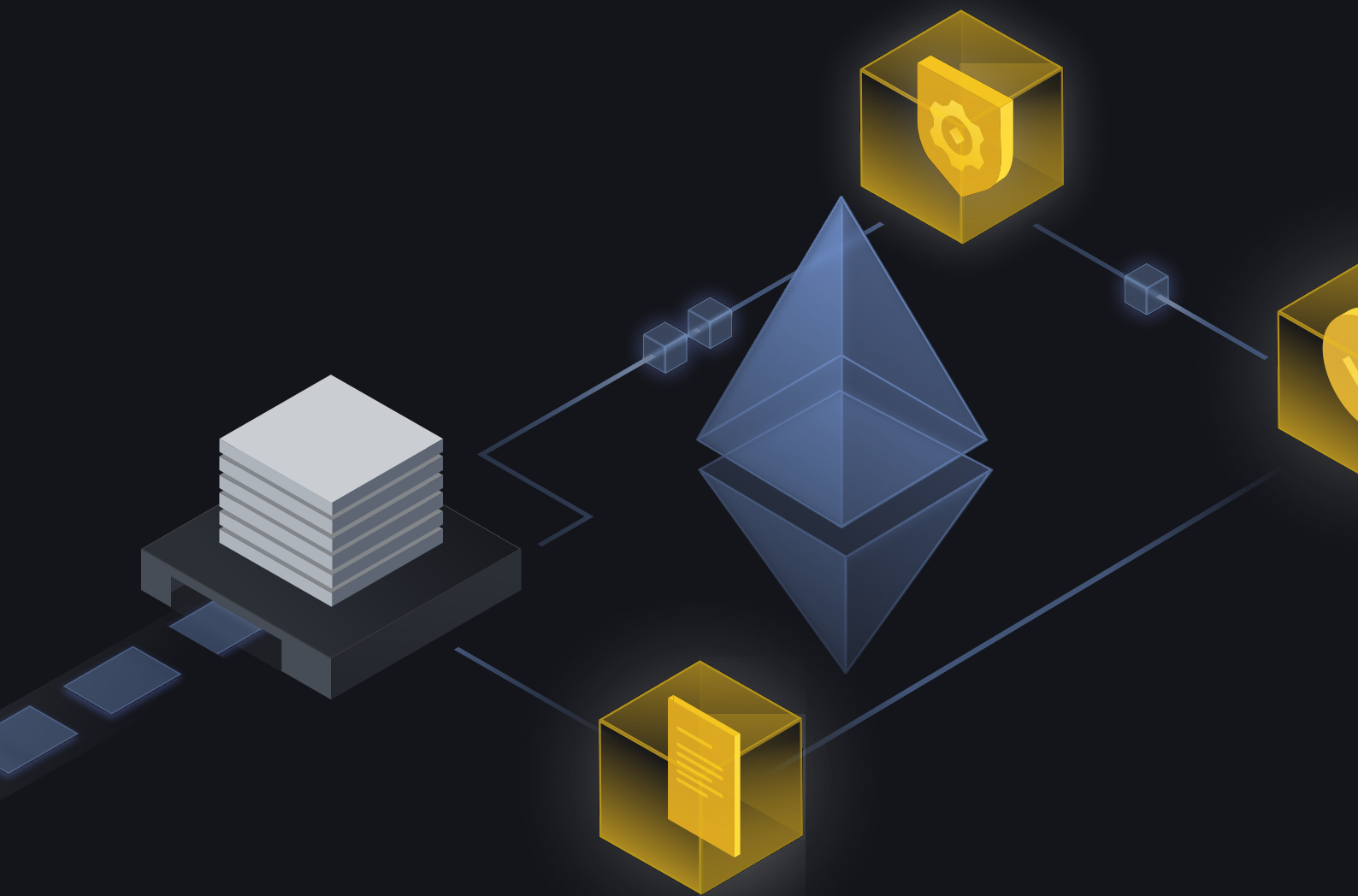


# Ethereum's Rollups are Centralized

**A Look Into  
Decentralized Sequencers**



# Table of Contents

<b>Key Takeaways</b>	<b>2</b>
<b>Introduction</b>	<b>3</b>
<b>What Are Sequencers?</b>	<b>4</b>
Why Rollups Use Sequencers and Why It Is an Issue	5
The Relevance of MEV	6
The Current State of the Sequencer Market	7
Further Issues	8
<b>The Solution: Decentralized, Shared Sequencers</b>	<b>10</b>
Overview	10
Espresso	11
Astria	17
Radius	21
Others	23
<b>Outlook</b>	<b>24</b>
<b>Closing Thoughts</b>	<b>26</b>
<b>References</b>	<b>27</b>
<b>Latest Binance Research Reports</b>	<b>29</b>
<b>About Binance Research</b>	<b>30</b>
<b>Resources</b>	<b>31</b>

## 1

# Key Takeaways

- ❖ Transaction sequencing has become a growing issue in the Layer-2 (“L2”) world. The primary role of an L2 rollup is to provide a secure venue for cheaper transactions. L2 rollups provide execution layers for users and then submit their transaction data to the parent Layer-1 (“L1”), i.e., Ethereum in the case of Arbitrum, Optimism, zkSync, etc.
- ❖ Sequencers are the entities that have been given the right to order these transactions into groups. A sequencer receives unordered transactions from users, processes them into groups off-chain, and generates a compressed batch of ordered transactions. The transactions can then be put into blocks and sent to the parent L1.
- ❖ Rollups do not actually need a sequencer; it is a design choice for a better user experience in the form of cheaper fees and quicker transaction confirmations. For instance, like how most rollups use the Ethereum base layer for data availability, they can also use it for sequencing. However, Ethereum’s base layer is likely to be relatively inefficient and expensive. This has meant that every major L2 rollup project has, so far, found it more convenient, cheaper, and user-friendly to run a centralized sequencer.
- ❖ As the sequencer controls the ordering of transactions, it has the power to censor user transactions (although complete censorship is unlikely as users can submit transactions directly to the L1). The sequencer can also extract the maximal extractable value (“MEV”), which could be economically harmful to the user base. Furthermore, liveness can be a major issue, i.e., if the sole, centralized sequencer goes down, then the entire rollup gets affected.
- ❖ The solution to the problem is shared, decentralized sequencers. Shared sequencers essentially provide decentralization-as-a-service to rollups. In addition to solving the issues of censorship, MEV extraction, and liveness, shared sequencers also introduce cross-rollup composability, unlocking all sorts of new possibilities.
- ❖ Espresso, Astria, and Radius are working on innovative shared sequencing solutions with various unique features in their respective architectures. While Espresso seeks to leverage EigenLayer to bootstrap its network, Astria maintains close ties with the modular data availability network Celestia. Radius brings its unique encrypted mempool to the conversation.

