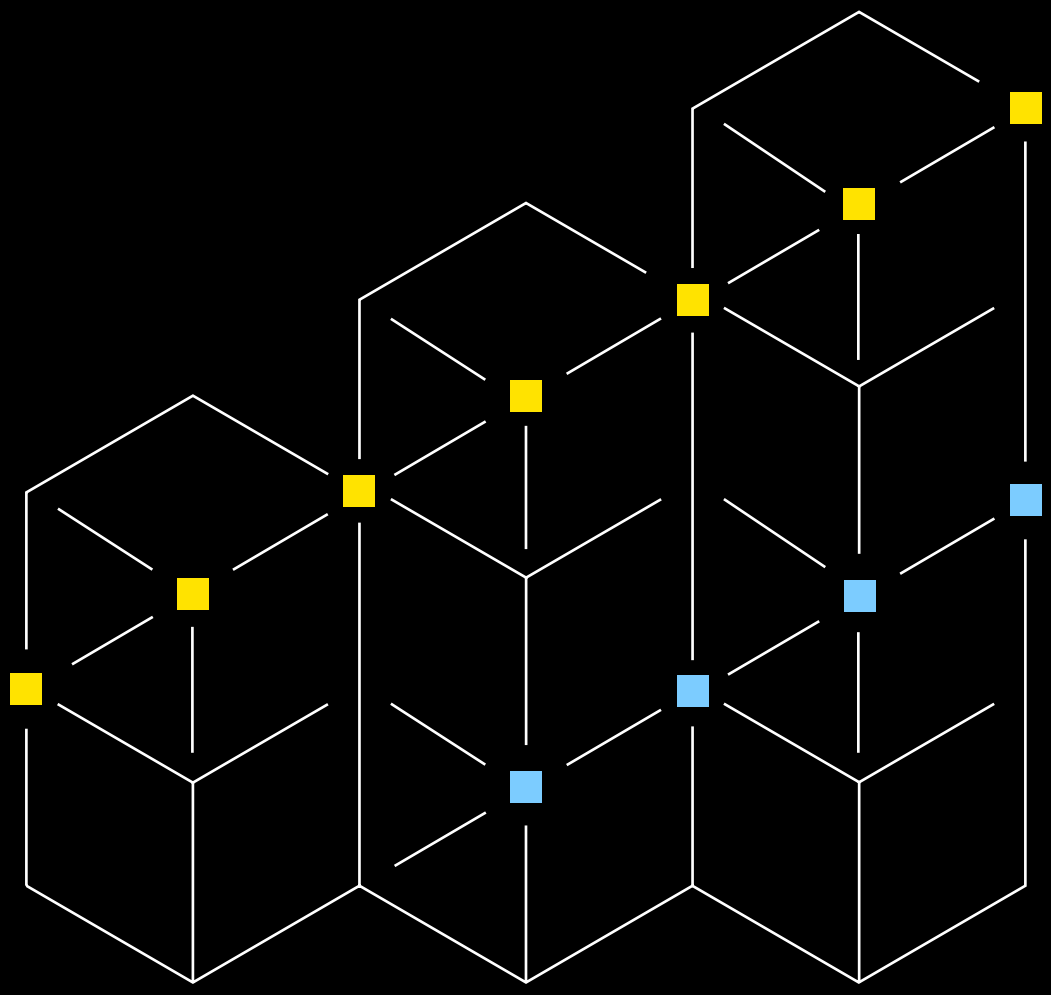
galaxy

Galaxy Research

The Costs and Benefits of Restaking

JULY 15, 2024



Author & Acknowledgements

Zack Pokorny
Research Analyst

This report is a product of Galaxy Research, a research organization within Galaxy, the leading provider of financial services in the digital assets, cryptocurrency, and blockchain technology sector. Galaxy Research provides top-tier market commentary, thematic views, tactical insights, and deep protocol research.

This report was written July 2024.

View our publicly available research at www.galaxy.com/research. Contact us at research@galaxy.com.

Contents

Summary

This report is the second in a three-part series diving into the risks and rewards of staking, restaking, and liquid restaking. The first report offers a comprehensive overview of staking, how it works on Ethereum and important considerations for stakeholders when engaging in this activity. This report offers an overview of restaking, how it works on Ethereum and Cosmos, and important risks associated with it.

Introduction

The industry's experimentation with scaling blockchains through modularity has led to the creation of many new protocols and supporting middleware. However, the need for each of these networks to spin up their own security moat, usually through a variation of proof-of-stake (PoS) consensus, is both a resource and time intensive process that has led to many isolated security pools.

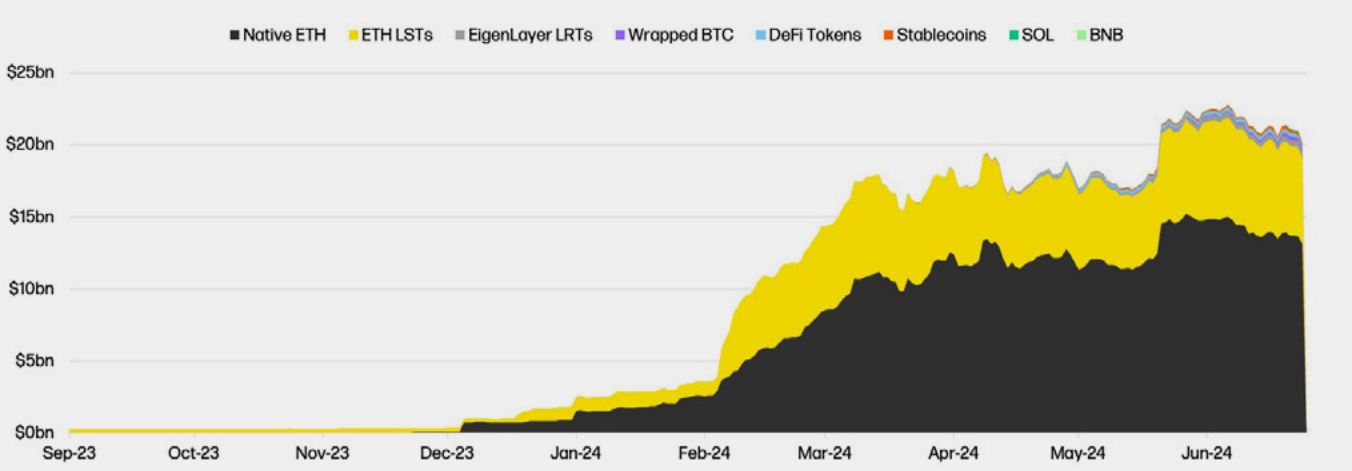
Restaking is the use of one blockchain's economic and computational resources to secure multiple blockchains. In the case of PoS blockchains, restaking allows the stake weight and validator set of one chain to be used across any number of other chains. The result is a more unified and efficient security blanket that can be shared by multiple blockchain ecosystems.

Though it wasn't always referred to as "restaking," the concept has a long history. The Polkadot ecosystem experimented with the idea as early as 2020. Cosmos launched a version of restaking called replicated security in May 2023; and Ethereum via EigenLayer in June 2023. Most of the value in restaking protocols are from stake locked on Ethereum. Ethereum is the most *economically* secure PoS blockchain by total value staked with more than $100 billion in staked ETH across one million plus validators (the term "validators" is not to be confused with validating nodes as the two are not synonymous in the context of the Ethereum ecosystem). "Economically" is italicized to highlight that there is a distinction between a chain's economic security and its overall insulation from attack or manipulation. A chain's level of economic security is not always indicative of how holistically secure the chain is.

As of June 25, 2024, there is $20.14 billion worth of assets being restaked. Ethereum is by far the largest protocol supporting restaking, with ETH and its derivative assets capturing $19.4 billion in restaked deposits, $18.3 billion of which were deposited by users in 2024. Notably, $58.5 million is restaked on Solana via Picasso and Solayer, and $223.3 million of wrapped BTC via Pell Network and Karak across a variety of chains, including Bitlayer, Merlin, BSC, and others. The following is a chart of the total value of restaked assets by type across the leading restaking solutions by total value locked (EigenLayer, Karak, Symbiotic, Solayer, Picasso, and Pell Network).

