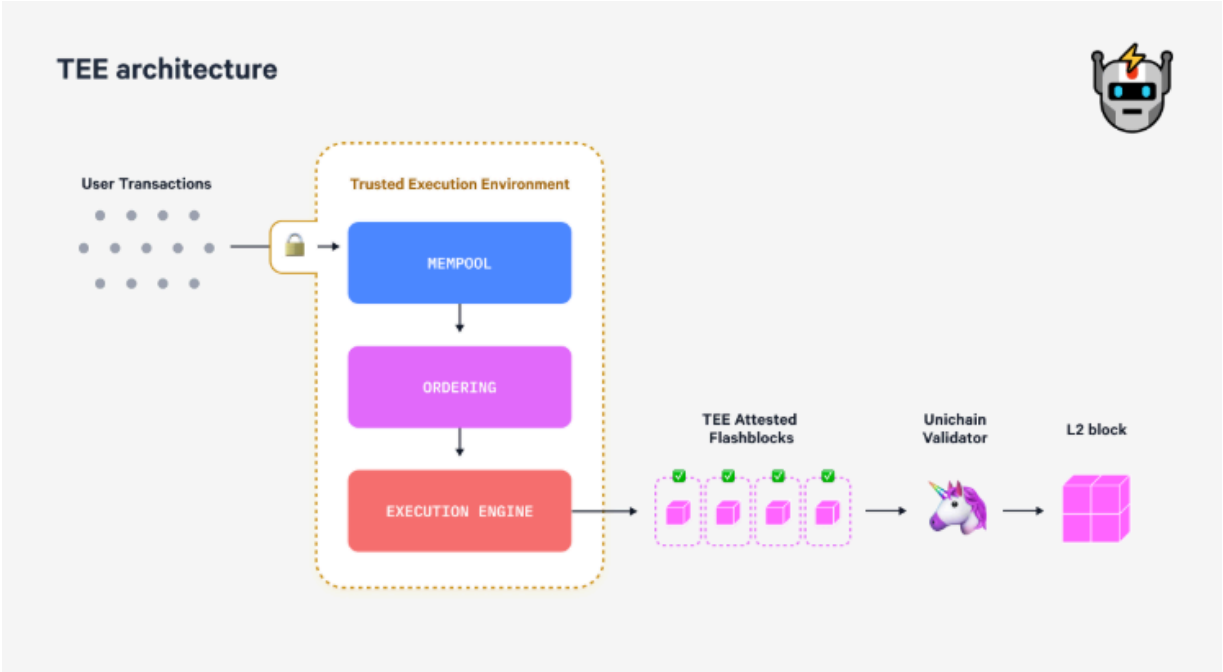
Source: Risc Zero, GSR.

TEEs

Blockchains establish trust between unknown participants and without a central leader by leveraging cryptography, economic incentives, and permissionless verification. However, blockchain's use of replicated execution is often infeasible for high compute / high speed use cases. Enter Trusted Execution Environments (TEEs), which are environments for executing code in a secure area of a processor and bring confidentiality, integrity, and verifiability to the computation by preventing unauthorized entities from outside the TEE from reading data or replacing/modifying code within the TEE and by providing attestations of the computing results. TEEs rely on trusted hardware to secure and authenticate computation, enforced through strict access control policies. They are accessible and cost-effective, and are thus widely used across mobile phones, servers, PCs, and cloud environments. And within a blockchain context, TEEs can be used as coprocessors to scale existing applications by replacing onchain logic with provable, low-cost, off-chain execution for high performance computing applications like AI. And they enable applications to trustlessly interact with Web2, store private data, and execute confidential programs.

