

Modular Blockchains:

The Race to Become the Top
Security Provider

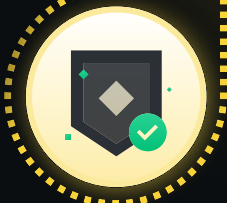


Table of Contents

Key Takeaways	2
Introduction	3
Setting the Scene: Monolithic vs. Modular	4
Why is this significant?	5
Where do Layer-2 rollups fit into this?	8
Ethereum	10
A closer look at restaking	11
Project in focus: EigenLayer	11
Cosmos	16
Replicated Security	17
Project in focus: Neutron	18
Osmosis and Mesh Security	20
Bitcoin	24
Project in focus: Babylon	24
Project in focus: Stacks	27
Closing Thoughts	29
References	30
Latest Binance Research Reports	31
About Binance Research	32
Resources	33

1

Key Takeaways

- ❖ Blockchains seek to perform four key functions: consensus, data availability, execution, and settlement. While monolithic blockchains perform all of these functions in the same layer and in a generalized manner, a modular approach seeks to separate them among different chains and protocols.
- ❖ Ethereum’s execution-focused Layer-2 (“L2”) rollups have succeeded in capturing market share and have become major revenue generators for Ethereum, which provides them with security. Other Layer-1s (“L1s”) have taken notice and are also seeking to enter the lucrative security market.
- ❖ EigenLayer seeks to solve the problem of fragmented blockchain security by pooling Ethereum’s security for other applications to utilize with their restaking technology.
- ❖ Cosmos has focused on a slightly different solution to help increase the security of its appchains with its Replicated Security model. Neutron is the first project to launch using this technology, with many others coming soon.
- ❖ A notable Cosmos project, Osmosis, has proposed its own version of shared security called Mesh Security, focusing on stakers rather than validators.
- ❖ On Bitcoin, Babylon has been working on a solution to leverage the security of the Bitcoin blockchain to increase the security of Cosmos appchains and eventually other proof-of-stake (“PoS”) blockchains.
- ❖ Stacks, with their novel proof-of-transfer (“PoX”) consensus mechanism, has also worked out a solution to using Bitcoin to secure its transactions. Developments in the upcoming Stacks Nakamoto Release will further solidify this technology.

Introduction

The concept of a “modular blockchain” is often discussed in the crypto community. However, various factors sometimes get overlooked in these broader discussions. What exactly are modular blockchains? How do they compare to the more familiar monolithic blockchains that we are used to?

Going one step further, what does the increased popularity of adding modular components to blockchains mean in terms of value accrual for Layer-1 (“L1”) chains? As we will discover, a number of protocols are seeking to utilize modularity to help improve the crypto-economic security of projects across different chains.

In this report, we will start by explaining the differences between monolithic and modular blockchains before diving into crypto-economic security-related infrastructure projects across Ethereum, Cosmos and Bitcoin. We will focus on restaking and EigenLayer for Ethereum, Replicated Security, Neutron, and Osmosis for Cosmos, as well as Babylon and Stacks for Bitcoin.

3 Setting the Scene: Monolithic vs. Modular

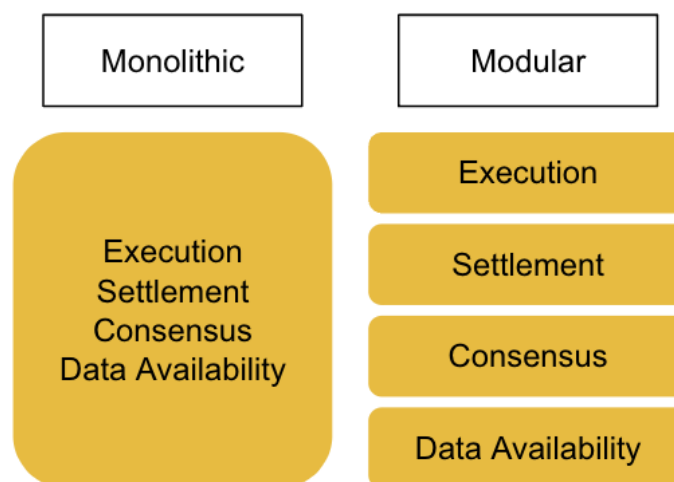
Let's begin our discussion with a brief overview of the **differences between modular and monolithic blockchains**.

Defining a blockchain at its most basic level as an immutable ledger of transactions, we can broadly classify the majority of blockchains, at least those with notable value attached to them, as **monolithic** blockchains. To fulfill its basic requirement of tracking valid transactions and data in a chronological manner, a **blockchain must perform four key functions**:

1. **Consensus**: reaching an agreement between validators or miners on transaction ordering, e.g., Proof-of-Stake ("PoS"), Proof-of-Work ("PoW"), etc.
2. **Data availability**: ensuring transaction data is available for the entire network to view
3. **Execution**: processing transactions to update the state of the blockchain
4. **Settlement**: resolving disputes, verifying the validity of transactions, and ensuring the "finality" of transactions

Monolithic blockchains, like Bitcoin and Ethereum, perform all of these functions on the same layer and in a generalized manner. **Modular blockchains, on the other hand, seek to separate these functions across multiple different chains.**

Figure 1: Monolithic vs. modular blockchains



Source: Binance Research

Why is this significant?

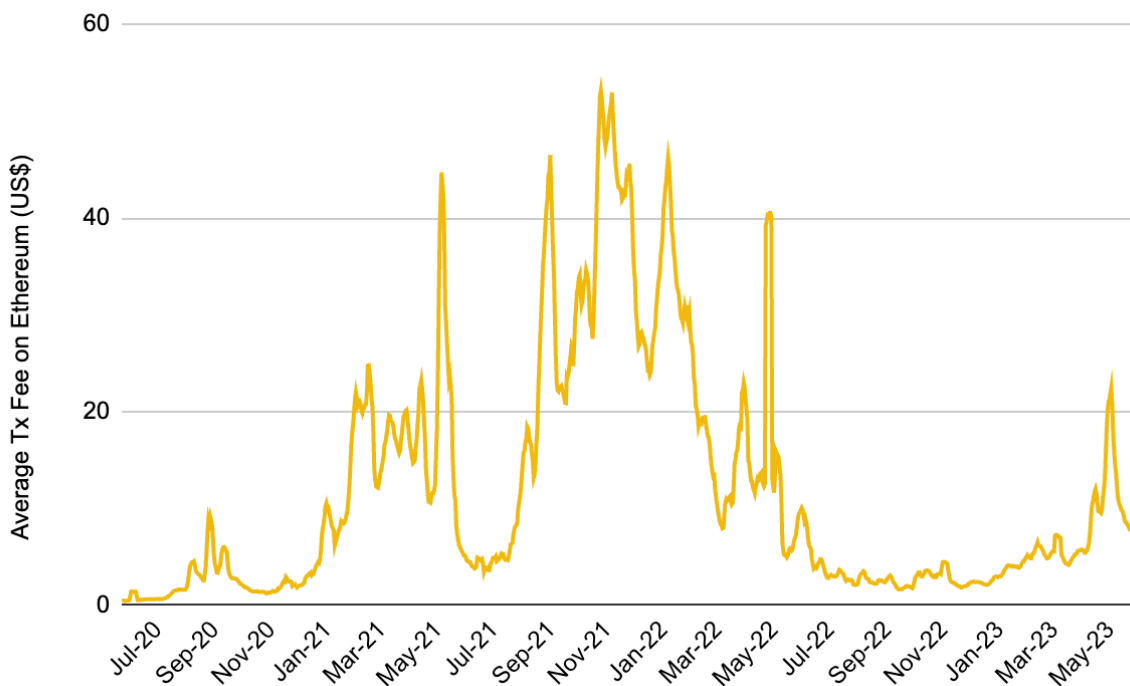
Given that monolithic blockchains seek to perform all the above functions through the same chain, this prevents them specializing in any one function. A **modular approach means that different blockchains can specialize in different parts of the stack and thus provide a more customized solution that is optimized** for different user needs.

We can evaluate monolithic vs. modular approaches through the [Blockchain Trilemma](#), the idea that a blockchain faces a tradeoff as it can only optimize for two out of three features: scalability, decentralization, and security.