## Introduction

As Ethereum's L2 rollup ecosystem continues to gain popularity, one aspect that is often overlooked is sequencers. Sequencers are responsible for transaction ordering and are utilized by rollups to provide a better user experience with cheaper fees and quicker transaction confirmations. However, the issue is that **all major Ethereum L2 rollups have, so far, found it most convenient, user-friendly, and cheaper to run their own sole, centralized sequencers.** Given the power the sequencer holds in terms of transaction censorship, MEV extraction, and creating a single point of failure (i.e., liveness issues), this could be perceived as an undesirable outcome and not in line with the ethos of crypto.

While **most of these rollups have addressed the decentralization of their respective sequencers and featured it as part of their roadmaps, there is no real consensus on how this is going to occur.** We should also note that Arbitrum and Optimism have both been live with their solutions since late 2021 and are, arguably, yet to make substantial progress on decentralizing their sequencers.

In this report, we take a closer look at the role of sequencers and the current state of the Ethereum rollup space. We then dive into the projects that are working on solutions, namely decentralized, shared sequencing networks. We provide a detailed overview of these projects and the unique parts of their solutions. We also reflect on what this might mean for Ethereum's L2 rollup landscape going forward.

## 3

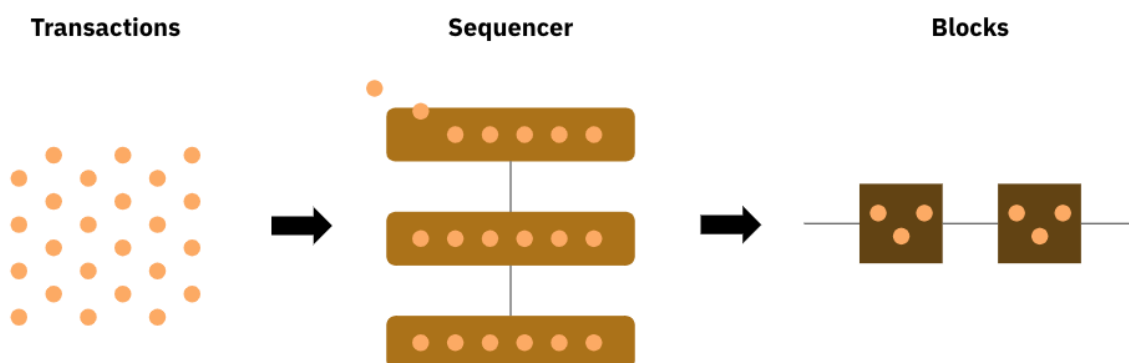
## What Are Sequencers?

Taking a step back, consider that a blockchain is a distributed data ledger consisting of timestamped transaction data ordered by blocks. Initially, this transaction data is unordered and unorganized. After being ordered, i.e., sequenced, it can then be organized into blocks and executed to create the new state of the blockchain. For Layer-1 (“L1”) blockchains like Ethereum, this transaction sequencing occurs on the Ethereum base layer itself.

Moving up a layer to Ethereum’s most popular scalability solutions, **Layer-2 (“L2”) rollups, transaction sequencing has become a growing issue**. Remember, rollups’ primary role is to provide a secure venue for cheaper transactions for users. As an oversimplification, L2 rollups provide execution layers for users and then submit their transaction data to the parent L1, i.e., Ethereum in the case of Arbitrum, Optimism, zkSync, etc. A single batch of transactions submitted to the L1 will typically contain hundreds or thousands of compressed L2 transactions, thereby reducing the cost of sending data to the L1.

In the L2 rollup world, the sequencers are the entities that have been given the right to order transactions into groups. **A sequencer receives unordered transactions from users, processes them into groups off-chain, and generates a compressed batch of ordered transactions**. The transactions can then be put into blocks and sent to the parent L1. The batched transactions are also made available on the data availability (“DA”) layer (usually Ethereum for most current rollups). It also provides a soft commitment to the user, i.e., **after receiving transactions from users, the sequencer provides a near-instant receipt as a “soft confirmation”<sup>(1)</sup>**. The “hard confirmation” is received after the transaction has been sent to the L1 layer.

**Figure 1: Where do sequencers fit in?**







Source: Binance Research


## Why Rollups Use Sequencers and Why It Is an Issue

Fundamentally, **sequencers have been tailored towards a very specific goal: improved user experience**. The use of a sequencer for your L2 transaction is akin to using a “fast lane,” which translates to **cheaper fees and quicker transaction confirmations**. The fact that the sequencer batches and compresses hundreds or thousands<sup>(2)</sup> of L2 transactions into a single L1 transaction saves on gas fees. In addition, the soft confirmation that the sequencer provides means that rollups are able to give their users fast block confirmations. This combination helps to improve the user experience of using an L2 rollup.

It is important to remember that **rollups do not need a sequencer; it is a design choice for a better user experience**. For instance, like how most rollups use the Ethereum L1 for data availability, they can also use it for sequencing. Justin Drake of the Ethereum Foundation recently termed these “**based rollups**”<sup>(3)</sup>. However, Ethereum’s base layer is likely to be relatively inefficient and expensive, particularly considering the high volume of L2 transactions. Essentially, the rollup’s transaction throughput will be limited by the data sequencing rate of the Ethereum L1. Users would also experience the same transaction confirmation delays as they would if they were to transact on Ethereum itself. **This has meant that every major L2 rollup project has, so far, found it more convenient, cheaper, and user-friendly to run a centralized sequencer**. While L2 users can submit their transactions directly to the L1 to bypass the sequencer, they would have to pay the L1 gas fees for transactions and the transaction might take much longer to finalize. This largely defeats the purpose of utilizing an L2 rollup for transaction execution in the first place.

**Figure 2: With the sequencer helping aggregate multiple transactions into a single L1 transaction, it helps keep the cost of transacting on L2 multiple times cheaper than on the Ethereum L1**

Logo	Name	Rollup type	Cost to send ETH (US\$)	Cost to swap tokens (US\$)
	Loopring	Zero Knowledge	0.02	0.42
	Polygon zkEVM	Zero Knowledge	0.03	0.38
	OP Mainnet	Optimistic	0.04	0.10
	zkSync Lite	Zero Knowledge	0.04	0.10

	Arbitrum One	Optimistic	0.05	0.16
	Ethereum	Base Layer	0.70	3.64

Source: l2fees.info, as of August 21, 2023

Given the fact that **the sequencer holds control over the ordering of transactions, it theoretically has the power to not include a user transaction** (although users can submit transactions directly to the L1 if they are able and willing to pay the gas fees). The **sequencer can also extract MEV from the group of transactions** (more on this later), which could be economically harmful to the user base. If there is only a single sequencer, as is currently the case for all major rollups, the centralization risks are even greater. In this scenario, **liveness** can be an issue, i.e., if the sole sequencer goes down, then the entire rollup gets affected. This risk can be mitigated with a multi-sequencer setup.