The use of TEEs within crypto continues to increase, with notable examples including trustless MEV solutions from Flashbots and Unichain, as well as onchain AI and DePIN verification. In more detail, Flashbots uses TEEs to address Maximal Extractable Value (MEV) on Ethereum, ensuring fair and secure MEV auctions and block construction processes. Unichain plans to leverage this through verifiable ordering of transactions that enables MEV to be internalized and captured for LPs. In addition, Automata Network integrates TEEs to provide a modular attestation layer that extends machine trust to Ethereum, utilizing TEE coprocessors for secure and private computation. Furthermore, Phala's TEE-based framework enhances a wide spectrum of applications reliant on attestation, with Phala Network utilizing Intel SGX to enable secure, verifiable off-chain computations that can integrate with blockchain smart contracts. Oasis Network employs TEEs for confidential smart contract execution, allowing developers to create dApps where sensitive data processing is kept private. Fireblocks uses TEEs, specifically Intel SGX, to secure API keys and other sensitive data, ensuring that even in the case of server compromise, cryptographic materials remain safe. Secret Network applies TEEs to execute smart contracts privately, protecting transaction details and computational outcomes from public view. Lastly, by leveraging ai16z (ElizaOS), anyone can build an autonomous ICO (aICO) that integrates with Eliza's multi-agent framework to manage token issuance, allocate funds, and autonomously engage with the community. With the integration of Phala's TEE plugin, every action—from token allocation to governance voting—is cryptographically secured and verifiable, ensuring that the aICO is entirely trustless, community-driven, and protected from human errors or interference. We believe the composability, customization, and security of TEEs unlock a wide range of use cases, and that TEEs will see increased usage across a myriad of crypto sectors in 2025 and beyond.

Flashblocks' TEE Architecture for Unichain



Source: Flashbots, GSR.