❖ Scalability:

- Scalability can be defined as the ability to increase the number of transactions being processed, i.e., throughput, without an equivalent increase in the cost of verifying those transactions.
- There are **two main ways to increase throughput**:
 - Firstly, we can **increase block sizes** and thus the number of transactions that can fit into each block. However, larger block sizes increase the hardware requirements of running a full node and thus harm the decentralization of the network.
 - The other method would be a modular approach, i.e., to **move execution of the transactions from the main L1 chain onto other chains, i.e., Layer-2 (“L2”) solutions**, and then use proofs to verify the transactions on the L1. This is essentially how the Ethereum roadmap has evolved over the last few years and why we have seen an explosion of L2 solutions like Optimism and Arbitrum. This is the “modularization” of Ethereum and one of the main ways it is stepping away from its monolithic origins toward a more modular approach.

Figure 2: Despite the popularity of Ethereum L2 solutions, gas fees on L1 regularly spike, illustrating the difficulty of scalability with a mostly monolithic architecture



Source: Binance Research, as of June 14, 2023

❖ Decentralization:

- We can consider decentralization in the context of the hardware requirements for running a full node. The lower the hardware requirements, the more users will be encouraged to do so, thus furthering the decentralization of the network.
- **Blockchains rely on a network of users, i.e., validators or nodes, who execute transactions and bundle them into a block, i.e., block producers.** To prevent malicious block producers from including invalid transactions, **blockchains also rely on nodes to verify the accuracy of each block** before adding it to the chain. Generally, **monolithic blockchains use the same set of validators to perform BOTH functions, i.e., full nodes.**
- However, this thoroughly limits the scalability and potential decentralization of monolithic chains, as throughput can only be increased by higher resource requirements for running full nodes.
- In a **modular blockchain system, the execution layer will be responsible for block production, while a separate layer can be responsible for verification.** This means that throughput can be increased by larger block sizes with higher resource requirements without limiting decentralization. Block production, which tends to become centralized due to economies of

scale, can operate in a relatively small group as long as their work is verified by a large and decentralized group of verifiers. Interestingly, this has also been a core thesis of Ethereum co-founder Vitalik Buterin, as outlined in his “Endgame”⁽¹⁾ article.

“We get a chain where block production is still centralized, but block validation is trustless and highly decentralized, and specialized anti-censorship magic prevents the block producers from censoring”

Source: Vitalik Buterin, Endgame

❖ **Security:**

- We can consider blockchain security from two different perspectives.
 1. Consensus or settlement assurance: This is sometimes generally referred to as **crypto-economic security** and essentially asks the question, **“Once a transaction is sent and included in a block, how costly is it to maliciously remove that transaction from the chain?”** Consensus mechanisms, such as PoS or PoW (as described above), provide these settlement assurances by creating economic costs. In practice, this means that in order to reorganize a blockchain, the attacker will have to gain control of a majority (51%) of hashing power in a PoW system or the majority of staked tokens in a PoS system. **For PoS chains like Ethereum, the likelihood of this type of attack is dependent on the value of ETH and the value staked on the network; the greater the amount for both of these numbers, the more costly it is for someone to attempt an attack.** In addition, PoS systems typically include **slashing** penalties, i.e., part or all of your staked tokens can be destroyed if you behave dishonestly, further adding risk to any potential attackers. Given the crypto-economic security that Ethereum has built up as a function of its market capitalization (“market cap”) and level of decentralization, “borrowing” that security using a modular blockchain approach is a key upcoming narrative and something we will explore [further](#).
 2. Validity: This type of security is concerned with the rules set out in a blockchain and whether any given block is valid according to those rules. **Validity security is independent of consensus security or the value of a token and depends on people running full nodes.** The relevant question here is, “How easy is it to run a node that fully verifies the chain?” The more participants that run a full node, the

better the validity security is. This ties in well with our above points on decentralization and further underscores the importance of taking a modular approach and dividing the roles of block producer and block verifier to ensure that a sufficient level of independent verifiers exists to keep a chain both decentralized and secure.







The overall point to take away from this is that a **modular approach can target all three key factors within the Blockchain Trilemma and might very well provide a more customizable solution that is optimized for both developers and users.**

Where do Layer-2 rollups fit into this?

Using a modular approach, blockchains can be optimized across different layers and perform different functions to maximize decentralization, security, and scalability as needed.

For example, let's consider Ethereum's L2 rollups, which focus on the execution aspect of a blockchain. On one side, we have optimistic rollups like Arbitrum and Optimism. On the other side, we have zero knowledge ("zk-") rollups like zkSync and StarkNet. What all of these have in common is the fact that they are **significantly cheaper than the Ethereum L1 to conduct activity** on and therefore are able to attract users and developers onto their platform.

Figure 3: Rollups are significantly cheaper than the Ethereum L1 to transact with

Logo	Name	Rollup type	Cost to send ETH (US\$)	Cost to swap tokens (US\$)
	Loopring	Zero Knowledge	0.02	0.44
	Polygon zkEVM	Zero Knowledge	0.03	0.11
	zkSync Lite	Zero Knowledge	0.04	0.09
	Arbitrum One	Optimistic	0.06	0.07
	Boba Network	Optimistic	0.07	0.17
	Ethereum	Base Layer	0.78	3.92

Source: l2fees.info, as of June 14, 2023

The other major factor that they all have in common is their method of execution. **L2 rollups, of both the zk and optimistic varieties, work by performing transaction execution outside of the L1 and then posting this data up to the L1, where consensus and settlement occur.** As transaction data is included in L1 blocks, rollups benefit from the security of Ethereum (i.e., to maliciously remove a rollup transaction, the attacker would need to gain majority control of Ethereum).

The relevant point to us is that the **act of posting transaction data to the Ethereum L1 incurs a cost**, which we can refer to as publishing fees. In fact, rollups like Arbitrum, Optimism, and zkSync are routinely on the list of the top gas spenders on Ethereum, which has created a **new form of value accrual for L1s.**

Figure 4: Four of the top ten Ethereum gas users are L2 solutions

Protocol	Fees Last 30 days (US\$M)
Uniswap	67.1
Tether	9.0
zkSync	8.8
Arbitrum	4.7
OpenSea	4.7
Blur	4.2
MetaMask	4.1
1inch	3.5
StarkNet	3.2
Optimism	2.7

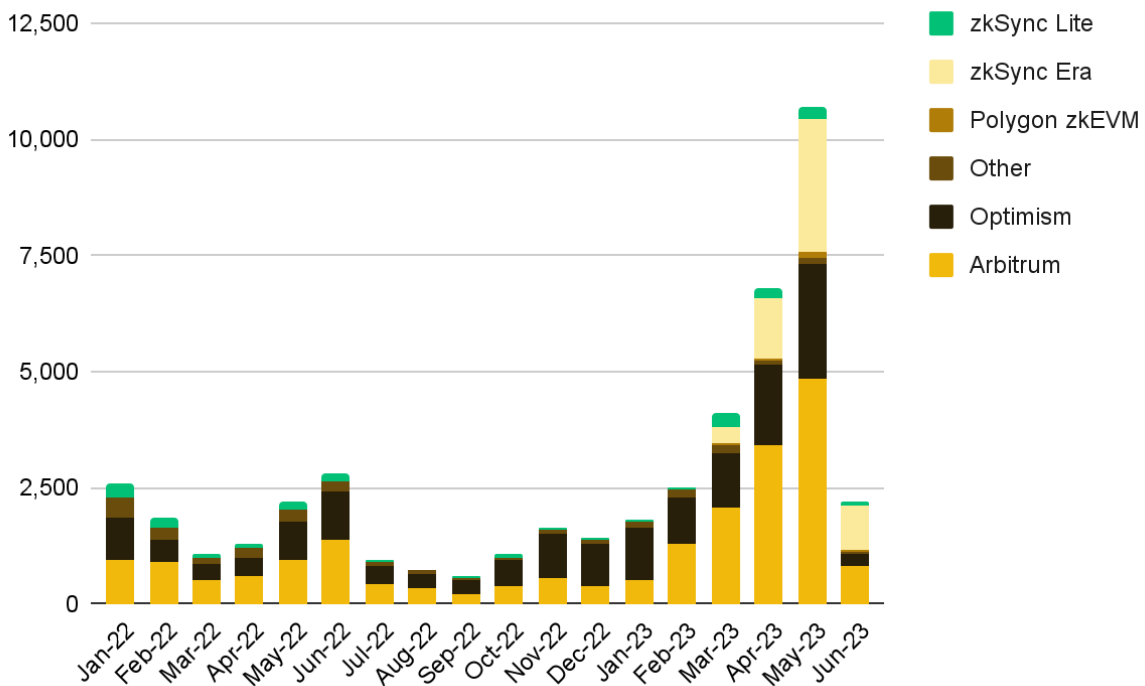
Source: Token Terminal, Binance Research, as of June 14, 2023