Total Value of Restaked Assets by Type

Source: Galaxy Research



Includes: EigenLayer, Symbiotic, Karak (All Chains), Pell Network (All Chains), Picasso (Solana), and Solayer
Data: Dune (glxyresearch), DeFiLlama

An estimated $1.7 billion is also restaked through Cosmos Hub validators and their model for restaking called replicated security.

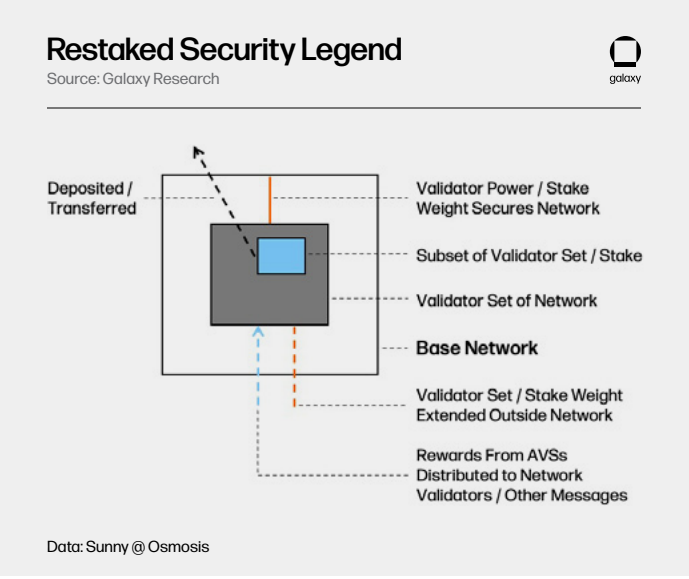
While the benefits of restaking for progressing the thesis of modularity and unifying economic security are clear, there are risks in implementation that should not be overlooked. This report offers an overview of the major restaking solutions built atop the Ethereum and Cosmos ecosystems. It will not dive into the risks presented by products built atop restaking protocols such as liquid restaking. This will be the primary focus of the next report in this series.

Important Definitions and Models

The following is a list of terms and their definitions that will be used repeatedly in this report:

- **Slashing** – the penalty given to validators who fail to do their job correctly or accurately. In addition to losing a portion of their stake, validators can also be jailed (temporarily removed from the active set of validators) or tombstoned (permanently removed from the active set of validators) as supplementary, non-economic penalties.
- **Slashing condition** – the basis on which validators are penalized (slashed). This can include double signing, downtime, or other malpractices unique to a given network.
- **Liquid Staking Token (LST)** – liquid fungible tokens that represent illiquid assets deposited by a chain's validators.
- **Liquid Restaking Token (LRT)** – liquid fungible tokens that represent illiquid ETH, LSTs, and other assets used as restaking collateral.
- **Node operator** – entities that run nodes and provide other services to actively validated services. The term encompasses EigenLayer node operators and Cosmos Hub validators engaged in replicated security throughout the report.
- **Actively Validated Service (AVS)** – any platform that relies on restaked resources for security. Actively Validated Services is abbreviated as AVS' throughout this report. The term encompasses EigenLayer AVS' and Cosmos consumer chains throughout the report.
- **Economic security** – the dollar denominated value of the assets staked by the validators of a network.
- **Computational security** – the hardware and software needed to validate a network.
- **Base Network** – the network whose staking assets and/or validator set are being used to economically and computationally secure AVS', also referred to as the "base protocol" or "base chain". The term can be applied in the context of both the Cosmos Hub and Ethereum.

The legend below is a key used to understand the profiles of some of the restaking models covered in the report. It is based off a keynote delivered by Sunny Aggarwal at the 2023 Shared Security Summit.



Restaking on Ethereum

EigenLayer is a set of smart contracts on Ethereum that enable restaking of assets to secure external services called AVS' (actively validated services). Smart contracts dictate the details of the relationship between node operators and EigenLayer AVS'. These details include components such as slashing penalties, rewards payouts, AVS registrations, and validator exits. AVS' do not inherit security from EigenLayer itself. EigenLayer smart contracts function as the middleware technology connecting AVS' to Ethereum validators and node operators and their underlying staked assets.

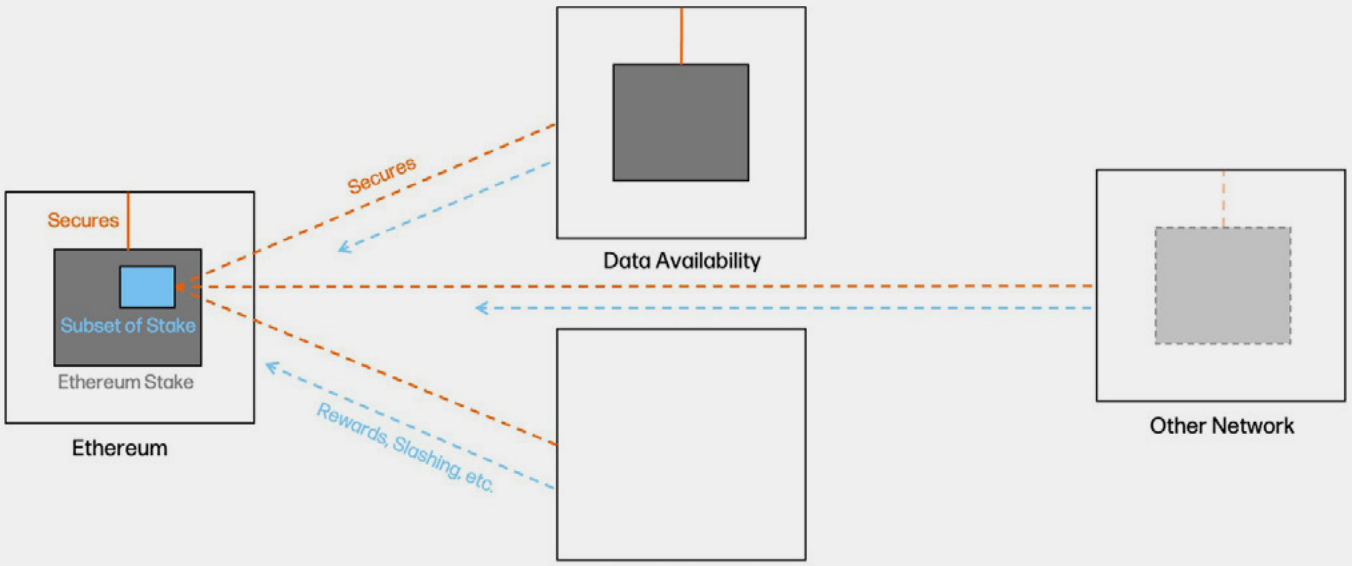
The graphic below offers a high-level overview of how EigenLayer restaking works. Note that EigenLayer is an opt-in system. Not all Ethereum validators, also called Beacon Chain validators, are required to be EigenLayer node operators and vice versa; Beacon Chain validators opting in to EigenLayer can point their withdrawal credentials to EigenLayer enabling AVS' to slash their stake and pay them rewards, while also being subject to the responsibilities of being a Beacon Chain validator.

EigenLayer enables a subset of Ethereum stake, which can be natively staked ETH in Beacon Chain validators or LSTs, to be leased by AVS', that may or may not have their own validator set and staking asset. In return, the leased subset of Ethereum stake earns rewards from each AVS for subjecting itself to additional slashing conditions. They are supplementary to Beacon Chain rewards earned directly by Beacon Chain validators or accrued through LSTs. A single unit of ETH or LST can be leased by any number of AVS'. However, each AVS adds additional slashing conditions to that unit of value.

At time of writing, EigenLayer is in an early phase of development and does not enforce any slashing conditions or restaking rewards. In theory, EigenLayer functions as an open marketplace where AVS' can freely purchase economic security from a subset of Ethereum validators and where Ethereum users and node operators can choose the AVS' they are willing to secure with their staked assets. This is a characteristic of EigenLayer that other comparable interchain-staking solutions, namely replicated security, do not have. It is a market driven approach that allows the equilibrium between supply and demand for restaked ETH to be found with less friction, though airdrop farming might skew it today.