Due to this setup, **sequencers can be seen as semi-trusted parties for users**. While the sequencer cannot prevent the user from using the L2, it can delay the user's transactions, cause the user to pay extra gas fees, and extract value from the user's transactions.

*“While the sequencer cannot prevent the user from using the L2, it can delay the user's transactions, cause the user to pay extra gas fees, and extract value from the user's transactions.”*

## The Relevance of MEV

[MEV](#) is of particular relevance here. MEV refers to the value that can be obtained from block production beyond the first-order mining (or staking) block rewards and gas fees. It is **value that is extracted through manipulation of transactions within a block, i.e., through their inclusion, exclusion, and altering of their ordering**. For example, common forms of MEV extraction include frontrunning and [sandwich attacks](#).






Given the role that sequencers play in L2 rollups, they have knowledge of all user transactions on an off-chain basis. Additionally, with these sequencers usually being run by the project itself or affiliated teams, e.g., the Optimism Foundation for OP Mainnet<sup>(4)</sup> and the Arbitrum Foundation for Arbitrum One and Nova<sup>(5)</sup>, many users are concerned about potential MEV extraction that they have no visibility on. Even without these concerns, with **projects running their own centralized sequencers, the level of trustlessness and decentralization of these protocols can certainly be questioned**.

## The Current State of the Sequencer Market

At the time of writing, all of the major Ethereum L2 rollups rely on a centralized sequencer. As more and more of Ethereum’s transactions are moving onto L2 solutions, despite the decentralization of Ethereum’s validator set itself, it would appear that a large number of its transactions (i.e., those on L2s) become subject to a centralizing force in the form of a sole sequencer.

*“At the time of writing, all of the major Ethereum L2 rollups rely on a centralized sequencer.”*

**Figure 3: All the top Ethereum L2 rollups use proprietary, centralized sequencers**

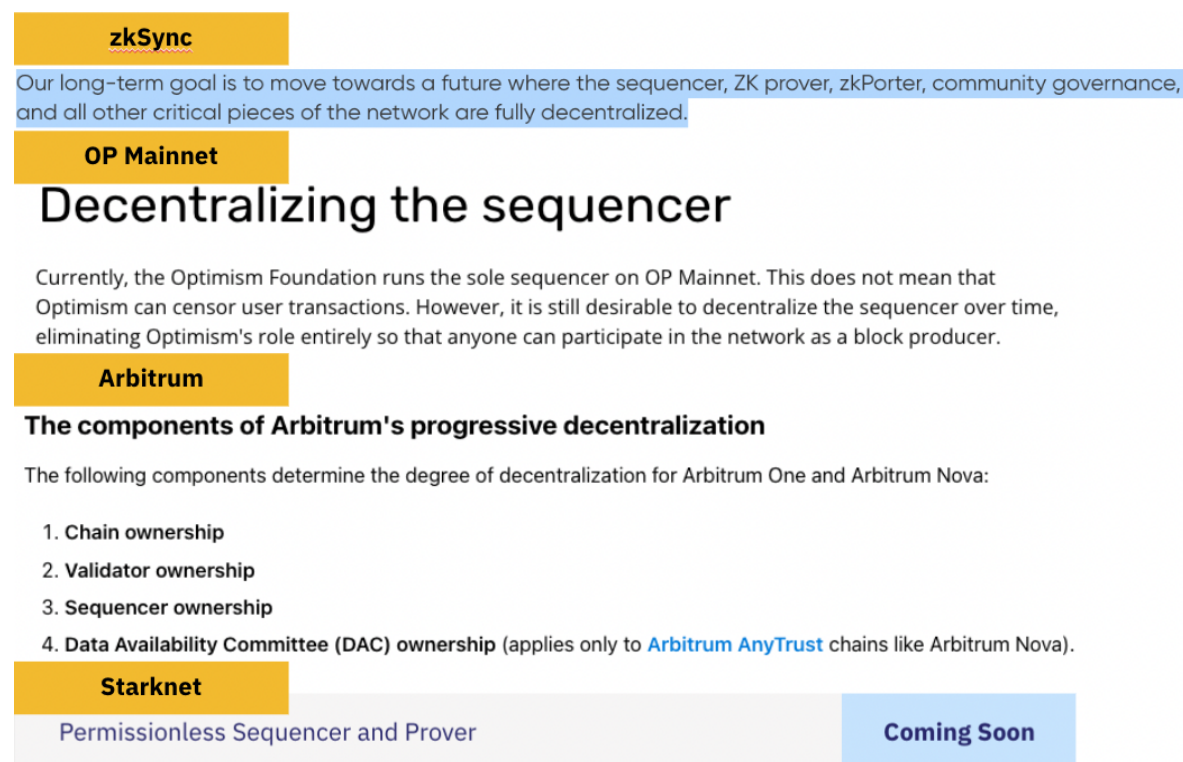
Logo	Name	Rollup type	TVL (US\$B)	Market Share
	Arbitrum One	Optimistic	5.6	56.2%
	OP Mainnet	Optimistic	2.6	26.4%
	zkSync Era	Zero Knowledge	0.4	4.2%
	dYdX	Zero Knowledge	0.3	3.4%
	Base	Optimistic	0.2	2.3%

Source: l2beat.com, as of August 21, 2023

Unsurprisingly, **most of these rollups have addressed the decentralization of their respective sequencers and featured it as part of their roadmaps.** While this is a positive sign that decentralization is part of the L2 vision, we should note that Arbitrum and Optimism have both been live with their solutions since late 2021 and are, arguably, yet to make substantial progress on decentralizing their sequencers.



**Figure 4: All the top rollups have addressed sequencer decentralization in their documentation**



Source: zkSync, OP Mainnet, Arbitrum, Starknet documentation, Binance Research

It would appear that the majority of top rollups have used their resources to improve their core products and features rather than focus on decentralization. This is not entirely a criticism, as it is somewhat understandable that, in this highly competitive environment, it would not be in any rollup's best interest to focus on decentralizing before they have a competitive product. However, as rollups mature, this view is changing, and the conversation is quickly moving toward sequencer decentralization and improving trustlessness.