In essence, rollups are secured by Ethereum security (where Ethereum functions as the consensus, data availability, and settlement layer) and pay fees for this privilege. **Given the fact that rollups have succeeded in capturing market share, this has become a top revenue source for Ethereum.** Other L1s have also taken notice and have been working on their own solutions to enter the lucrative security market. Combine this with our discussion on splitting different components of blockchains via the modular blockchain thesis, and we can begin to conceptualize the race to become the top security provider and why this is becoming a key goal for L1s.

4 Ethereum

Ethereum boasts the highest security budget of all PoS chains, with over 19M⁽²⁾ \$ETH staked, amounting to US\$34B+⁽³⁾ of value securing the chain. To clarify once again, this essentially means that to gain control of the chain, an attacker would have to control at least 51% of this value – not an easy task, given the numbers in play. As mentioned above, L2 rollups have been key users of this security and pay fees to Ethereum for this opportunity. In fact, **mainnet publishing fees have been rising this year, and fees in May reached an all-time high**, largely contributed to by rising transaction costs on the Ethereum L1 (which were up on the back of renewed meme coin mania, especially \$PEPE).

Figure 5: Ethereum L2 mainnet publishing fees in May were over five times higher than in January



Source: The Block Data, Binance Research, as of June 14, 2023

Figures 4 and 5 show us that the business of selling security to other applications can be a meaningful value accrual and revenue generation mechanism for L1s. As such, it is not surprising that this business model has gained traction. In fact, a slightly different but closely related method of borrowing Ethereum’s security has slowly become part of the conversation in recent months. Enter **restaking**.

A closer look at restaking

The problem that restaking seeks to solve is that of **fragmented blockchain security**. At a basic level, every time a builder wants to create a decentralized network, they need to establish some form of crypto-economic security. In the Ethereum network, for example, this is created through the staking of \$ETH tokens. However, it can be incredibly inefficient for other services to follow suit. **To establish a new PoS network, for example, there are significant capital costs. Let's say the project issues a token to fulfill this security function; they would then have to convince network participants to take on the price risk of staking this new token as well as the opportunity cost when compared to simply staking \$ETH instead.** Additionally, **generating sufficient security can be a time-consuming process. Even then, the security one can generate is likely to be inferior to that of Ethereum itself.** What this often results in is that many projects, which do not necessarily need to issue their own token, are forced to do so while painstakingly and slowly attempting to create their own crypto-economic security. **Restaking seeks to solve this problem by pooling Ethereum's security and making it available for other applications to utilize.**

Project in focus: EigenLayer

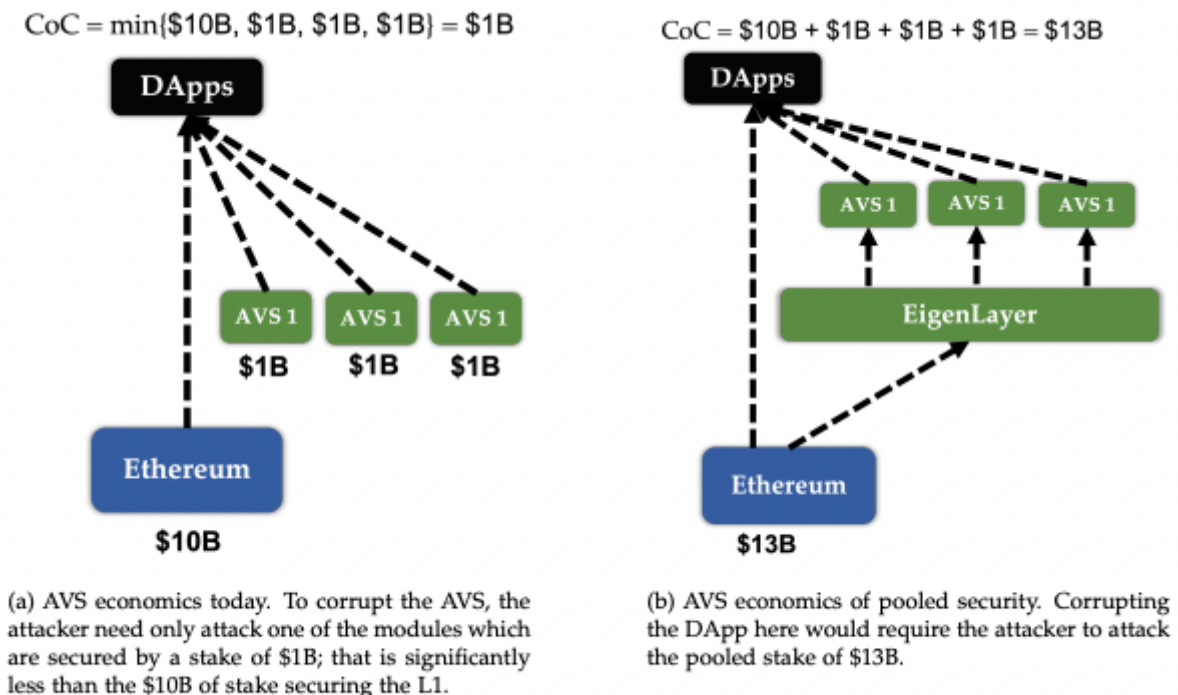
EigenLayer calls itself a “**restaking collection for Ethereum**”⁽⁴⁾ and aims to create a marketplace for decentralized trust. It is a new project in the crypto space and allows **Ethereum stakers to repurpose their staked \$ETH to secure other applications** built on the network. Stakers can choose additional services to secure via their staked \$ETH and earn revenue from doing so. In return, they **agree to grant EigenLayer additional slashing rights on their staked \$ETH** (on top of the slashing rights on the base Ethereum L1 staking contract). Essentially, EigenLayer is a set of smart contracts allowing staked \$ETH to provide security to applications beyond just Ethereum. It thus extends Ethereum's base layer security to services built on top of it. EigenLayer refers to these services as actively validated services (“AVS”).

❖ Mechanism:

- EigenLayer introduces **two novel ideas**: pooled security via restaking and free-market governance.
 - **Pooled security via restaking**: EigenLayer enables pooled security by enabling protocols to be secured by restaked \$ETH rather than their own tokens. This is done through an opt-in process, whereby validators agree to new slashing conditions
 - (incentivizing them to act honestly) while earning revenue in exchange for providing their services. The result is a pooling of Ethereum's very strong crypto-economic security among other protocols built on top of it.

- **Free-market governance:** EigenLayer provides an open market mechanism that allows validators to determine their own risk/reward trade-off and choose which protocols to provide security to. EigenLayer sees this as akin to the service that venture capital firms provide, whereby their backing is essential to innovation but the profit comes at a risk (the risk of slashing in this case).
- Together, these create an **open and competitive marketplace** where validators can sell pooled security while protocols can buy it for a price. This removes the significant capital cost of bootstrapping a new security model, as protocols can just purchase it. It also helps create a **flywheel** whereby the more valuable the protocols created via EigenLayer, the higher the returns for \$ETH stakers, leading to a higher value of \$ETH and thus better Ethereum security, which in turn creates better security for each EigenLayer project, further incentivizing users to create new projects on it.