EigenLayer Restaking Security Model

Source: Galaxy Research



Data: Sunny @ Osmosis

Restaking on Cosmos

Cosmos' replicated security is enabled by the Cross-Chain Validation (CCV) module which exists at the application layer of the Cosmos protocol tech stack. Replicated security is enabled by in-protocol infrastructure of the Cosmos Hub and consumer chains, instead of by applications that exist on top of the chains themselves. Replicated security relies on light clients, lightweight versions of client software that can run on resource-constrained devices, for the Cosmos Hub and consumer chains. It also relies on the Inter-blockchain Communication (IBC) protocol to transmit messages about Cosmos Hub validators, their stake, and the rewards they earn from securing a consumer chain.

Under replicated security, *almost* all Cosmos Hub validators and their stake (top 95% by voting power) must secure consumer chains that are passed through governance, even if they don't vote in favor of onboarding a consumer chain in the process (hence the name "replicated security"). The Cosmos Hub's validator set, and stake weight are effectively copied across all consumer chains. This is unlike EigenLayer's approach where restakers, node operators, and Beacon Chain validators voluntarily decide to restake to AVS' of their choice. If ATOM stakers do not wish to subject their assets to consumer chain slashing, they can redelegate their stake to validators outside the top 95% that may not secure consumer chains. However, doing so comes with tradeoffs that can result in lower ATOM staking rewards for the delegator, among other risks. As of June 25, 2024, there are 113 of 180 validators in the Cosmos Hub's active set that fall under the 95% threshold.

The graphic below offers a high-level overview of how replicated security works; note that it looks like that of EigenLayer, with the exception that the entire ATOM stake (less 5% red block) secures consumer chains and that consumer chains do not hold their own sovereign validator sets in any circumstance (Cosmos Hub validators stand in their place). Stride, a Cosmos consumer chain, uses "governors", which are validators that accept STRD stake to vote on governance. However, these governors do not build blocks or validate transactions on the network.

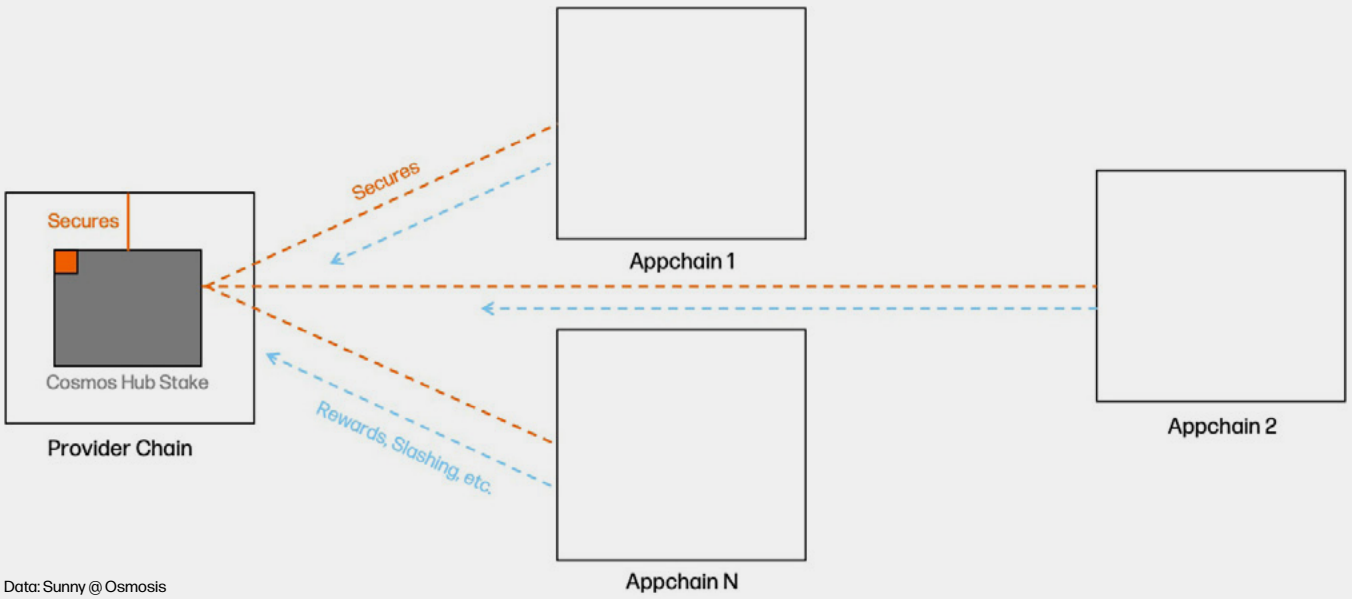
It's important to note that Cosmos Hub validators run separate software, and in some cases separate hardware, to secure consumer chains with their ATOM stake. Consumer chain transactions are not executed on the Cosmos Hub and do not occupy Cosmos Hub block space despite almost every Cosmos Hub validator securing each consumer chain; the block space of the base chain and each consumer chain are mutually exclusive.

Partial set security (more info and proposal vote) was introduced as a part of the Gaia upgrade allowing subsets of ATOM stake to secure consumer chains. Partial set security is more akin to the EigenLayer model in that Hub validators have the choice of securing consumer chains; and consumer chains can outline minimum amounts of stake needed to secure their chain. Partial set security will be reliant on governance in the first iteration before adding permissionless consumer chain launches. As of June 25, 2024, no Cosmos chains have launched under partial set security.

Additionally, a proposal introducing security aggregation to the Hub, starting with BTC, was published in early May 2024. If passed, this would allow Hub validators to receive BTC delegations via Babylon to safeguard the Hub and its consumer chains, and pave way for any on-chain asset to be used as economic security through Hub validators.