## Further Issues

It is worth highlighting that there is some discussion around the level of risk posed by the reliance on centralized sequencers.

As highlighted above, given that sequencers hold control over the ordering of transactions, they can exclude user transactions and also extract MEV. However, sequencers ultimately cannot censor a user from a rollup completely. A user can bypass the sequencer and submit transactions directly to the L1 (as long as they are happy and willing to pay the increased gas cost). **While a misbehaving sequencer may cause the transaction to be delayed and the user to bear extra costs, it ultimately cannot completely censor.** This fact has likely been a contributing factor as to why no major L2 rollup has been ultra-focused on

decentralizing their sequencer until this point. Nonetheless, the **sequencer reordering transactions to extract MEV remains an issue**, especially with private [mempools](#) like those of OP Mainnet<sup>(6)</sup>.

Perhaps a greater issue is that of **liveness**. Given that the **major rollups are running sole, centralized sequencers, their entire rollup will be adversely affected if these go down**. While users can still get their transactions through by going directly to the L1, this is not particularly sustainable and is unlikely to work for the majority of transactions. Remember, the whole point of using an L2 rollup is to save on transaction costs. Given that one of the fundamental ideologies behind crypto is to prevent dependence on a sole, centralized provider (like in the traditional finance world), sequencer centralization is clearly an important issue that needs to be addressed imminently and is one of the key unlocks that shared sequencers will bring to the L2 rollup market.

*“Given that one of the fundamental ideologies behind crypto is to prevent dependance on a sole, centralized provider (like in the traditional finance world), sequencer centralization is clearly an important issue that needs to be addressed imminently and is one of the key unlocks that shared sequencers will bring to the L2 rollup market.”*

# The Solution: Decentralized, Shared Sequencers

## Overview

The emerging solution to the above issue is decentralized, shared sequencers. While different projects bring different approaches to their unique solutions, the underlying idea of replacing the sole, centralized sequencer remains the same. **“Shared” here refers to the fact that multiple different rollups can use the same network**, i.e., transactions from multiple rollups are aggregated in a mempool before being sequenced (helping mitigate MEV extraction and the potential for censorship). **“Decentralized” here refers to the concept of leader rotation**, i.e., there is not always a single actor ordering all the transactions but rather a leader selected from a decentralized set of actors. This helps against censorship and provides liveness guarantees.

This is very similar to how various different L1s operate using leader rotation mechanisms. In fact, **building a decentralized sequencing layer is akin to building a decentralized L1, i.e., you need to build a validator set**. As we will see later in this section, different projects are taking different approaches to this requirement.

Shared sequencers aim to mitigate the issue of MEV extraction, provide censorship resistance, and improve liveness guarantees for rollups, i.e., combat the issues that centralized sequencers suffer from (as described [above](#)). Additionally, two other points to note are:

- ❖ **Decentralization-as-a-service:** Shared sequencer solutions aim to provide sequencer decentralization to an arbitrary number of rollups. **All of these rollups will then benefit from the censorship resistance and liveness characteristics that can only be provided by a decentralized network without needing to establish that network themselves.** Given that this can be a very costly and time-consuming process, this is a major selling point for shared sequencer networks. Remember, no existing rollup has decentralized their sequencer, and most of them have plenty of capital<sup>(7)(8)(9)</sup> to do so, implying that this is not a wholly trivial issue. If the likes of Astria or Espresso can offer sequencer decentralization out of the box, rollups can continue to focus on differentiating and optimizing their performance to better serve a diverse range of users.
- ❖ **Cross-rollup composability:** As these shared sequencer solutions aim to handle transaction ordering for multiple rollups, they will be able to **provide unique interoperability guarantees that are not currently possible**. For example, users

should be able to specify that a transaction on Rollup 1 can be included in a block if and only if a different transaction on Rollup 2 is also included in the same block. By enabling such **conditional transaction inclusion**, shared sequencers can unlock new possibilities, including **atomic cross-rollup arbitrage**.

Numerous projects have been working on shared sequencing solutions. We highlight a few notable players and their strategies below.

## Espresso

Espresso Systems is a company working on building tools to bring Web3 into the mainstream, with a particular focus on L2 rollups and the Ethereum ecosystem. Prior to their work on shared sequencers, they have been involved in improving blockchain privacy, having developed the CAPE<sup>(10)</sup> application. They have also contributed to open-source developer tools with their Jellyfish<sup>(11)</sup> cryptography library and other initiatives like Hyperplonk<sup>(12)</sup>.

In November 2022, Espresso started sharing their work on the **Espresso Sequencer**.

### ❖ Overview

- The Espresso Sequencer is a decentralized shared sequencing network designed to **decentralize rollups while providing secure, high-throughput, low-latency transaction ordering and data availability**.
- It is designed to handle the decentralized sequencing and data availability of rollup transactions, functioning as a middleware network between rollups and the underlying L1.
- The Espresso Sequencer is designed to be **virtual machine (“VM”) agnostic**, i.e., it can be used with non-Ethereum VMs and is also **available for both zero-knowledge (“zk”) VMs and optimistic VMs**.

### ❖ How does it work?

- At the center of the sequencer is a **consensus protocol, HotShot**. HotShot is based on the HotStuff<sup>(13)</sup> consensus protocol, combined with the latest developments in a number of different areas<sup>(14)</sup> (Pacemakers, verifiable information dispersal (“VID”), etc.).
- HotShot is **open and permissionless and decentralizes participation in the sequencer network**, offering high throughput and quick finality while also maintaining safety and liveness guarantees. HotShot uses a **Proof-of-Stake (“PoS”) security model**, and one of the key requirements the Espresso team has placed on it is to achieve strong performance without compromising on

the size of the validator set. Specifically, **at a minimum, HotShot should be able to scale to include participation from all Ethereum validators** (currently over 700K<sup>(15)</sup>).

- Espresso Systems seeks to achieve Ethereum-level security for their sequencer by **engaging Ethereum’s existing validator set**. There are two key reasons for this setup:
  - i. **Security:** Launching a decentralized PoS consensus protocol is extremely costly and energy-intensive. Even then, acquiring a sufficient number of network participants may be a significant challenge. **By engaging the same set of validators as Ethereum, the sequencer can attain a level of security, liveness, and decentralization that would be very difficult to achieve on its own.** The Espresso sequencer can benefit from sharing crypto-economic security with what is generally ranked as the second most decentralized cryptocurrency after Bitcoin.