Figure 6: An illustration of the pooled security model of EigenLayer



Source: EigenLayer whitepaper

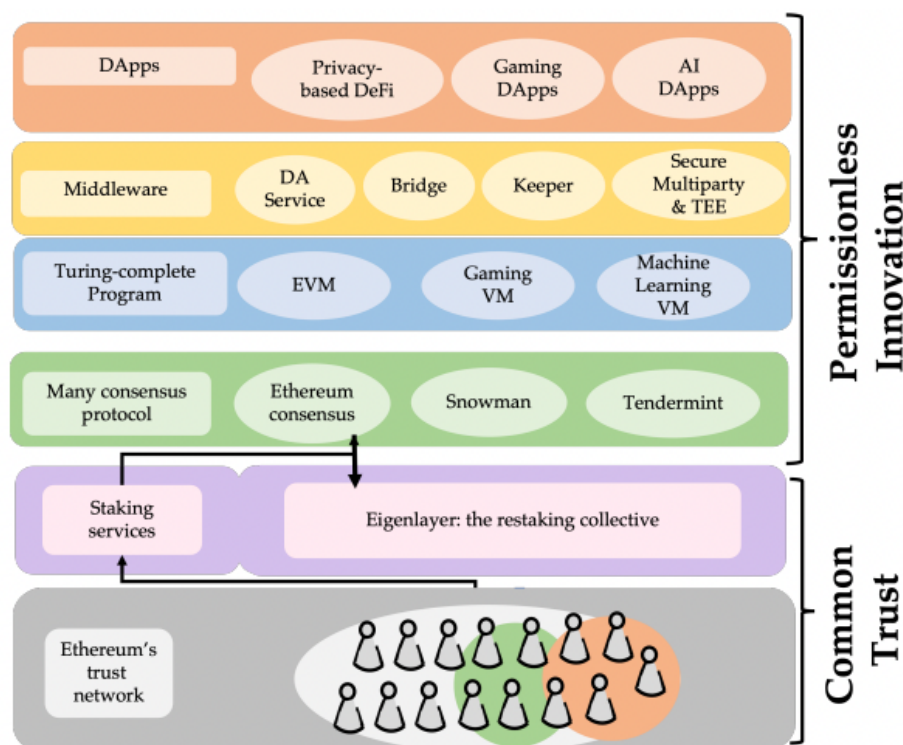
❖ **Use cases and opportunities:**

- The set of possibilities enabled by EigenLayer is rather broad and can encompass all sorts of protocols, from Ethereum sidechains to middleware and modular layers. Nonetheless, the **most relevant protocols are likely those where bootstrapping security is most difficult and those with some**

level of synergy between them and Ethereum. It is also worth noting that restaking is available for both natively staked \$ETH and liquid staking tokens like \$stETH, \$rETH, etc.

- **EigenDA:** This is EigenLayer’s first product and is a **data availability** (“DA”) solution for Ethereum. As briefly described in [Setting the Scene: Monolithic vs. Modular](#), this is part of a blockchain that ensures all transaction data is available for network participants to view and thus allows them to verify it and trust the network. Ethereum has a native DA layer, and others such as Celestia and Polygon Avail are also working on their solutions. EigenLayer founder Sreeram Kannan has previously mentioned that they are **aiming for around 10 MB/s of throughput with their solution⁽⁵⁾ compared to 80 KB/s for Ethereum, a roughly 125x improvement.** One advantage that EigenDA might have over competing solutions is that their use of existing \$ETH validators and stakers means that there is no need to bootstrap a new set of validators or a new token. **EigenDA also allows for dual staking**, which can essentially add two layers of security: one general to the L1 and one specific to any project that decides to use EigenDA. The L2 project, Mantle, has recently [outlined](#) its plans to use EigenDA for DA.
- **MEV-Boost with EigenLayer:** Maximum extractable value (“MEV”) refers to the value that can be extracted from ordering transactions in particular ways (in the block building process). Block builders can sometimes front-run users, often leading to “bad” MEV. To combat this, Flashbots designed a mechanism called MEV-Boost. However, in its current form, MEV-Boost only features full block building, which leads to limitations in centralization and security. A solution using EigenLayer, which features a partial block MEV-Boost, has been proposed, which could help increase decentralization and censorship resistance. More technical details can be found [here](#).
- A secure **blockchain messaging service** with an interoperability protocol called **Hyperlane** has also been [proposed](#).

Figure 7: The potential for permissionless innovation with EigenLayer



Source: EigenLayer whitepaper

❖ **Risks:**

- One risk to consider is that of **validators colluding to attack a set of EigenLayer protocols simultaneously**. This risk can arise because validators may choose to restake multiple times for multiple different services, which could theoretically make an attack economically feasible. The EigenLayer [whitepaper](#) discusses this in more detail and proposes the solution of an open-source dashboard that monitors validator restaking and could allow protocols to incentivize those validators that are only participating in a limited number of protocols.
- The risk of **unintended slashing** is also worth considering. This could be a result of a programming bug or any number of smart contract security issues in protocols that are built on top of EigenLayer. Two solutions are proposed to combat this: (1) **security audits**; and (2) a **governance layer that can veto slashing** decisions via multisig (although this may raise some centralization concerns).
- **Protocol sustainability** is also a risk for the adoption of EigenLayer. Tokens can provide useful monetary incentives and revenue for protocols, and if all value is now accruing towards \$ETH instead of protocol-native tokens, it may be difficult for certain projects to thrive and develop in the long term.






- Finally, referring to Vitalik Buterin's recent blog post, "[Don't overload Ethereum's consensus](#)," there are potential risks in building complicated financial systems on top of restaking. If these systems spiral out of control and significant monetary value is lost, **some in the community might expect an Ethereum hard fork** to fix these errors. **Vitalik argues that any such expectations should be resisted, and it should be understood that Ethereum cannot be held accountable for any application-level mishaps.** This might limit the types of protocols that are able to launch on EigenLayer and might drive some towards other platforms. That said, EigenLayer founder Sreeram did respond⁽⁶⁾ in a constructive manner, stating that EigenLayer's underlying thought process is consistent with Vitalik's.

❖ **Next Steps:**

- On June 14, EigenLayer launched their Stage 1 Mainnet⁽⁷⁾. This is the **first of three stages before a complete launch** and EigenLayer's initial functionality is similar to what has been accessible in testnet since April. At this current stage there are **restaking limits**, namely, 3,200 tokens for each supported liquid staking asset (Lido stETH, Rocket Pool rETH and Coinbase Wrapped cbETH) and 9,600 native \$ETH. Many more liquid staking tokens are set to be supported in the future. There is also a 7-day withdrawal delay to serve as a security measure for the time being.

Cosmos and its application-specific blockchain (“appchain”) thesis have steadily gained traction over the last year. As a brief overview, the **Cosmos ecosystem is centered around the Cosmos Hub, which is an appchain secured by the \$ATOM token**. A number of other appchains, referred to as “Zones,” are connected to the Cosmos Hub and use the **Inter-Blockchain Communication** (“IBC”) protocol to communicate and transfer data between one another. A “Hub” is essentially a Zone that facilitates communication with multiple other Zones. While the Cosmos Hub is the first and largest of its kind, other contenders such as Osmosis, Axelar, and Evmos have also begun to emerge. At the time of writing this report, there are 59 IBC-enabled Zones in the Cosmos ecosystem, with a market cap of over US\$9B.