Cosmos Replicated Security Model

Source: Galaxy Research

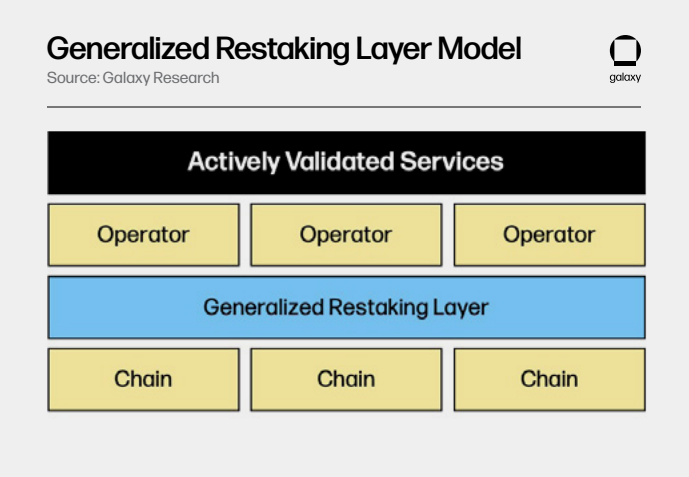


Data: Sunny @ Osmosis

Generalized Restaking Protocols

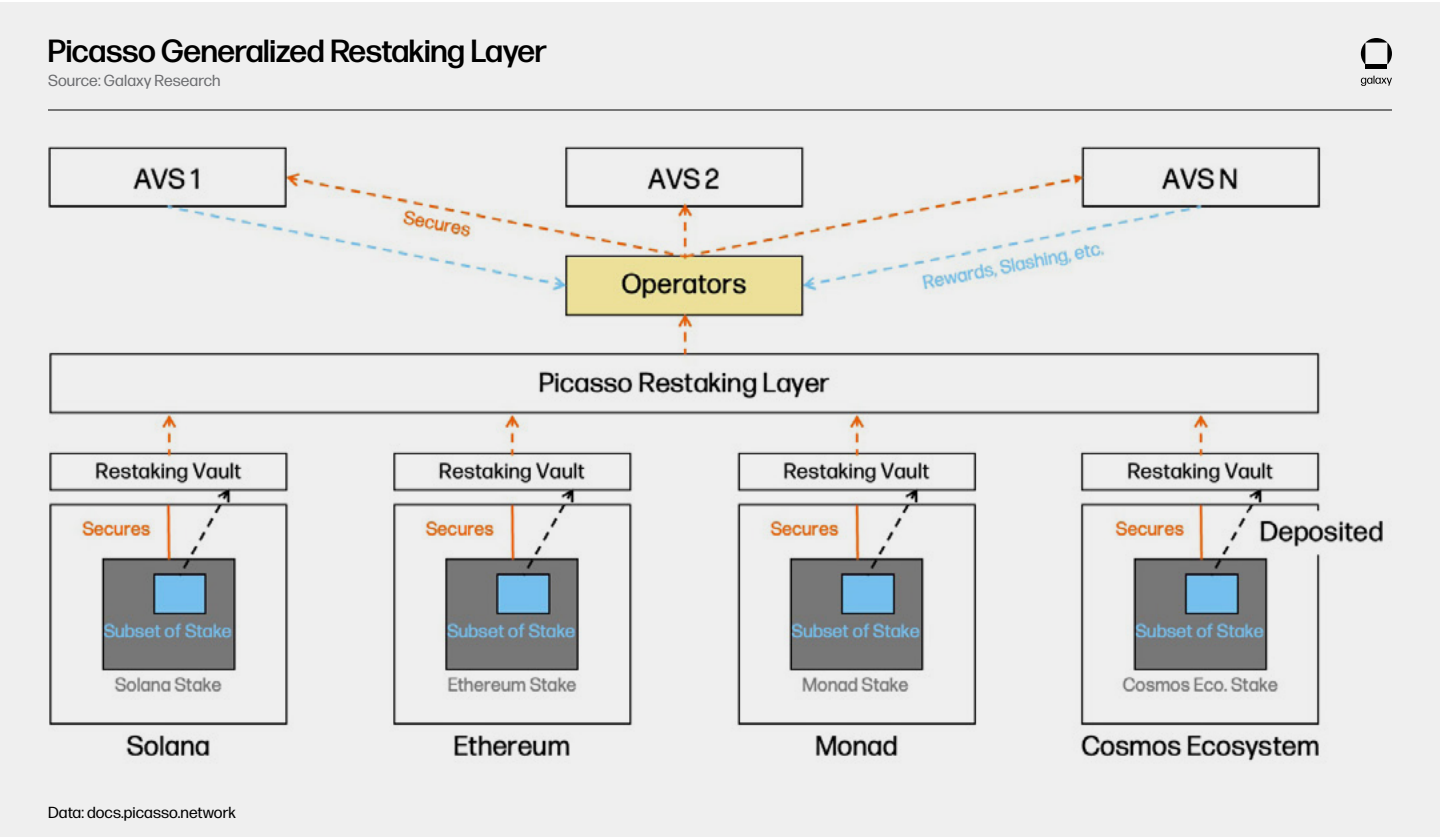
Generalized restaking, also referred to as universal restaking, is a restaking system that enables the pooling of assets native to many chains in the restaking process. This approach is more asset and base chain agnostic, as it allows for the pooling of many staking assets across multiple chains. The model is "generalized" in the sense that assets can be pooled from many chains. From a high level, generalized restaking relies on an additional layer, or series of contracts across multiple blockchains, that sit between the source chains of economic security and AVS'. Below is a simplified graphic of how generalized restaking works.

Picasso and Karak are examples of generalized or universal restaking platforms.



Picasso

Picasso is a generalized restaking blockchain built using the Cosmos SDK. It connects base chains to Picasso via IBC. The Picasso chain receives details about deposited assets on base chains via IBC and then allocates user funds accordingly to AVS'. The "Orchestrator" smart contract on the Picasso chain is responsible for allocating user funds to Picasso node operators, registering and unregistering AVS', among a number of other duties. From a high level, Picasso's restaking solution closely resembles that of EigenLayer which allows for the subset of a network's stake weight to opt-in to secure AVS'. The architecture is copied across multiple base chains and ultimately pooled on Picasso. Node operators under Picasso are selected via governance. At time of writing, the restaking layer is only accepting deposits from Solana through



Data: docs.picasso.network

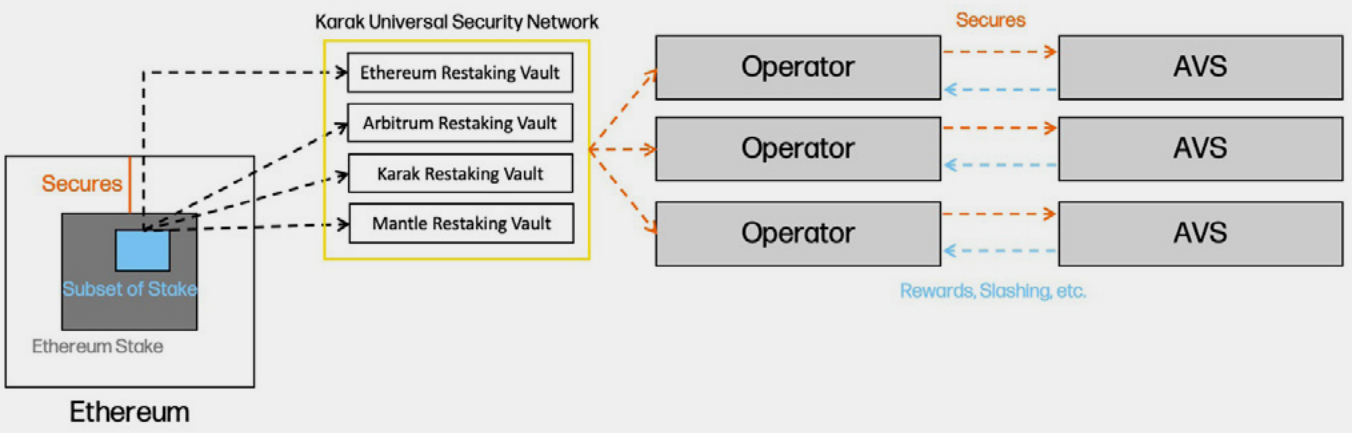
SOL LSTs and native SOL as restaking collateral. Picasso's roadmap includes expanding to Cosmos chains and assets after AVS' begin launching on Solana. The first AVS, which enables IBC connections between Solana and external blockchains, launched in April 2024.

Karak

Karak is a universal restaking layer accepting deposits from Ethereum, Arbitrum, Mantle, BSC, and the Karak Network, a general-purpose Layer 2 built on top of Karak as an AVS. It relies on ETH LSTs as the primary staking asset and supplements them with stablecoins, Pendle tokens, EigenLayer liquid restaking tokens (LRTs), liquid staked BNB, and wrapped bitcoin. The LSTs accepted are wrapped and bridged from Ethereum or are native to the chain they can be deposited on. It functions similarly to Picasso in that it allows several assets across many networks to be pooled and restaked. Unlike Picasso, which exists as a standalone Layer 1 and propagates assets over IBC, Karak is strictly a collection of smart contracts built across multiple chains, including Ethereum Layer 2s. Karak also accepts a wider breadth of assets than Picasso such as stablecoins.

The benefits of a unified security model, under any restaking solution, also comes with risks. The risks of restaking models can be categorized by the three main types of stakeholders involved in the restaking supply chain. This includes base layer networks, node operators, and AVS'. The next section of this report dives into the risks taken on by these entities in the context of restaking on EigenLayer and Cosmos. End users delegating their assets through restaking solutions are downstream of these entities and therefore inherit the downsides of all the risks, and their symptoms are detailed below.

Karak Universal Restaking Layer
Source: Galaxy Research



Data: docs.karak.network

Risks to Base Networks

Base networks derive security from the same staked assets native to their chain that are used in restaking. Consequentially, the primary risks to base networks from restaking pertain to slashing events impacting base chain security and centralization of base chain stake distribution.