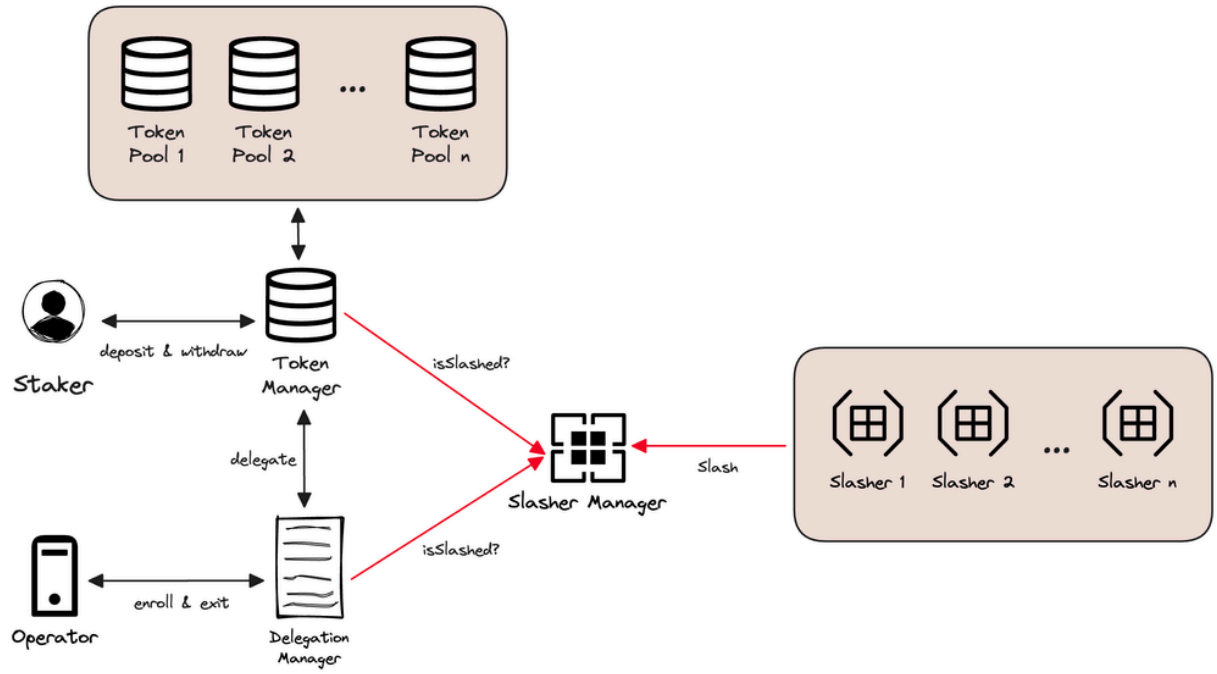
Restaking for Verifiable SaaS

Restaking protocols can be thought of as marketplaces for decentralized trust, or perhaps more concretely security-as-a-service protocols, and the paradigm is, in our opinion, one of the biggest innovations in blockchain technology in some time. Ethereum, for example, provides a narrow scope of decentralized trust, where validators stake ETH to determine the canonical chain and validity of blocks, meaning that Ethereum provides economic security for its decentralized applications, but not beyond. Restaking protocols, however, expand Ethereum's trust layer by enabling native ETH stakers, LST holders, and (sometimes) any ERC-20 to restake their tokens to secure bridges, oracles, sidechains, and many more. Such applications, known as Actively Validated Services or AVSs in Eigenlayer parlance, simply rent security from restakers, alleviating the need to otherwise bootstrap their own validator set and offer high inflationary rewards, while restakers receive additional yield in exchange for taking on increased slashing conditions. And, this is all made possible by (node) operators, who accept staked ETH that is delegated to them (or use their own stake) and run the AVS software modules that perform the validation services for the AVSs. Now, anyone can build new blockchain services beyond simple dapps without having to worry about procuring more traditional blockchain

security, allowing developers to focus on the product or service at hand and ultimately unlocking a flurry of innovation.

While the concept of restaking originated with Eigenlayer, several other restaking projects have sprung up with different approaches. Symbiotic likewise enables decentralized networks to rent security from Ethereum, but aims to take a modular approach, giving stakers, operators and networks wider latitude in defining their security agreements. Karak takes a similar approach to Symbiotic, though they've further expanded the set of assets the protocol allows for staking and are taking a chain-agnostic approach. Restaking is also expanding beyond the Ethereum ecosystem. Solayer is building a Solana-native restaking protocol along with the InfiniSVM, a blockchain aiming to scale Solana while leveraging Solayer's security. Jito has likewise built a restaking solution on Solana to complement its existing liquid staking service. And the ideas behind restaking have even made their way to Bitcoin with Babylon, with its innovative use of remote staking via EOTS, timestamping, and others, to enable Bitcoin to be staked to secure proof of stake networks, allowing them to rent economic security from Bitcoin and providing Bitcoin holders with a new source of yield for their assets. We look forward to seeing how restaking enables new types of trust-minimized services and ultimately applications in 2025.

Simplified EigenLayer Architecture



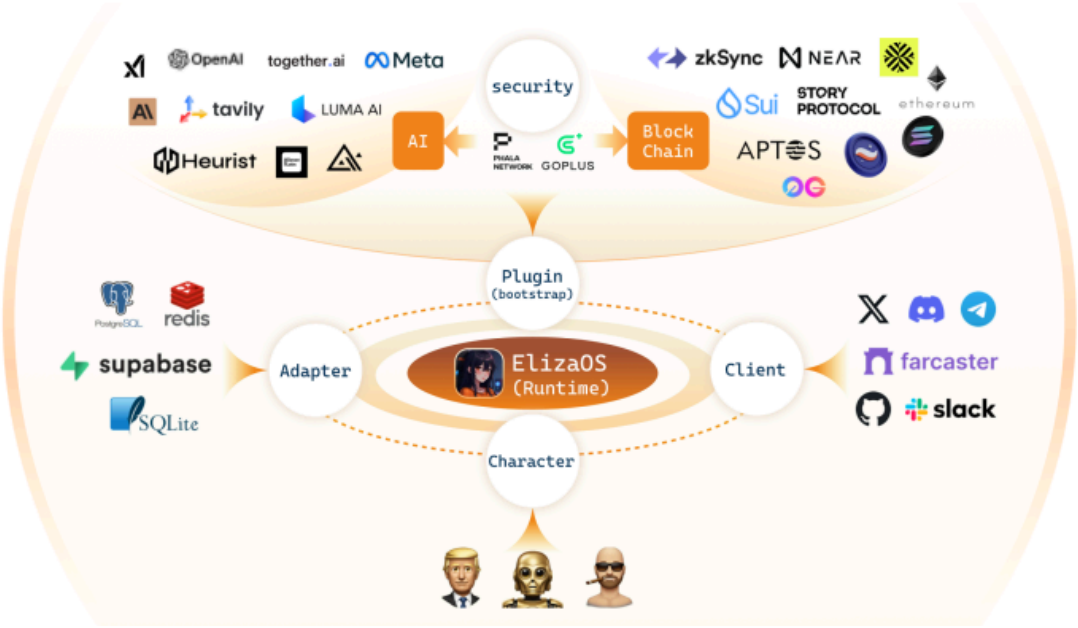
Source: EigenLayer, GSR.