Figure 8: On-chain activity of the top five Cosmos appchains from the last 30 days

Logo	Name	IBC Volumes (US\$M)	Total Txns (M)	Monthly Active Users (K)
	Osmosis	293.5	2.7	134.9
	Stride	248.9	2.0	34.7
	Cosmos Hub	159.6	1.3	228.9
	Axelar	88.1	9.0	7.9
	Secret Network	55.5	0.4	25.1

Source: mapofzones.com, as of June 7, 2023

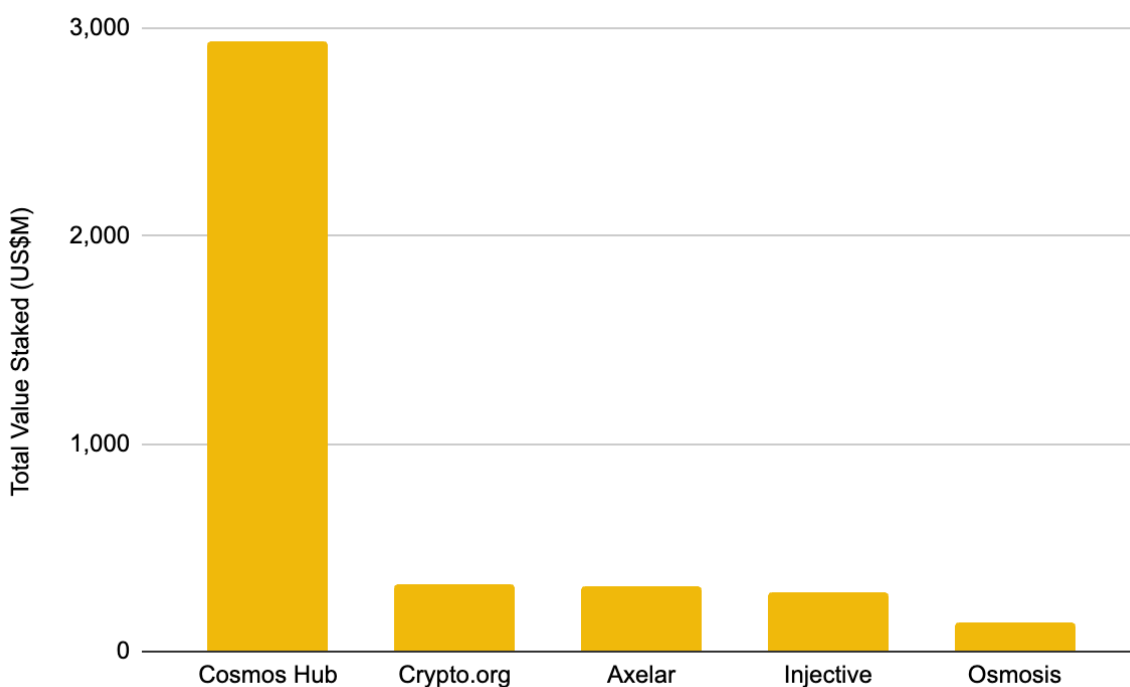
While the Cosmos ecosystem has helped birth major projects like Osmosis and attracted others to migrate (dYdX being the most notable example⁽⁸⁾), growth is still slower than many in the community would like to see. On top of this, many have seen the increasing dominance of Ethereum L2 rollups as being majorly competitive to Cosmos appchains, and some have felt that Cosmos might be falling behind. **One of the key issues that Cosmos appchains face is the responsibility of bootstrapping a sufficiently staked and decentralized validator set.** To this end, all Cosmos Zones have issued their own tokens, to varying degrees of success. For new appchains with a low token price and relatively limited

staking, this is a difficult bottleneck to surpass and has impacted the attractiveness of these projects (and made them potential attack targets given the relatively weak crypto-economic security). This is where **Replicated Security** (previously Interchain Security V1) comes in.

Replicated Security

Replicated Security is the first feature of Cosmos’ Interchain Security Model. Recently approved with overwhelming support (over 99%⁽⁹⁾) from the community, this feature allows the **Cosmos Hub (referred to as a “provider chain”) to lend its security to other blockchains (referred to as “consumer chains”) in return for fees**. This essentially means that new Cosmos appchains can be launched and utilize the security of the Cosmos Hub while avoiding the expensive and painstaking work of bootstrapping and maintaining their own validator sets. To make it clear, this arrangement would mean that in order to attack a consumer chain, you would have to gain control of the Cosmos Hub itself. In other words, the consumer chain completely inherits the security of the provider chain.

Figure 9: The Cosmos Hub is by far the most crypto-economically secure appchain in the Cosmos network and thus an ideal provider chain due to the high cost of attack



Source: mapofzones.com, as of June 8, 2023

Key Features

- ❖ **Role of governance:**

- To launch as a Replicated Security Cosmos appchain, a project must **first be approved by \$ATOM holders** following a detailed governance proposal.
- Afterward, the **project must be approved by Cosmos Hub's active validators**, which are currently fixed at 175. A minimum of $\frac{2}{3}$ of the validator set must approve the chain for it to pass.

❖ **Role of Cosmos Hub validators:**

- Once a consumer chain is approved to join the network, the **entire Cosmos Hub validator set must validate blocks for the consumer chain**.
- Validators cannot opt in or out, and any downtime in validating the consumer chain's blocks will carry the same slashing penalties as they would for validating the Cosmos Hub.

❖ **Consumer chain economics:**

- In order to incentivize Cosmos Hub validators, **consumer chains will often negotiate a revenue sharing agreement** with them. This can include **transaction fees** (currently set at 25%, but they can be increased and are subject to governance), **application fees** (e.g., MEV, swap fees, etc.), as well as **token inflation** (if the consumer chain has their own native token).

❖ **Centralization concerns:**

- As mentioned above, all 175 members of the Cosmos Hub validator set are required to start validating blocks for any approved consumer chains. This **requires validators to run extra nodes and additional machines, thus creating additional hardware and labor costs**. While this might not be an issue for larger validators, it could be a significant burden for smaller parties, especially if the number of consumer chains increases.
- It has been **estimated by community members that roughly 10% of the validator set already operates at a loss⁽¹⁰⁾**. Assuming that adding another node to validate a new consumer chain would double their expenses, more of the group would become unprofitable. Even if the expenses do not double, the fact that all Cosmos Hub validators must validate consumer chain blocks will affect profit margins across the board. Given that **this will be most harmful to smaller validators, some could drop out, leaving only the largest validators on the chain**. This is a potentially **centralizing force and could impact the ability of Replicated Security to scale effectively**.

Project in focus: Neutron

Neutron is a **general-purpose, permissionless smart contract platform** built on top of Cosmos. Notably, Neutron is the **first project to utilize Replicated Security** and be launched on the Cosmos Hub as a consumer chain.

❖ Revenue sharing:

- In exchange for providing security to Neutron, the **Cosmos Hub will receive 25% of its transaction fees and 25% of its MEV revenue**. MEV revenue will be denominated in their native \$NTRN token, while transaction fees will be a mix of \$ATOM and \$NTRN.
- **Neutron also airdropped 7% of the total \$NTRN supply** (equivalent to 58.3% of its initial circulating supply) to Cosmos Hub stakers, with any unclaimed airdrop to be sent to the Cosmos Hub community pool.

❖ Use cases:

- Neutron sees cross-chain **DeFi** as a major initial use case. Through leveraging Cosmos Interchain Accounts (“ICA”) and Interchain Queries (“ICQ”) from launch⁽¹¹⁾, **applications that deploy on Neutron can retrieve data from other IBC-enabled chains in a trustless and permissionless manner**. This is a powerful combination and could allow frictionless cross-chain DeFi to permeate within the Cosmos ecosystem.
- The relatively low crypto-economic security across various Cosmos appchains has thus far prevented large-scale DeFi projects from occurring, as it limits the amount of funds that users are comfortable deploying. This can change with Neutron, given that it leverages the security of the well-capitalized Cosmos Hub.
- Because Neutron provides a permissionless smart-contract environment that is secured by the Cosmos Hub, projects can launch on top of it and benefit from high levels of security without launching as a separate appchain. Instead of worrying about incentivizing a validator set (if they were to launch as an appchain) or creating additional cost burdens on Hub validators (if they were to launch as a consumer chain), projects can launch as smart-contracts on top of Neutron and gain all the benefits of Replicated Security and cross-chain compatibility without incurring additional costs for Cosmos Hub validators or themselves. This level of **vertical scaling** makes Neutron a powerful and suitable project to be the first partner for Cosmos Hub in its launch of Replicated Security.

“Instead of worrying about incentivizing a validator set (if they were to launch as an appchain) or creating additional cost burdens on Hub validators (if they were to launch as a consumer chain), projects can launch as smart-contracts on top of Neutron and gain all the benefits of Replicated Security and cross-chain compatibility without incurring additional costs for Cosmos Hub validators or themselves.”