Slashing Events Impacting Base Chain Security

Slashing conditions enforced at the restaking layer can negatively impact the security of base chains and the applications that exist on top of them, chiefly, if stake at the restaking layer is concentrated among a small number of node operators. This is especially a concern for EigenLayer and Ethereum, as Ethereum houses a diverse suite of applications holding $41.2b in total value locked (TVL) excluding that of EigenLayer ($59.3b including it) as of June 25, 2024. Penalties triggered by AVS' have potential to significantly reduce the amount of staked assets available for securing the base chain depending on the relative size of restaked assets to staked ones on the base chain.

As of June 25, 2024, only ~17% of total Ethereum staked on Beacon Chain is restaked and 98.26% of all restaked ETH is captured by EigenLayer. The share of Beacon Chain deposits that are natively restaked through EigenLayer is 11.93%. The slashing of natively restaked ETH most directly impacts Ethereum protocol security, as these deposits represent collateral directly staked to the Ethereum protocol. This is unlike restaked LSTs, where a token carrying the value of Beacon Chain deposits is slashable before the underlying deposit itself. As a result, there are potential avenues to slashing LSTs that do not change base chain security. More on this idea will be covered in a future report focused on the dynamics of LRTs. EigenLayer does not enforce any slashing conditions on node operators today, so the risk of negative impacts to the security of Ethereum today via restaking are minimal. This changes, however, when slashing is implemented. Cosmos replicated security took a similar approach to limiting slashing penalties upon initial launch. The steps EigenLayer is taking in this regard are not exclusive to the restaking solution.

Under replicated security, 95% of Cosmos Hub stake is used to secure AVS'. A slashing penalty enforced on the AVS layer thus has a near 1:1 impact on Hub economic security. This idea also applies to centralization forces on the Hub's stake, which will be examined later. Unlike Ethereum, the Cosmos Hub doesn't support smart contracts or the applications they enable. However, economic security still plays an important role in safeguarding the network.

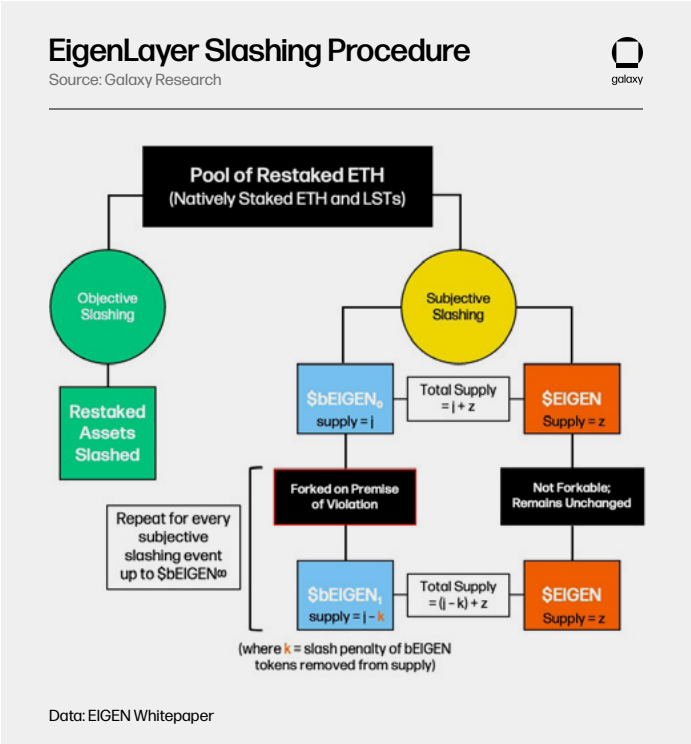
Other than the share of base chain security at risk of slashing through restaking, it is also important to consider the types of offenses that AVS' can enforce that may result in slashing.

Intersubjective Faults on EigenLayer

Not all slashing offenses on AVS' may be objectively and cryptographically verifiable. This idea was introduced by the Eigen Foundation in a whitepaper explaining the $EIGEN token. In the paper, the team explains that intersubjective faults, that is faults not easily verifiable on-chain, in some AVS', such as oracles, can result in base chain splits. On-chain enforcement of behaviors on EigenLayer AVS' may require off-chain agreement, or social consensus, among network observers - a tedious process that can end in a fork of the base chain if there is widespread disagreement among node operators about the correct state of the AVS.

To address the burden on Ethereum consensus due to intersubjective faults, the EIGEN token can be used by validators to enforce intersubjective slashing via token forks instead of base chain forks. This idea was originally introduced by Paul Sztorc in 2014 through the Truthcoin whitepaper, and more recently popularized through EigenLayer. It essentially offloads the need for social agreement among base layer validators by allowing node operators to express their preference about intersubjective faults and claims on the restaking layer through the EIGEN token.

The graphic below highlights the slashing procedure for the EIGEN token:



Data: EIGEN Whitepaper

The left side of the graphic above visualizes the objective slashing procedure. Objective slashing penalties are mathematically and cryptographically provable offenses, like double signing and downtime, that are verifiable through on-chain protocols. For these offenses, restaked assets can be slashed without the need for universal agreement among chain observers. The right side of the graphic visualizes the intersubjective slashing procedure. Penalizations in these instances can require social agreement between chain observers. Through the EIGEN token, node operators can rely on agreement around slashing the staked supply of EIGEN, instead of staked ETH. As such, there are two "classes" of EIGEN:

1) vanilla EIGEN that can be held in externally owned accounts (EOAs) or used to interact with decentralized finance (DeFi) applications.

2) bEIGEN, or staked EIGEN, that is forkable and may be subjected to slashing penalties.

Each new fork of bEIGEN results in dwindling supply, as the slashing penalty is manifested by removing the slashing offender's bEIGEN from the circulating supply. By having the ability to slash the token and socially agree on its next fork, EigenLayer can extend Ethereum PoS security more efficiently beyond its borders by limiting the input needed from Ethereum base layer. AVS' can also substitute their own token as an intersubjective token in place of EIGEN if they choose to. This is a basic explanation of how the EIGEN token and intersubjective slashing work; precise details can be found in the EIGEN whitepaper.

Objective Faults on Cosmos

Under replicated security, AVS' are restricted to only slashing on the same basis as that of the Cosmos Hub. This includes downtime and double signing, objectively verifiable faults that result in jailing or tombstoning and up to 5% of stake being slashed. In part, this is because replicated security requires the vast majority (95%+) of base layer economic security and validators to secure AVS'. As a result, validators colluding to attack a consumer chain would result in the price of ATOM (Cosmos Hub staking asset) cratering. This idea doesn't apply to partial set security or EigenLayer's approach to restaking, as only a small portion of total stake may be used to secure AVS'.

Cosmos Hub validators vote on governance proposals to review what AVS' can be secured through replicated security. This process vets consumer chains before they can participate in shared security. Once accepted as consumer chains and launched on mainnet, there are additional measures taken to safeguard the Hub from consumer chain slashing. They include:

1) Governance proposals to review the integrity of AVS double signing claims on Hub node operators. This protects the Hub from accepting slash packets sent by a malicious AVS to permanently remove honest validators from the network. In the future, Cosmos Hub developers are working towards enabling AVS' to submit slash packets that can be automatically verified by the Hub instead of through governance. Prop #818 is an example of this process. In this scenario two Hub validators accidentally double signed on Neutron, a Cosmos consumer chain.

2) Throttling, or layering, of slash penalties for downtime such that no more than 1% of the Hub's validator set can be slashed and jailed at a single point in time. This preserves the liveness of the Hub even in the event of genuine malpractice at the AVS layer. However, cryptographically proving downtime can be difficult.

3) Restrictions on consumer chain influence over slashing parameters. Only the Hub validators can outline the penalties consumer chains can enforce upon its stake and validator set. Doing so ensures the liveness and overall security of the Hub cannot not be jeopardized by AVS'.

Fraud votes will be introduced the next iteration of Cosmos shared security. These are governance proposals that enable the slashing of validators that perform non-objectively verifiable attacks stemming from qualities unique to partial set security (i.e. the subset problem).