*“The Espresso sequencer can benefit from sharing crypto-economic security with what is generally ranked as the second most decentralized cryptocurrency after Bitcoin.”*

- ii. **Incentive alignment:** Conceptually, it **makes sense to engage Ethereum L1 validators in running the protocols that Ethereum L2 rollups are running on.** On a practical level, in a centralized sequencer setup, nearly all of the fees and MEV that the rollup generates are likely to be captured by the sequencer. If none (or very little) of this value is shared with L1 validators, then it is fair to worry whether this could impact the security of the rollup. For example, L1 validators could be bribed to fork the rollup and profit more than they would if they managed the rollup contract honestly. Decentralizing the sequencer and working with L1 validators for its security is a good way to mitigate any such concerns.
- Espresso will seek to establish this partnership through restaking contracts, specifically with **EigenLayer**. Through EigenLayer restaking, **users can stake their ETH and Ethereum liquid staking tokens (“LSTs”) across multiple protocols to extend economic security beyond Ethereum itself.** They earn fees in return for doing so, but they also agree to additional slashing conditions. Restaking is an efficient way to subsidize entry into this system, as stakers do not need to deploy extra capital and can just use their previously staked ETH. This **reduces the cost of capital for securing other**

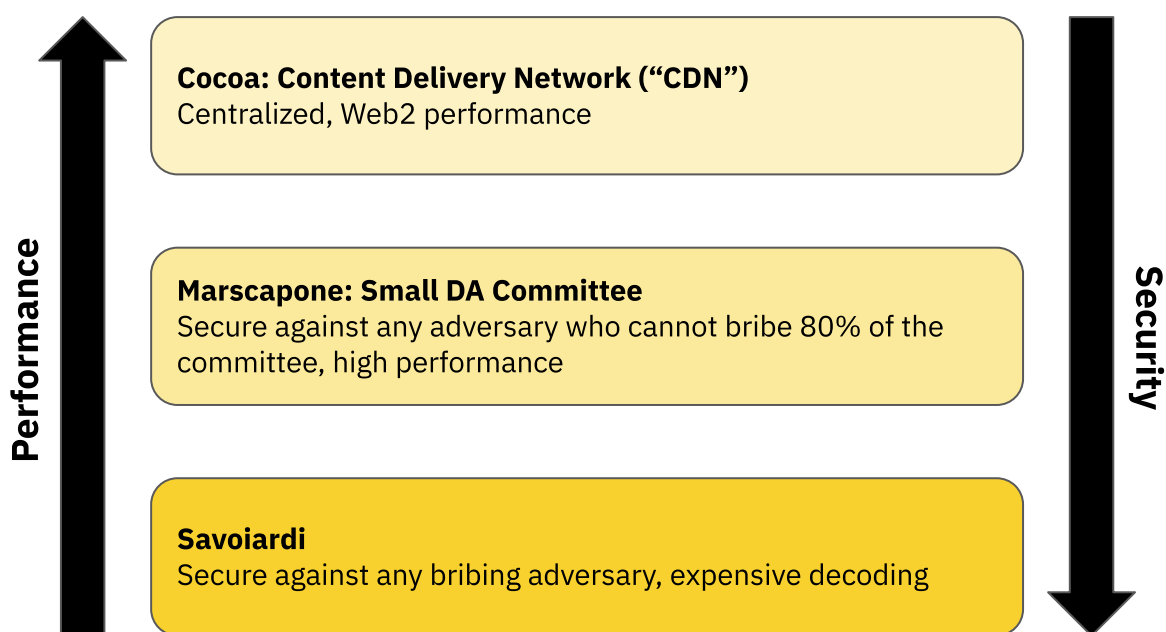
**protocols** and means that the **Espresso Sequencer can gain access to Ethereum’s staked capital base and decentralized validator set without having to bootstrap their own validator set.**

- To learn more about EigenLayer and restaking, check out our report, [Modular Blockchains: The Race to Become the Top Security Provider](#).

#### ❖ **Tiramisu data availability<sup>(16)</sup>**

- As previously highlighted, most rollups rely on the L1 blockchain, e.g., Ethereum, for data availability. However, this is not ideal as block space on L1 blockchains like Ethereum is scarce and very expensive, therefore creating high transaction fees for users – an undesirable outcome. Espresso Systems uses their highly efficient Tiramisu data availability solution to solve this.
- Much like the classic Italian dessert, the Tiramisu solution has **three novel layers**. Together, they ensure the availability of data to all parties who need it – in our case, the respective rollups that the sequencer is ordering transactions for.
  - i. Tiramisu’s **base layer is called Savoiardi**. This is a **bribery-resilient** layer (similar to Ethereum’s [danksharding](#) proposal) and provides the **highest level of security**. However, due to this property, this is the least user-friendly of the three layers. To solve this, Espresso added two additional layers to their solution.
  - ii. **Mascarpone** is the middle layer and guarantees **efficient data recovery via the election of a small DA committee**.
  - iii. **Cocoa** is the aptly named “sprinkling on top” of the entire system. Cocoa helps Tiramisu provide “[Web2-level performance](#)” by providing Tiramisu with a **content delivery network**. This helps with efficient data recovery and massively accelerates data dissemination. Given that this layer is inherently centralized<sup>(17)</sup>, it is **entirely optional, and Tiramisu works perfectly without it**. It is helpful for accelerating data availability and can easily be changed or removed.
- We should note that Espresso Systems has designed their protocol with **flexibility and modularity** in mind, and **rollups using their sequencer are able to use any other data availability solutions if they do not want to use Tiramisu**.

Figure 5: The three layers of the Tiramisu data availability solution



Source: Espresso Systems [blog](#), Binance Research

#### ❖ Notable Partnerships<sup>(18)</sup>

- The Espresso Systems team has been consistently announcing partnerships since July. **EigenLayer** was the first such partnership announcement, and given its importance in the architecture of the Espresso Sequencer, it is worth keeping a close eye on how it evolves. EigenLayer itself [launched](#) its Stage 1 mainnet on June 14.
- Alongside the Doppio testnet announcement, Espresso announced a partnership with **Polygon zkEVM**. This partnership represented the **first end-to-end integration of the Espresso Sequencer with a fully functional zk-rollup** (a fork of Polygon zkEVM). The testnet let users submit transactions to the fork, which were then routed to and sequenced by nodes running Espresso’s HotShot protocol.
- Espresso is supporting **Injective**, the IBC-enabled<sup>(19)</sup> Cosmos SDK chain, in integrating their sequencer into **Cascade**. Cascade is the **first inter-chain Solana SVM rollup for the IBC ecosystem** and allows Solana contracts to be deployed for the first time on Injective and the broader IBC ecosystem. The testnet integration with Cascade is expected in late 2023, with the mainnet expected in 2024.