❖ **Response to centralization concerns:**

- To reduce the financial burden of running an extra node to validate Neutron's blocks, Neutron announced plans to offer a **soft opt-out for the bottom 5% of the active Cosmos Hub validator set** (around 74 validators at the time of writing). The feature will allow the **bottom 5% of validators to avoid penalization for "opting out" of running nodes for Neutron while still allowing them to continue receiving their share of the rewards as outlined in the revenue sharing agreement** above.
- This may be a **more sustainable solution for smaller validators' operations** while still maintaining sufficient security for Neutron (95% of the validator set will still have to validate Neutron blocks). However, it does mean that **Neutron's liveness will be compromised**, which could lead to more difficult chain upgrades or increased risks of chain halts (as around 5% of the network could be offline at any given time).

❖ **Who has already launched?**

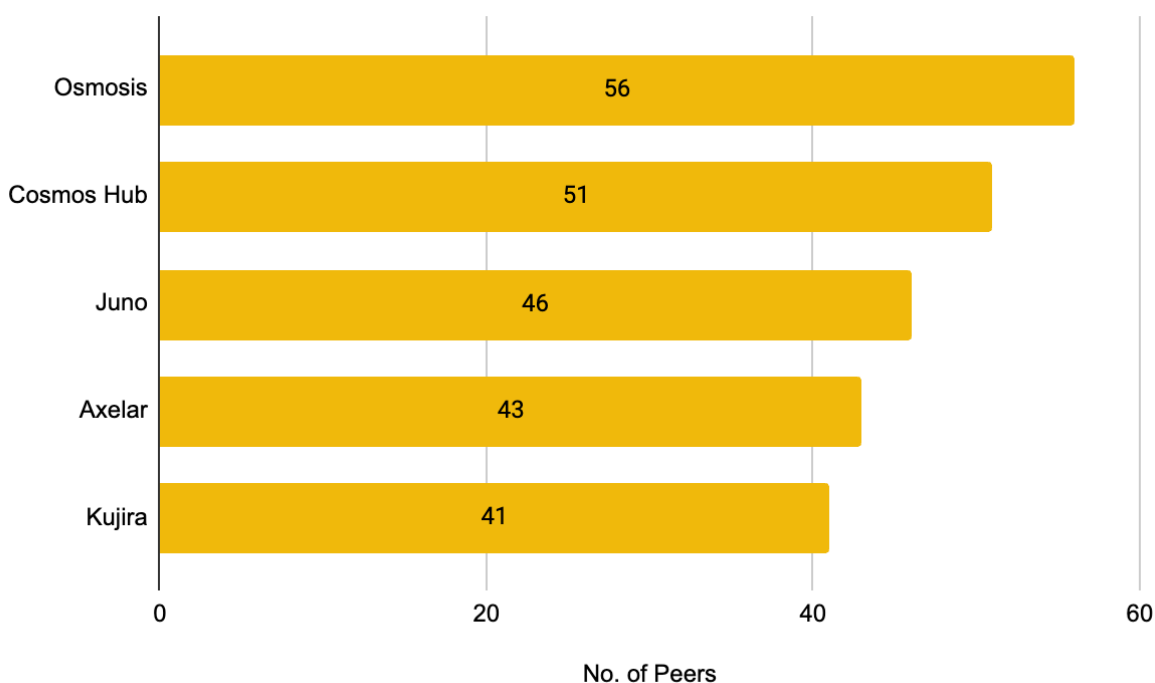
- Even before Neutron went to the mainnet in early May, a number of dApps expressed interest in launching on top of it.
- Astroport became the first decentralized exchange ("DEX") to launch on Neutron in early June⁽¹²⁾. Catalyst, which enables cross-chain swaps, is also set to launch on Neutron⁽¹³⁾ in the coming weeks.
- Mars Protocol is set to launch Red Bank⁽¹⁴⁾, an advanced cross-chain credit protocol, on Neutron in the near future. Apollo DAO, a DeFi aggregator for yield optimization, is also set to follow suit⁽¹⁵⁾. Perhaps most notably, liquid staking giant **Lido expressed interest as early as September 2022 in launching on Neutron**⁽¹⁶⁾ and it is heavily rumored to do so, though we have yet to hear any recent updates on the matter.

Osmosis and Mesh Security

Osmosis, an appchain in the Cosmos ecosystem that is based on automated market makers ("AMMs"), is also working on another shared security solution similar to Replicated Security.

Before explaining further, we should note that **Osmosis** is not an ordinary appchain in the ecosystem. It has **consistently topped IBC volumes** (as shown in Figure 8) and is the **most-connected among all other chains** (even more than the Cosmos Hub itself).

Figure 10: Osmosis has the most direct connections to other Zones in the Cosmos ecosystem



Source: mapofzones.com, as of June 8, 2023

The solution that the Osmosis Grants Program (“OGP”) is working on with Axelar, the Akash Network, the Osmosis Foundation, and the ATOM Accelerator is called **Mesh Security**. The development of Mesh Security will be bottom-up, and it will be developed as a public good by teams from across the Cosmos ecosystem.

❖ **What is Mesh Security?**

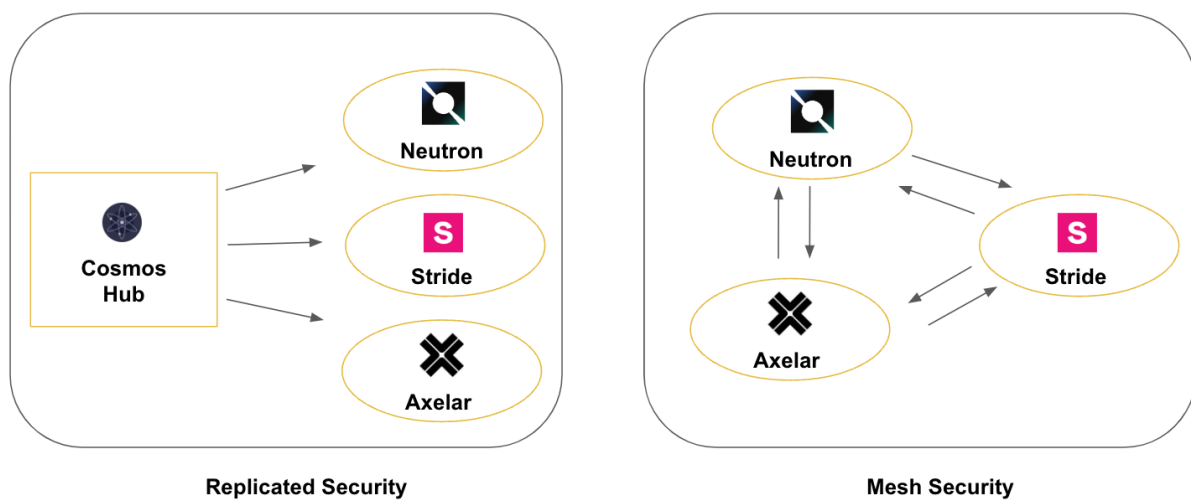
- Mesh Security allows **token delegators (not validators) with staked tokens on one Cosmos chain to restake them on another partner chain.**
- If the validator they have chosen to restake with on the partner chain misbehaves, the staked tokens get slashed on both chains. In return for this risk, token delegators receive staking rewards.

❖ **How does this differ from Replicated Security?**

- With Replicated Security, security flows unilaterally, i.e., from the provider chain down to the consumer chain. With **Mesh Security, security can flow bidirectionally or multilaterally** as different appchains can combine their market caps for security.
- In the Replicated Security model, validators are required to run additional nodes to validate the blocks of the consumer chain. There is **no such validator requirement in the Mesh Security model, which is simply focused on token delegators**, i.e., stakers.

- Replicated Security targets early-stage projects that do not necessarily want to bootstrap or maintain their own validator set and are happy to rely entirely on the Cosmos Hub validator set. Contrarily, **Mesh Security targets appchains that already have a sufficiently capitalized validator set but want to enhance their level of economic security and strengthen their bonds with other chains in the ecosystem.** For this reason, the group behind Mesh Security sees it as complementary rather than competing with Replicated Security. In fact, they even posit⁽¹⁷⁾ that as appchains utilizing Replicated Security reach higher levels of maturity, they can look to transition to the Mesh Security model.