Restaking introduces the potential for slashing based on additional parameters enforced by AVS', instead of strictly by the base chain. This introduces higher degrees of both reward and penalties. However, on the Cosmos Hub, the ability for consumer chains to enforce additional slashing penalties is heavily restricted and controlled by Hub validators via governance. On Ethereum, it is unclear the impact that slashing will have on base chain security due to the nascency and diversity of its restaking solutions and AVS'. Again, no penalties are currently live on EigenLayer AVS', the largest restaking solution live on Ethereum. In the future, there may be functionality introduced to EigenLayer that does support automatic slashing initiated by AVS' that cause underlying stake securing Ethereum to be compromised.

Centralization of Base Chain Stake Distribution

The same reasons that drive centralization in stake in the base networks' environments can apply additional centralizing pressure through the validation of AVS'. This is broadly driven by the revenues captured by, and overall profitability of, node operators (which is bound to the opportunities offered by AVS'), their timing to market, and their abilities to scale. Therefore, measures taken to prevent centralization of stake on the base protocol, whether they be algorithmically enforceable rules or self-regulating measures taken by base layer validators, may be circumvented by the introduction of restaking yields.

Replicated security is unique in that the Cosmos Hub validator set and native stake is effectively copied across AVS', and every node operator engaged in replicated security runs the same, additional services. However, the rewards earned from staking by node operators are not equal. Node operators with larger balances of stake under management earn higher rewards than node operators with smaller balances of stake under management. While the costs of securing AVS' are equal across all Hub node operators, rewards are variable and depend on the amount of stake under management. Because of this, Hub node operators with large balances of stake under management have a greater chance of offsetting the costs of securing new AVS'. Smaller node operators are at greater risk of operating at a loss or shutting down operations entirely.

Under partial set security and the implementation of security aggregation, the cost/reward dynamics of running AVS' will change for node operators as they will be able to opt-in to securing different sets of AVS'. However, this may still lead to staking rewards being unequally captured by large node operators as users may choose to delegate additional stake to operators earning higher restaking yields than others. In these cases, the stake distribution of the base layer may experience stronger centralizing pressure than what is present today.

Restaking creates centralizing pressures on Ethereum as well. Certain restaking protocols like Karak and Symbiotic do not offer permissionless onboarding of Beacon Chain node operators. In these cases, users wanting to restake native ETH must do so

through a set of permissioned node operators, otherwise users can stake other assets such as LSTs, which are already sources of centralization at the base layer. Restaking protocols that do support permissionless native restaking are healthier for base layer stake centralization in that it allows restaking rewards to be captured by anyone at any time without the need for permissioned sets of node operators. EigenLayer supports the permissionless onboarding of natively staked ETH through EigenPods. Any user can spin up an EigenPod to operate as a Beacon Chain validator node operator and earn restaking rewards. To do this, node operators must give EigenLayer smart contracts the ability to enforce additional slashing condition on their staked ETH. As of June 27, 2024, there are 3.9 million native ETH locked in EigenPods.

Liquid restaking on Ethereum also creates centralizing pressures. LRT apps that accept native ETH deposits as restaking collateral may centralize Beacon Chain stake in a similar way to LST apps. LST apps incentivize users with higher staking yields and liquidity on their native ETH deposits, just as LRT apps do. The advantage of LRTs over LSTs is that LRTs pass additional yield to users from restaking that LSTs do not. If an LRT app does not accept native ETH as restaking collateral, users must stake other assets, most commonly LSTs, thereby increasing demand for LSTs and exasperating the centralizing force of these liquid staking assets on the base layer.

Risks to Node Operators

The risks posed to node operators are largely operational and pertain to their abilities to scale and establish streamlined processes for adding and removing AVS'. Faults in any of these areas can result in slashed stake or an uncompetitive product. Each AVS added by a single node operator introduces additional facets of intricacy, costs, and responsibility to them.

The varying types of AVS' also mean unique costs and procedures may be required by node operators for supporting each AVS, making processes and infrastructure across services difficult to duplicate. This can lead to node operators running dozens, and possibly hundreds, of services requiring unique infrastructure and processes to operate across hundreds to thousands of validators. Ultimately, the diverse nature of AVS' can make scaling and managing operations strenuous for node operators.

The procedures for removing support from AVS' are equally as important as adding them. This is especially true in the context of restaking where AVS churn can be high. Ensuring smooth off-boarding processes is important to not getting slashed or causing operational confusion across AVS'. This is even more true in cases where node operators are using the same servers to run AVS' and Ethereum validator software.

Node operators also face social risk. Adding and removing AVS' has direct impact on yields and risks for end users who are restaking their assets through restaking node operators. Communicating details about opting-in/out of AVS' and notifying end users of actions that can impact their delegated funds is an extremely important responsibility of node operators. Failure to do so can result in eroded trust from end-users that harms business and carries reputational risk for node operators.

Risks to Actively Validated Services

Economic security is shared, or pooled, under restaking, meaning many AVS' and base chains have rights to slash the same value that collectively secures them. The risk is that out of protocol entities can directly impact the security of an AVS (both AVS to AVS and base chain to AVS), like the dynamic of AVS slashing impact on base chain security. Feeding into the slash risk from other AVS' and base chains is volatility in the dollar value of the assets securing AVS', and their ability to adequately incentivize node operators.

Economic security is measured in dollars and supplied in native units of digital assets (e.g. an AVS is secured by $100 million worth of ETH). Fluctuations in the values of the assets securing AVS' impact their economic security. Using higher quality and more liquid assets to secure AVS' is key to mitigating the volatility in their economic security. Some AVS' may still elect to use more volatile assets for a variety of reasons (e.g. new user acquisition or ecosystem alignment). The risk of dollar volatility is not unique to AVS', base chains face the same headwinds with volatility in the dollar value of natively staked assets especially in the early months and years following a mainnet launch.

Secondly, there is pressure on AVS' from node operators and end-users about whether they will produce enough "real" value (either from transaction fees or revenues produced by the AVS' functionality) to make it profitable enough for node operators to service them. Thus, AVS' may choose to launch with inflationary tokens to adequately cover the liabilities owed to node operators. Even so, over time, node operators could deem that they are not receiving adequate incentive to continue running some AVS'. This may leave certain AVS' without enough validators and staked assets to secure them, which would negatively impact these AVS' security.

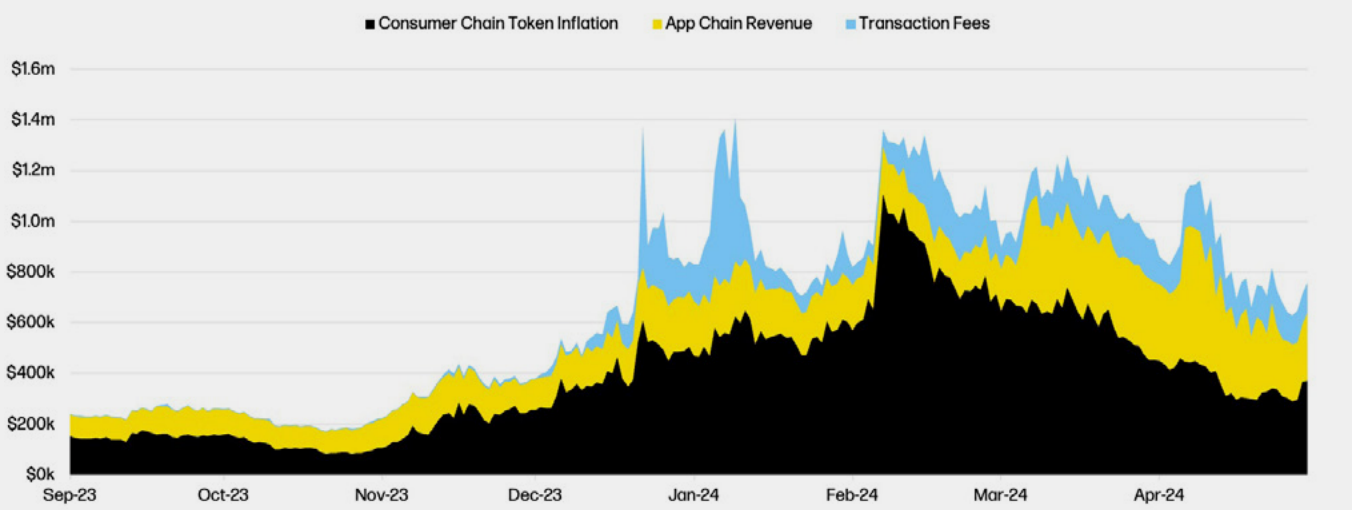
While we don't know what the incentive landscape will look like with restaking via EigenLayer, we have an idea of what it looks like in Cosmos replicated security excluding MEV through April 2024 (and a price per ATOM of ~$8.75). Galaxy Research estimates consumer chains add roughly 0.04% of yield to Hub validators, or $0.003 per one ATOM earned for validators in the top 95 percentile by voting power.