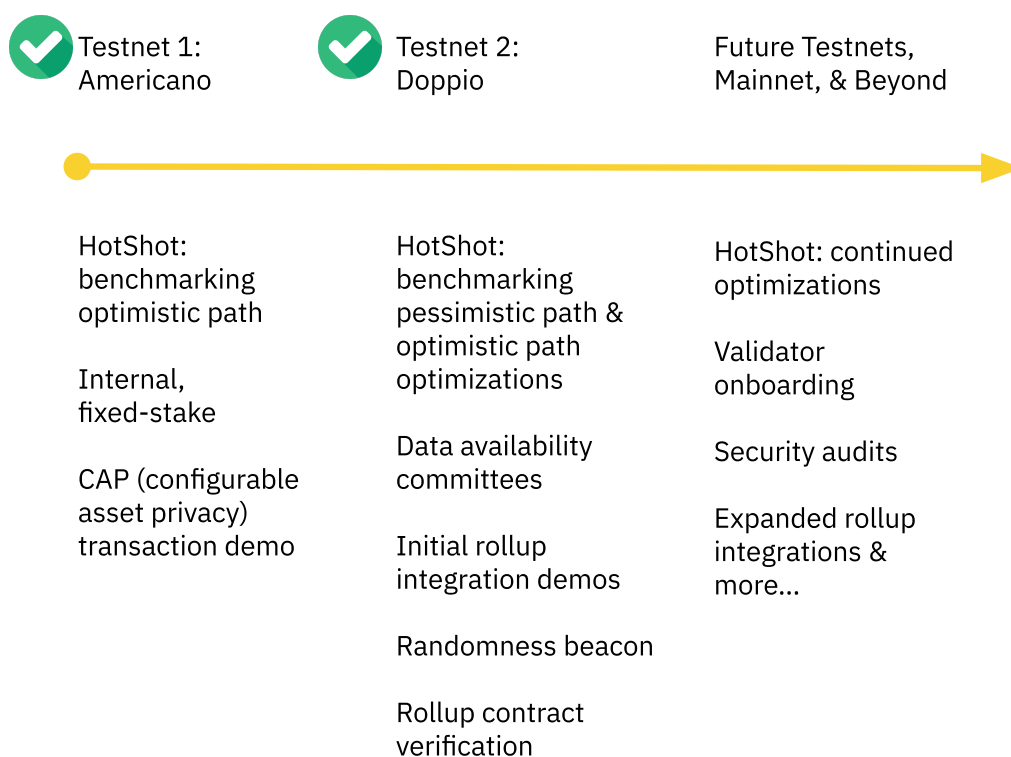
- **AltLayer** has also joined the Espresso Systems ecosystem. AltLayer is a **rollup-as-a-service platform** that allows developers to launch highly scalable rollups with multi-VM support. With their partnership, developers will be able to decide if they want to launch their rollup with AltLayer’s solution and/or the Espresso Sequencer. The teams will also work on other integrations and see how their designs can complement each other.
- Espresso Systems is collaborating with **Caldera** to deploy an **OP Stack-based optimistic rollup that uses the Espresso Sequencer and Tiramisu**. Caldera enables developers to deploy custom-built rollups for their applications. Following the deployment of the rollup, **future L2s** building on top of Caldera **will be able to easily opt into using the Espresso Sequencer and Tiramisu as plug-in components for their rollup**.
- **Spire**, a Layer-3 (“L3”) **rollup-as-a-service** company, has announced that it will integrate with the Espresso Sequencer and Tiramisu. Spire’s infrastructure allows developers to easily deploy their own L3 appchain on top of a zkEVM L2. Spire will work with the Espresso team to integrate their solution into the Spire L3 framework. A testnet is expected in 2024.

#### ❖ Latest updates

- **November 28, 2022:** [Americano](#) was the first **testnet** for the Espresso Sequencer and HotShot. The initial post contains additional technical details; however, it should be noted that it was an internal testnet and not for the general public.



**Figure 6: The roadmap for the project was released along with theAmericano testnet and initial announcement post**



Source: Espresso documentation, Binance Research

- **July 20, 2023:** Doppio was the second major milestone and testnet for HotShot and the Espresso Sequencer. Alongside the announcement, Espresso Systems released a [whitepaper](#) for the entire project. Doppio brought numerous efficiency improvements to HotShot, including verifiable information dispersal (“VID”), a new view synchronization subprotocol, and signature aggregation for quorum certificates<sup>(20)</sup>. Doppio also implemented the first two layers of Tiramisu, with future testnets expected to include the third and final layer. Espresso Systems also unveiled the **first end-to-end integration of their sequencer with a fully functional zk-rollup**, specifically a **fork of the Polygon zkEVM**.
- **August 4, 2023:** The Doppio testnet was **officially opened to the public**. Documentation on how users can submit transactions to the above-mentioned Polygon zkEVM fork was also released. Performance benchmarks were also published<sup>(21)</sup>, along with the expected **next steps**. Specifically, they announced that they are **beginning to onboard a number of rollups and rollup-as-a-service companies to their sequencer**. They also announced that they will be **contributing to the OP Stack** through their work on Optimism’s leader election proof of concept (following their recently accepted RFP<sup>(22)</sup>).

## Astria

Astria is building a shared sequencer network and is also one of the key companies spearheading the move away from centralized sequencers. Alongside this, they are also working on the **Astria EVM, which will be the first rollup powered by their shared sequencer network**. The rollup will get fast, censorship-resistant transaction ordering from their network and will leverage Celestia for data availability. Celestia, the modular blockchain network and DA layer, is very familiar to Astria. Founder Josh Bowen has previously worked at Celestia, and Astria's introductory [blog](#) has multiple mentions of the project and its ecosystem.