Figure 11: While Replicated Security uses a hub-and-spoke, unilateral security model, Mesh Security is more focused on bilateral or multilateral security



Source: Binance Research

❖ **Potential benefits for the Cosmos ecosystem:**

- First and foremost, **Mesh Security would increase crypto-economic security** across the board while **still allowing appchains to retain their sovereignty.** Many Cosmos appchains already have a level of shared economic dependency, and Mesh Security will help to support these relationships from a security perspective.
- While focused on bilateral and multilateral security, **Mesh Security also allows for unidirectional relationships** (similar to Replicated Security). Larger chains can “underwrite” new chains by running a validator for them, allowing them to be completely secured by the restaked tokens of an appchain with a higher market cap. Notably, this **can be done without governance approval from the provider chain**, which is different from the Replicated Security model.
- Increased utility: There are **cases where a service is best run through multilateral security**, i.e., a name service protocol might be best served in

the form of a consumer chain that is secured by all other appchains in the “mesh”, rather than controlled by the validators of just one appchain.

❖ **Timeline:**

- Mesh Security is set to be completed in **three phases** lasting approximately **three months each**.
- With the initial announcement on May 18, 2023, we would imagine the earliest we could expect to see a mainnet launch would be sometime in early 2024.

It will be interesting to monitor how Replicated Security progresses following the launch of Neutron and with others like the liquid staking protocol Stride, which is planning⁽¹⁸⁾ to launch later this year. Whether Mesh Security is truly complementary or becomes competitive will also be a key story to follow as we enter 2024.

6 Bitcoin

With a market capitalization of over US\$500B in our current market (more than twice as large as the second largest crypto asset, Ethereum), Bitcoin remains the de facto king of crypto. Regarding decentralization, Bitcoin boasts over 17K nodes⁽¹⁹⁾, compared to just over 9K for Ethereum⁽²⁰⁾. While this is just one aspect to consider when analyzing decentralization, it is something to note. Combining these facts with the theoretical cost of a 51% attack on Bitcoin of over US\$1M per hour⁽²¹⁾, we can understand why the usage of Bitcoin as a security layer has long been discussed and deliberated in the community.

Project in focus: Babylon

Babylon is a Cosmos project that aims to **leverage the security of Bitcoin to enhance the security of Cosmos appchains and other PoS chains**. The key feature of Bitcoin that Babylon seeks to use is its **timestamping**. Bitcoin solves the [double-spend problem](#) by timestamping transactions and then distributing them to form the basis of PoW consensus. These timestamps provide an irreversible chronological record of transactions and can thus help settle any security issues on the chain.

Bitcoin can also be used to timestamp events from other chains in a process called **checkpointing**. The transactions that timestamp these events are then referred to as **checkpoints**. The Babylon Chain uses this feature and periodically records the checkpoints of other PoS networks on the Bitcoin blockchain, which helps provide a layer of security for transactions. If an attacker attempted to corrupt a PoS network that utilizes Babylon Chain, they would have to attack the Bitcoin blockchain itself, essentially creating Bitcoin-equivalent security for these chains. Babylon is starting its journey focusing on Cosmos Zones but hopes to expand onto all types of PoS chains.

Figure 12: Babylon Chain utilizes the timestamp feature of Bitcoin to help secure other chains

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

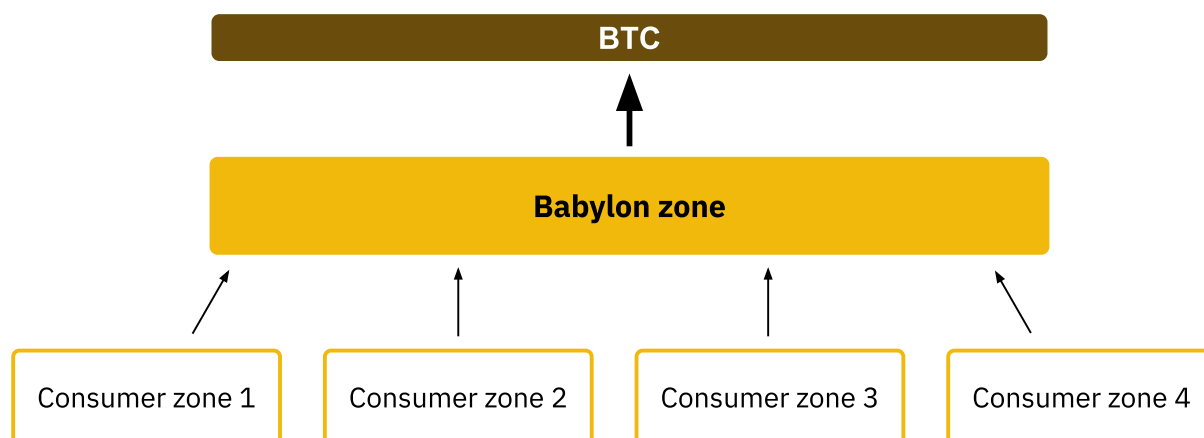
Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network **timestamps** transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Source: Bitcoin whitepaper

❖ How does it work?

- Babylon uses a **three-part architecture**: (1) Bitcoin, as the timestamping service; (2) the Babylon Chain, a Cosmos Zone, as the middle layer and aggregator; and (3) other Cosmos Zones, as the consumers of security.
- **Checkpoints from participating Zones are sent to the Babylon Chain via IBC.** Babylon Chain aggregates these so that only one checkpoint stream must be put onto Bitcoin to timestamp transactions from all the different Zones simultaneously.
- This **aggregated checkpoint is then sent to Bitcoin.** The finality of the Bitcoin network is usually considered to be around six blocks (taking about an hour), after which the transactions included in the aggregated checkpoint can be considered protected via the full security of Bitcoin. In return, the participating Cosmos Zones obtain Bitcoin timestamps with validity proofs from Babylon Chain.
- Participating validators can also **download Babylon Chain blocks to verify all the checkpoints** and ensure that Babylon validators behaved honestly.

Figure 13: Babylon Chain architecture



Source: Babylon Chain Blog, Binance Research

❖ **Use cases:**

- **Faster unbonding periods:** Due to the characteristics of PoS chains, specifically the potential for so-called long-range attacks⁽²²⁾, the withdrawals of a user's staked tokens, i.e., the unbonding period, can often take days or even weeks. Liquid staking is one solution that has emerged to alleviate this issue, although it comes with its own risks. PoS networks that utilize Babylon to post checkpoints to Bitcoin can reduce this period from weeks to just a few hours. Technical details can be found [here](#).
- **Bootstrapping new Zones:** For those Zones that have limited appetite to maintain their own validator set or are struggling to do so because of low token valuations, using Babylon can be an effective way to use Bitcoin to secure their chain (similar to the arguments presented in the [Cosmos](#) section).
- **Increase censorship resistance:** While Cosmos Zones may be vulnerable to censorship of transactions if malicious nodes control over one-third of the total stake, Babylon Chain allows these transactions to still be timestamped to Bitcoin. While we will abstract from the technical details, this essentially raises the lower limit of censorship from 34% to 51%⁽²³⁾.
- **Benefits of slow finality:** While PoS chains usually have slow unbonding periods for their stake, they tend to have extremely fast finality of transactions. On the contrary, Bitcoin transactions have much quicker unbonding but slower finality (usually considered to be around six blocks, i.e., an hour). Babylon Chain can turn this slow finality into an advantage by allowing PoS chains to leverage the complete security of the Bitcoin network⁽²⁴⁾. Essentially, clients of the PoS chain can wait until the timestamp of the PoS block is many blocks deep inside the Bitcoin chain before confirming the finality of the transaction. This can preserve the safety of high-value transactions using Bitcoin's security, even if the PoS chain has a

relatively low token valuation or low crypto-economic security.

❖ **Risks:**

- A key point to remember is that the Babylon Chain helps record checkpoints for **past blocks** in the Bitcoin chain, protecting them with the robust security of Bitcoin. New blocks are still dependent on the validators of each individual PoS network, and neither Babylon Chain nor Bitcoin can take responsibility for protecting these blocks.
- Although still in its testnet stage, there is likely to be at least some level of centralization in the Babylon Chain architecture. This aspect should be carefully monitored and considered as we approach a mainnet.