AI Agents

With the TAM seemingly growing every day - Nvidia CEO Jensen Huang recently called agentic AI a multi-trillion dollar opportunity - the buzz around crypto AI agents continues to intensify. The term AI agent refers to AI systems that can autonomously act in a goal-directed manner by reasoning and executing tasks in pursuit of their objectives. AI agents caused a buzz in 2023 with systems like AutoGPT and BabyAGI, and with frameworks like Langchain, implementing agentic systems based on LLMs. Since then, there's been growing experimentation and interest in AI agents within crypto, with the thought that crypto provides the most natural financial rails for agents to transact. This potential captured the imagination of many with Terminal of Truths and its associated GOAT memecoin. Though Terminal of Truths is not itself autonomous and operates through its creator, it gave the impression that it was pursuing its own evangelizing goals and utilizing crypto to achieve them. This woke many up to the promise of a digital economy of AI agents using crypto, with many speculators latching on to the potential opportunities of having autonomous agents promoting their memecoins on social media.

Several AI agent platforms have risen to prominence in recent months. These platforms enable developers to create AI agents and/or provide launchpads for AI agent-related tokens. For example, Virtuals is a platform that provides both: the team behind it is working on a framework called G.A.M.E. to allow developers to create custom-built agents, and they've launched a pump.fun-style interface to enable anyone to launch an agent with an associated token on Base. Over seven thousand agents with tokens were launched using Virtuals in November alone. In addition, Eliza is another popular open-source framework for developing AI agents that can interact through various forms of social media. Eliza is built by the team at ai16z, a DAO that aims to surpass a16z's investment success through the use of AI agents. The ai16z team has launched AI agents that post on Twitter and have drawn engagement similar to Terminal of Truths, including with Marc AIndreessen and degenspartanAI. Of note, Virtuals has similarly been used to launch AI agents that have become popular on social media, including Luna which generates TikTok style influencer content, and aixbt which provides commentary about crypto. Lastly, the subsector features the emergence of DeFAI, which in its early stages allows users to interact with DeFi through LLM interfaces. For example, Wayfinder introduces a unique agent framework model that encodes skills and smart contracts as nodes into a 'hierarchy of agents', that offers scalability of tasks and actions such as executing swaps, monitoring prices, writing smart contracts, or creating social agents similar to Truth Terminal or aixbt.

ElizaOS AI Agent Framework



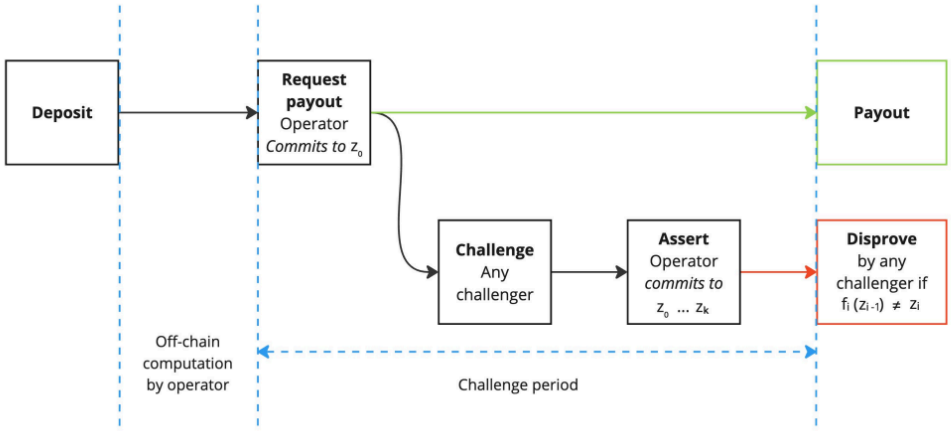
Source: eliza.os, GSR.