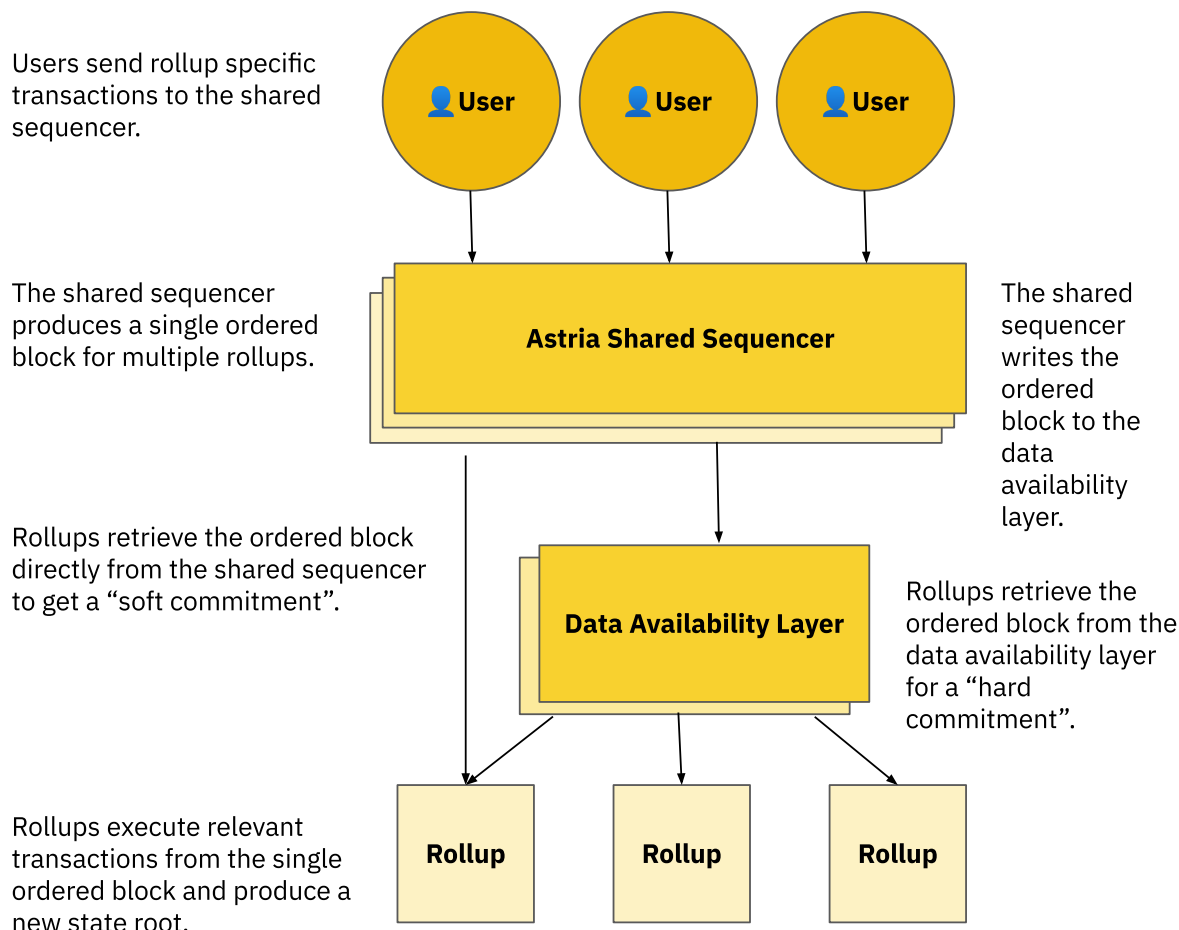
### ❖ Overview

- Astria's shared sequencer network allows **multiple different rollups to share a single, permissionless, decentralized network of sequencers**. With this network, Astria provides an out-of-the-box solution that equips rollups with censorship resistance, quick block confirmations, and atomic cross-rollup composability.

### ❖ How does it work?

- Astria's **shared sequencer network is itself a middleware blockchain that utilizes CometBFT<sup>(23)</sup> (a fork of Tendermint Core) to come to consensus on an ordered set of transactions**. The network is designed to accept transactions from multiple rollups, after which they are ordered into a single block and written to the DA layer.
- Rollups can retrieve ordered blocks from Astria immediately after they are created to provide users with a fast block confirmation via a "**soft commitment**." Alternatively, rollups can retrieve ordered blocks from the DA layer for a "**hard commitment**," as once written to the DA layer, the transaction order is considered final. This provides users with the hardest finality, which might be useful in cases with high-value transactions, etc.

**Figure 7: Astria’s shared sequencer network**









Source: Astria documentation, Binance Research

❖ **Astria EVM**

- As described above, Astria EVM will be the first rollup powered by the Astria shared sequencer network.
- Most current rollups execute and sequence transactions themselves, and use Ethereum as the DA layer. Astria EVM will focus on execution while using Astria’s shared sequencer for sequencing and Celestia for DA.

**Figure 8: Focusing on three key layers of the L2 process, we can see how rollups tend to utilize their own proprietary sequencers and Ethereum’s DA capabilities (we also show the Ethereum L1 itself as a comparison)**

	Execution	Sequencing	Data Availability
	Arbitrum One	Arbitrum Sequencer	Ethereum
	Arbitrum Nova	Arbitrum Sequencer	Data Availability Committee
	OP Mainnet	Optimism Sequencer	Ethereum
	zkSync Era	zkSync Sequencer	Ethereum
 Astria	Astria EVM	Astria Shared Sequencer	Celestia
	Ethereum Virtual Machine	Ethereum Sequencer	Ethereum

Source: Rollup documentation, Binance Research

- Astria’s **goal for their EVM is to help bootstrap Celestia’s rollup ecosystem** by acting as a hub for liquidity and bridging. It will also mean that the Astria team has a live test case for how rollups can best integrate with their shared sequencer network.

#### ❖ Vision

- Astria’s **vision for the future involves thousands of decentralized, sovereign rollups**. They envision each of these rollups being tailored to unique use cases and applications.
- Their shared sequencer network plays a key role in their vision by helping streamline the rollup development process. Their solution means that rollup developers can focus on innovative use cases while being able to easily integrate with a decentralized network, providing them with quick, censorship-resistant transaction ordering and cross-rollup composability.