The distinction between the restaking dynamics on Cosmos under replicated security vs Ethereum is that the market driven nature of EigenLayer allows supply and demand for restaking services to naturally find an equilibrium when either is too scarce or too abundant.

Again, base chains face the same headwinds with incentivizing participation in security in the early months and years following a mainnet launch. However, both these risks are especially pertinent to AVS' relying on restaking solutions as they don't directly own the security they rely on. Depending on restaking yields and EigenLayer smart contract functionality, competition between AVS' for shared security may be fierce and cause validators to frequently reshuffle what set of AVS' they support at any given time. This may in turn facilitate faster turnover of AVS' and heightened volatility in the economic security of AVS'.

Annualized ICS Revenue From Consumer Chains to Cosmos Hub by Source (Less MEV)

Source: Galaxy Research



Data: Numia, CoinGecko

Other Considerations

There are a few other risks and considerations of restaking worth highlighting. They include restaking and leverage, the influence of airdrop farming on restaking protocols, and the influence of restaking on asset liquidity.

Restaking and Leverage

Restaking in and of itself is not financial leverage. Instead, it is a more abstract type of leverage contingent on the responsibilities and capabilities of node operators. This is because node operators are slashed on their actions and abilities to operate within the rules of the

AVS' they opt-in to, instead of being penalized on the basis of asset prices (e.g. a margin call). This is akin to taking on an increasing amount of responsibility at your job. The more projects you take on the greater your chance of committing an error and getting fired or receiving a pay cut. However, you can't lose your job if you misallocate your own individual company sponsored 401k and lose all your savings.

The basis of penalization in restaking is within the control of node operators, as they voluntarily opt-in to slashing conditions and control the hardware/ software they run. This is not the case with financial leverage where individuals cannot control the markets that ultimately penalize them. This is a key distinction because the basis of penalization lies solely on the capabilities and actions of node operators and the penalization of one node operator does not have an impact on another's stake (i.e. one validator cannot be slashed for wrongful actions of another), as is the case with the negative feedback loop/ daisy chain effect of financial leverage unwinding.

Even so, as explained earlier in this report, penalizations of node operators can have a cascading impact on the security of AVS' and the base chain. For example, if 1 ETH securing three AVS' is slashed by one of them, all three AVS' secured by that 1 ETH take negative hits to their security blankets. This can make malicious attacks and collusion easier to carry out on AVS' and their base chains.

Influence of Airdrop Farming and Chasing Hype on Restaking

Airdrop farming can skew the supply of restaked security. Points have incentivized users to deposit their assets into restaking protocols independent of demand for restaked security from AVS', inflating the supply of restaked assets. Airdrop farming can also have negative effects on how applications are designed. The fast-paced nature of points and catching the momentum of an ecosystem can push builders into launching apps before they are ready for deployment or fully fleshed out for the purpose they are intended to serve. The result can be phantom apps that are not used over the long-term, or apps that lack key functionalities, such as the ability to withdraw or transfer assets. In the end all these forces driving inorganic supply for restaking will have to be unwound, which can have negative impacts on asset prices and cause other problems across DeFi products with ties to restaking. Over time, the industry will gain a clearer picture of what true supply for restaking looks like (which is a function of demand), especially as restaking protocols deployed on Ethereum and Cosmos become more feature complete.

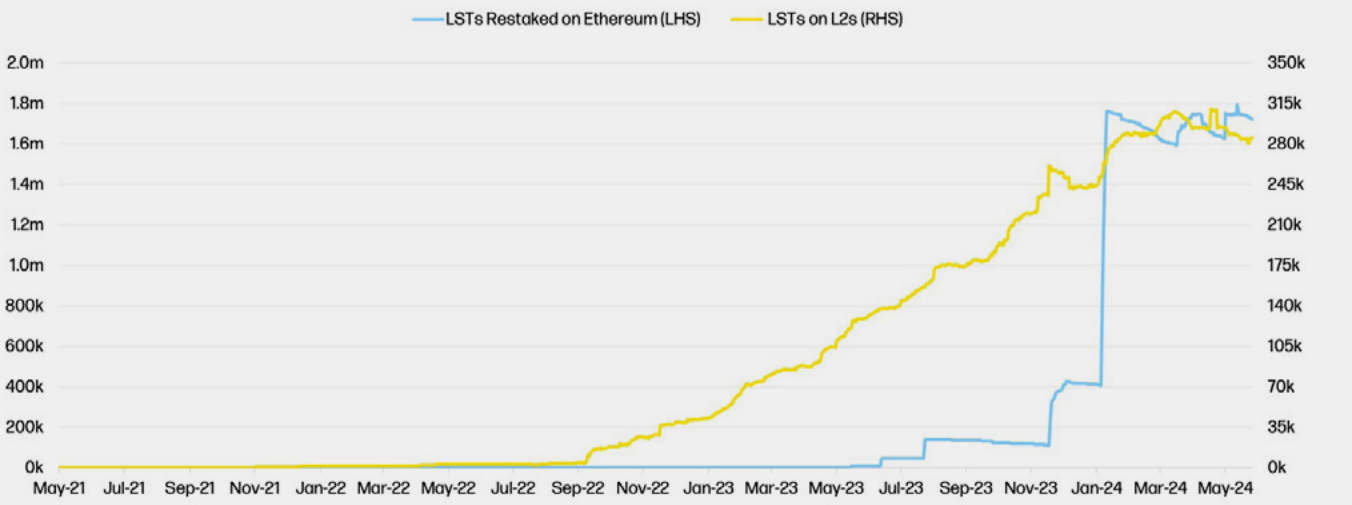
Restaking Liquidity Vacuum

Another consideration in the context of Ethereum restaking is the attraction of liquidity to Ethereum L1. The goal of Ethereum's rollup centric roadmap is to push L1 activity and liquidity off chain, but restaking incentivizes activity to stay on or return to L1. This dynamic is emphasized through points programs at both the restaking protocol and LRT protocol levels.

The chart below offers a view of what this trend looks like through the lens of LSTs restaked on Ethereum L1 and LSTs circulating on L2s. The amount of LSTs on L2s peaked in April 2024 and has been range bound since February 2024 after 21 months of consistent growth. At the same time, the amount of LSTs staked on Ethereum L1 went parabolic.