❖ **Integrations and timeline:**

- Babylon has already integrated with 28 chains, with a total market cap of over US\$1.5B⁽²⁵⁾. These include the majority of top Cosmos appchains, such as Osmosis, Injective, Akash, Juno, Secret Network, Evmos, Stride, Sei, and many more.
- Babylon's testnet went live in March. They plan on releasing another testnet in the summer before a mainnet launch near the end of the year.

Given the hybrid model of Babylon, which combines PoS and PoW and then adds IBC for communication, we can view it as seeking to **leverage the best parts of Ethereum, Bitcoin, and Cosmos**. It is a promising new approach to blockchain design and relies on key features from existing platforms. It will be interesting to monitor how this approach performs with their current Cosmos cohort and whether the team can successfully branch out to include other PoS networks.

Project in focus: Stacks

Stacks sees itself as a Bitcoin layer and is essentially a **blockchain that seeks to function as a secondary layer for Bitcoin smart contracts**. Stacks uses the \$STX token for transaction fees and to incentivize miners of Stacks blocks. Additionally, it relies on a novel **Proof of Transfer** ("PoX") consensus mechanism.

❖ **Proof of Transfer ("PoX")**

- PoX seeks to **reuse the work that has already been done by Bitcoin miners** for their PoW consensus and use it to secure Stacks.
- On one side, PoX miners bid for blocks using (previously mined) \$BTC, and the winner is rewarded in \$STX as a block reward. The winning miner has then earned the right to commit a new block to the Stacks blockchain.
- On the other side, "stackers" (i.e., stakers) can stake their \$STX to participate in the PoX consensus and earn \$BTC rewards for their services.

- In this way, PoX reuses the work done by Bitcoin miners, does not consume significant energy, and can pay \$BTC rewards to \$STX stakers.

❖ **How does it use Bitcoin security?**

- Hashes of all Stacks layer smart contracts and transactions are recorded and settled on the Bitcoin blockchain. This process is how Stacks records its history to the Bitcoin chain, thus inheriting its security.

❖ **What is next?**

- Q4 2023 will bring the Stacks Nakamoto Release, enabling two key features: sBTC and greater Bitcoin finality⁽²⁶⁾.
 - sBTC: This will introduce a trust-minimized, non-custodial two-way peg system allowing users to “bridge” \$BTC from L1 into sBTC on the Stacks layer. Users will be able to send \$BTC to a multi-sig wallet on the L1 (controlled by a decentralized group of “stackers” who have locked up their STX to secure the Stacks chain) and mint an equivalent amount of sBTC on Stacks. This sBTC can then be used for DeFi, NFTs, and more.
 - Greater Bitcoin finality: Following the Nakamoto Release, 100% of Bitcoin security will determine finality on the Stacks layer. Practically, this means that to reverse transactions on the Stacks chain, attackers must target Bitcoin, which is an extremely expensive and logistically difficult process. This will add another level of security to Stacks transactions.

❖ **Projects on Stacks**

- Since their 2021 mainnet launch, numerous projects⁽²⁷⁾ have launched on top of Stacks, including Bitcoin Name System (“BNS”), Alex, Hiro Wallet, etc.
- With the Nakamoto Release improving security and adding a decentralized method to access Bitcoin capital on L2, we look forward to seeing who else will look to build or deploy on Stacks.

Closing Thoughts

L1s are constantly searching for methods to meaningfully accrue value, while smaller projects continue to have trouble incentivizing and maintaining an effective and decentralized validator set. The launch and success of Ethereum L2s have shown that selling security can become a top revenue source for L1s. As such, other chains have taken notice and entered the race.

Cosmos is a notable example, having pivoted to providing security for appchains in exchange for fees to accrue value to its ecosystem and the \$ATOM token. Osmosis has also noticed and evidently wants a piece of the pie through its Mesh Security initiative. The use of Bitcoin to secure other chains is an older story that has yet to take off in a significant way, although Babylon and Stacks are bringing new innovations that might supercharge this market too.

We are still in the exploration phase of security as a primary source of value accrual for L1s, and this is likely to become a monopolistic market. The most decentralized and largest blockchain will be most difficult to attack, and this will likely be the most attractive security layer. Higher demand for a blockchain to provide security will increase the value of its native token, further drawing in validators to help maintain the network and get a share of its fee market. This, in turn, should lead to further decentralization, thereby starting a flywheel. As they say, liquidity begets liquidity.

References

1. <https://vitalik.ca/general/2021/12/06/endgame.html>
2. <https://ethereum.org/en/staking/>
3. <https://coinmarketcap.com/>
4. <https://docs.eigenlayer.xyz/overview/whitepaper>
5. https://mirror.xyz/0xmantle.eth/me_Moy37CCvreI38AGGDmXX_W8s8i0iTHCqE7W61LL8
6. <https://twitter.com/sreeramkannan/status/1660388931622563840?s=20>
7. <https://www.blog.eigenlayer.xyz/eigenlayer-stage-1-mainnet-launch/>
8. <https://dydx.exchange/blog/dydx-chain>
9. <https://www.mintscan.io/cosmos/proposals/187?ref=hackernoon.com>
10. <https://twitter.com/0xSpaydh/status/1641942728459292672?s=20>
11. <https://neutron.org/#accord>
12. https://twitter.com/Neutron_org/status/1665713435902877697?s=20
13. https://twitter.com/Neutron_org/status/1658140120149639175?s=20
14. https://twitter.com/Neutron_org/status/1664404979153616900?s=20
15. <https://www.mintscan.io/neutron/ecosystem>
16. <https://research.lido.fi/t/lido-for-the-interchain/2886>
17. <https://osmosis.zone/blog/mesh-security-initiative-announcement>
18. <https://stride.zone/blog/strides-2023-roadmap>
19. <https://bitnodes.io/>
20. <https://etherscan.io/nodetracker>
21. <https://www.crypto51.app/>
22. <https://www.babylonchain.io/blogs/why-is-stake-unbonding-so-slow>
23. <https://www.babylonchain.io/blogs/censorship-resistance-via-babylon>
24. <https://www.babylonchain.io/blogs/bitcoin-security-beyond-unbonding>
25. <https://babylonscan.io/>
26. <https://stx.is/sbtc-pdf>
27. <https://docs.stacks.co/docs/category/services-using-stacks>

Latest Binance Research Reports



Monthly Market Insights - June 2023

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



The zkEVM World: An Overview of zkSync

A closer look at zkSync and the growing zkEVM ecosystem



Institutional Custody in Crypto

A detailed study of the institutional custody landscape



BRC-20 Tokens: A Primer

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

About Binance Research

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



Shivam Sharma

Macro Researcher

Shivam is currently working for Binance as a macro researcher. Prior to joining Binance, he worked as an investment banking associate and analyst at Bank of America on the Debt Capital Markets desk, specializing in European financial institutions. Shivam holds a BSc in Economics degree from the London School of Economics & Political Science (“LSE”) and has been involved in the cryptocurrency space since 2017.

Resources



Read more [here](#)



Share your feedback [here](#)

General Disclosure: This material is prepared by Binance Research and is not intended to be relied upon as a forecast or investment advice and is not a recommendation, offer, or solicitation to buy or sell any securities or cryptocurrencies or to adopt any investment strategy. The use of terminology and the views expressed are intended to promote understanding and the responsible development of the sector and should not be interpreted as definitive legal views or those of Binance. The opinions expressed are as of the date shown above and are the opinions of the writer; they may change as subsequent conditions vary. The information and opinions contained in this material are derived from proprietary and non-proprietary sources deemed by Binance Research to be reliable, are not necessarily all-inclusive, and are not guaranteed as to accuracy. As such, no warranty of accuracy or reliability is given, and no responsibility arising in any other way for errors and omissions (including responsibility to any person by reason of negligence) is accepted by Binance. This material may contain 'forward-looking' information that is not purely historical in nature. Such information may include, among other things, projections and forecasts. There is no guarantee that any forecasts made will come to pass. Reliance upon information in this material is at the sole discretion of the reader. This material is intended for information purposes only and does not constitute investment advice or an offer or solicitation to purchase or sell any securities, cryptocurrencies, or any investment strategy, nor shall any securities or cryptocurrency be offered or sold to any person in any jurisdiction in which an offer, solicitation, purchase or sale would be unlawful under the laws of such jurisdiction. Investment involves risks.