BTC L2s

Bitcoin reached a $2T market cap for the first time in 2024 and looks poised to further cement itself among the world's most valuable assets in 2025 with a more crypto-friendly regulatory landscape and increasing institutional adoption. Unfortunately, Bitcoin holders do not have a way of making their Bitcoin capital productive while still preserving the unparalleled security that the Bitcoin blockchain provides, or as close to it as possible. Bitcoin L2s promise to change that by adding programmability and scaling Bitcoin's throughput while utilizing cryptographic and/or cryptoeconomic mechanisms to minimize added trust assumptions. 2024 witnessed significant advancements in the tech needed for trust-minimized Bitcoin L2s, with multiple teams pushing Turing complete computation via BitVM forward and many making progress towards safe and practical bridge designs. Several of these designs are expected to reach mainnet in 2025, marking a turning point in Bitcoin scaling and programmability. Bitcoin L2s will unlock an array of new trust-minimized applications for Bitcoin including DeFi, native stablecoins, payments, privacy, NFTs, games, and more, and we expect a Cambrian explosion of experimentation and new applications on Bitcoin with the advent of L2s. The excitement around these new possibilities has even started to spread among Bitcoin's famously technologically conservative community, with some voices within the community starting to call for Layer 1 upgrades that could make Bitcoin L2s easier to implement like bringing back Bitcoin's scrapped opcode OP_CAT, among other potential upgrades.

Numerous teams are working towards launching BTC L2s. Some notable ones include the team at Alpen Labs who are building Strata. The team's research efforts have helped push the overall Bitcoin L2 ecosystem forward including their recent proposed design for the Strata bridge, which draws inspiration from bridge designs outlined in the BitVM2 paper. Citrea has similarly sought to improve upon state of the art BTC L2 bridge designs and has helped contribute research to the broader space as part of the BitVM Alliance. Their Clementine bridge design similarly builds upon BitVM2 and they've innovated on their zk-prover design to adapt to Bitcoin's computationally and data constrained environment. Along the same lines the team at BOB, which collaborated in writing the BitVM2 paper, are among the leaders in making trust-minimized BitVM-based bridging possible. Their L2 design is further notable in that it is simultaneously an L2 for Ethereum and Bitcoin – it is starting out as a OP Stack rollup on Ethereum and will progressively add settlement capabilities on Bitcoin as the requisite technology matures. Another project bringing unique innovations to the BTC L2 space is Bitlayer, whose OP-DLC bridge design cleverly combines Discreet Log Contracts with BitVM to address potential bridge liquidity issues. While much attention has been dedicated to Bitcoin rollups, several teams have been innovating in the Bitcoin sidechain space. Projects like Mezo and Botanix are implementing innovative bridge designs based on threshold signatures, providing an alternative to rollups' BitVM bridges, which while highly promising nonetheless come with some technical risk given their novelty. Beyond teams building Bitcoin L2s, there are other projects building enabling infrastructure like Nubit, which is building a dedicated Bitcoin data availability solution and along with other tools. Overall, 2025 is shaping up to be a historic year for Bitcoin L2 development and we look forward to seeing the progress all of these teams make.

BitVM2 Bridge Withdrawal Challenge Process



Source: BitVM2 whitepaper, GSR.

About GSR

GSR has over a decade of extensive experience in the crypto market, serving as a trusted liquidity provider and active, multi-stage investor. Our suite of services includes OTC Trading, Derivatives, and Market Making. GSR is actively involved in every major sector of the digital asset ecosystem, working with token issuers, institutional investors, miners, and leading trading venues.

Find out more at www.gsr.io.

Follow GSR for more content: Twitter | Telegram | LinkedIn

Required Disclosures