Liquid Staking Tokens (LSTs) Restaked on Ethereum Against LSTs Circulating on L2s

Source: Galaxy Research



LSTs on L2s Include stETH, rETH, ankrETH, mETH, cbETH, sfrxETH, oETH, swETH
Data: Dune (glxyresearch)

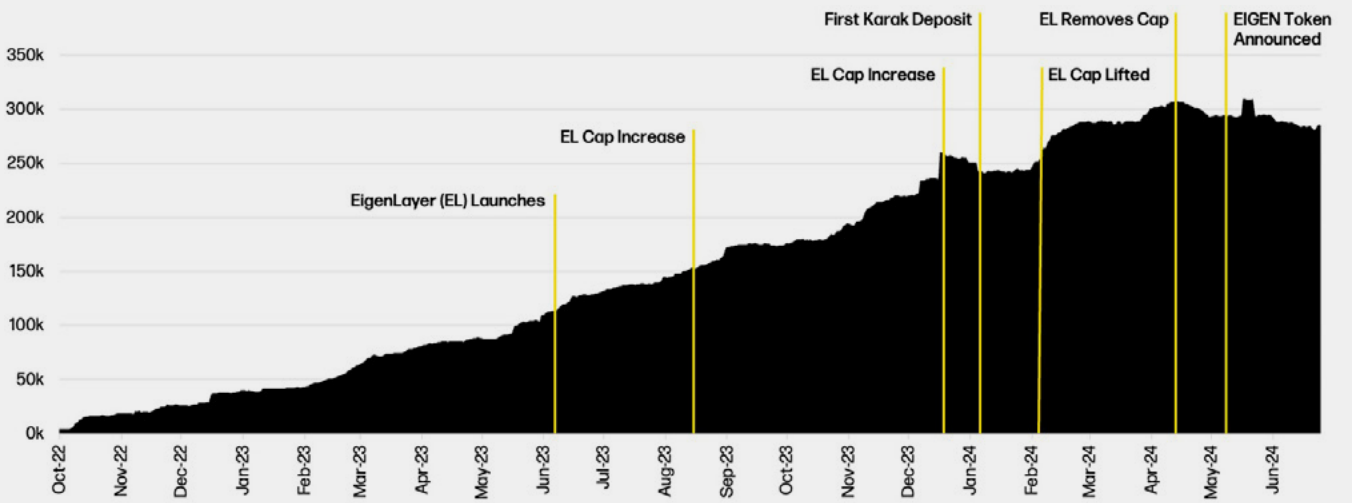
The chart below tracks the all-time trend of the observed LSTs on L2s with key restaking events overlaid.

While LST liquidity on L2s has been flat, LRTs are becoming more prominent. LRTs are found on Arbitrum, Base, Blast, Linea, Mode, OP Mainnet, and Scroll with 69% of their supply by native units being on Arbitrum and Blast. Not pictured in the chart is 24,744 ezETH and 7,396 eETH on Mode.

Despite the growing prominence of LRTs on L2s, LSTs retain significantly higher levels of liquidity and adoption than that of LRTs. However, as explained in the analysis above, the prominence of LSTs is starting to wane as they are being locked up in restaking protocols launched on the base chain, Ethereum. It is important to consider the potential impact of stalled LST expansion on the overall liquidity in decentralized finance applications on L2s, especially in lieu of comparable liquidity from LRTs.

Liquid Staking Tokens (LSTs) Restaked on Ethereum Against LSTs Circulating on L2s

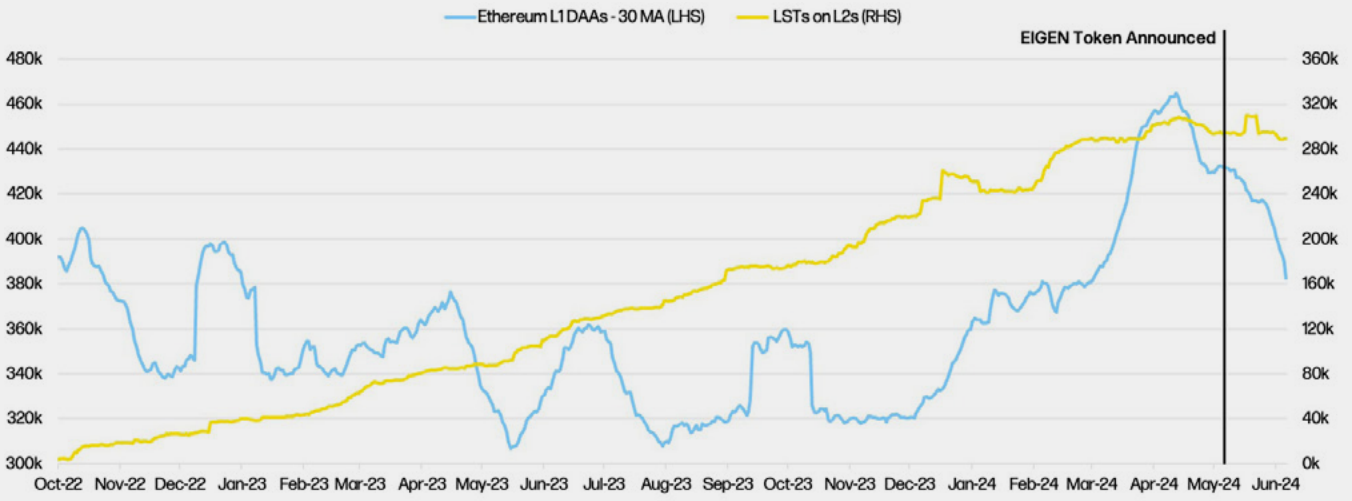
Source: Galaxy Research



LSTs on L2s Include stETH, ankrETH, mETH, cbETH, sfrxETH, oETH, swETH
Data: Dune (glxyresearch)

LSTs Circulating on L2s Against Ethereum L1 Daily Active Addresses

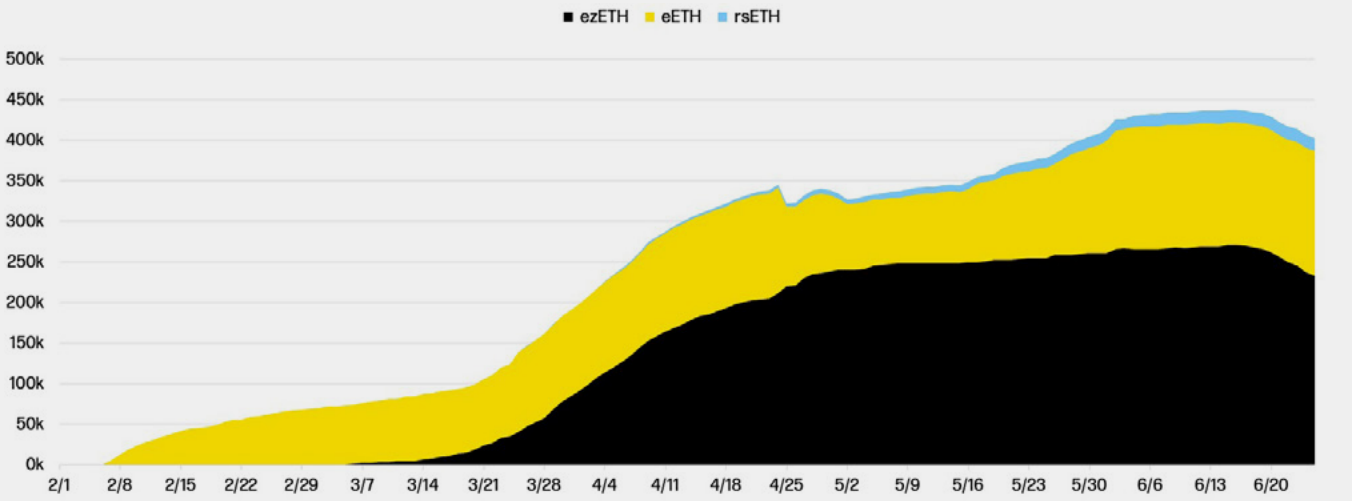
Source: Galaxy Research



LSTs on L2s Include stETH, ankrETH, mETH, cbETH, sfrxETH, oETH, swETH
Data: Dune (glxyresearch)

Liquid Staking Tokens (LSTs) Restaked on Ethereum Against LSTs Circulating on L2s

Source: Galaxy Research



L2s include Arbitrum, Linea, Base, Scroll and Blast
Data: Dune (glxyresearch)

Conclusion

Restaking is an important primitive in the evolution of public blockchains; it is intended to create a more unified and efficient security model for blockchain applications that can be exported and shared by multiple protocols at the same time. The idea and its implementation in the Ethereum and Cosmos ecosystems are still in a nascent phase of experimentation and research. Many details about how restaking protocols will work in practice are still unknown. Further, their exact impact on stakeholders such as base networks, node operators, and AVS' remains unclear. However, in this report, we have detailed the important risks and considerations of restaking for the primary entities involved in the activity in the early phases of its evolution. Areas of further research include liquid restaking protocols and other types of products and services that can be built on restaking protocols.

Contact Us

galaxy.com

For all inquiries, please email contact@galaxy.com.

Legal Disclosure