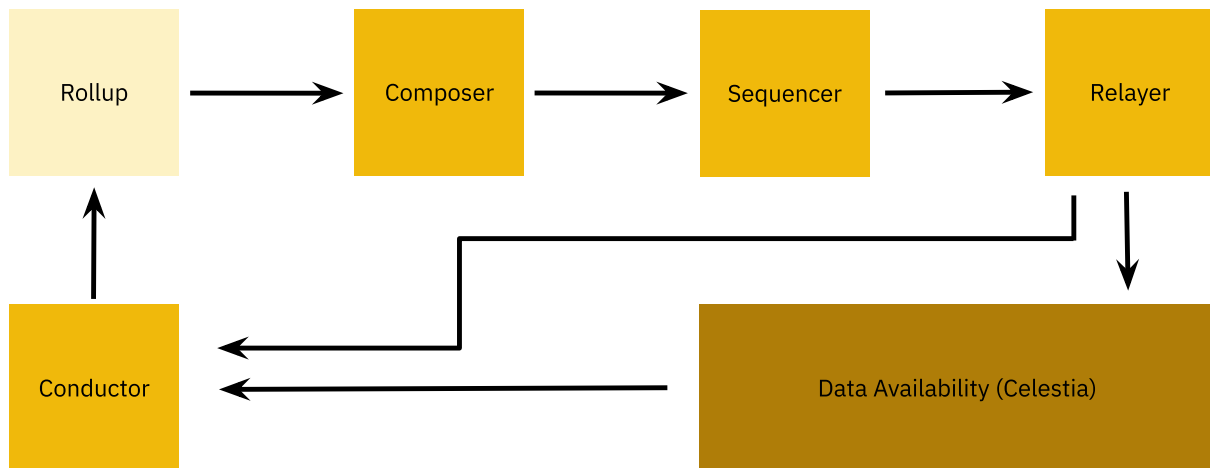
#### ❖ Astria Development Cluster

- On August 16, Astria unveiled its development cluster<sup>(24)</sup>, **containing all the different components required to launch a rollup on Astria’s shared sequencer network**. The goal of the cluster is to make developing and testing the Astria network and integrations with Astria as easy as possible.
- Components include:
  - Astria sequencer:** block-producing node for transaction ordering. The development cluster relies on a single node. When in mainnet, a decentralized set of nodes will be used.

- ii. **Data availability layer:** a local Celestia network to provide hard finality.
- iii. **Rollup:** a Geth<sup>(25)</sup> rollup node that performs executions and stores state.
- iv. **Composer:** retrieves pending transactions from the rollup’s mempool and submits them to Astria’s CometBFT mempool.
- v. **Conductor:** after receiving individual blocks, filters them for each individual rollup. These filtered blocks are then passed to the rollup for execution.
- vi. **Relayer:** sends sequenced blocks to the conductor and the data availability layer, Celestia.

➤ Having been recently announced, it will be interesting to monitor which companies decide to deploy rollups on Astria’s development cluster.

**Figure 9: The different components of Astria’s development cluster**



Source: Astria documentation, Binance Research

#### ❖ Latest updates

- In April 2023, Astria announced a US\$5.5M seed round<sup>(26)</sup>.
- As mentioned above, in August 2023, the team unveiled their development cluster.
- The **Astria team is also working on a Devnet** to kick things off. This is **expected in the coming weeks**.
- Their code is open-source, and further documentation is also available on their official GitHub [page](#).

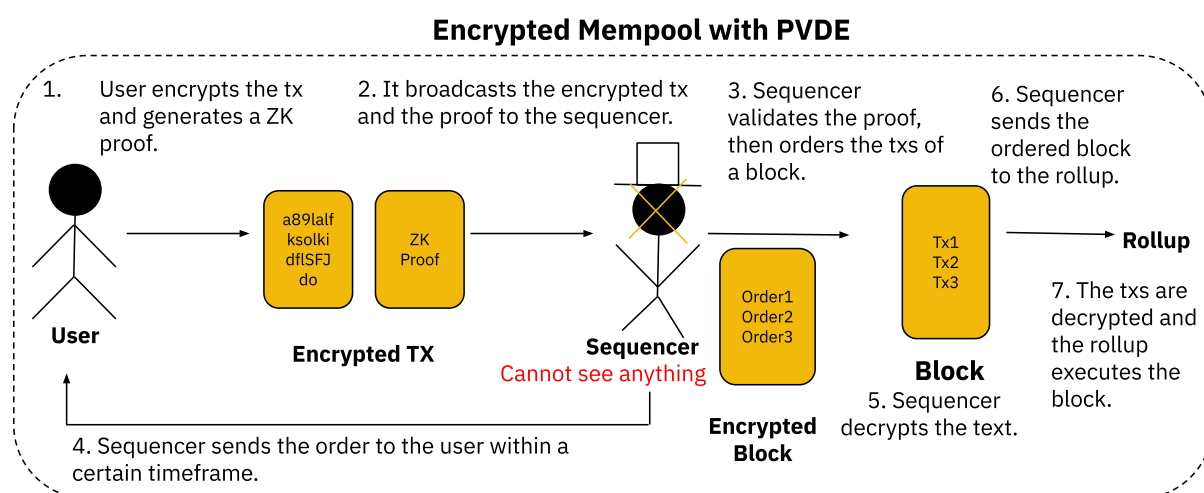
## Radius

Radius is building a trustless shared sequencing layer that uses **encryption** to decentralize the sequencer, prevent censorship, and minimize harmful MEV. Their solution is **blockchain-agnostic** and can be used for various types of rollups.

### ❖ How does it work?

- Radius uses an **encrypted mempool** to achieve its goal. Essentially, the contents of each user transaction are encrypted after being submitted. The **sequencer orders the groups of transactions without being able to see the contents of each transaction**, thus preventing the sequencer from extracting MEV or censoring.

**Figure 10: The Radius transaction process**



Source: Twitter (@Hyunxukee, Co-founder of Radius), Binance Research

- What this ultimately means is that **Radius' solution can resolve MEV and censorship issues with just a single sequencer**. As the contents of transactions are encrypted, even a single sequencer cannot act maliciously. This means that there is **no need to introduce a consensus mechanism**, which might be advantageous from a speed and scalability perspective. This distinguishes the Radius solution from Astria and Espresso, which both rely on consensus mechanisms to order transactions.
- While an encrypted mempool on a single sequencer solves two of the key issues with centralized sequencers, MEV and censorship, it still has a single point of failure. To **ensure liveness, Radius uses a distributed sequencer network with multiple sequencers operating simultaneously**. A **single sequencer will be selected from this group** to operate as the sequencing

layer. There are various proposals<sup>(27)</sup> regarding how the single sequencer will be selected, including a secret election mechanism, sequencer group sharding, etc.

#### ❖ Practical Verifiable Delay Encryption (“PVDE”)

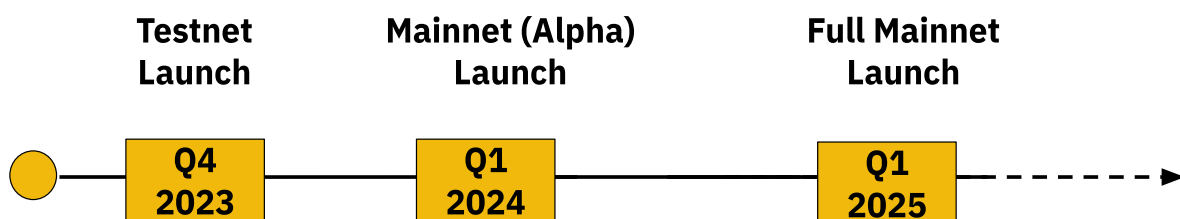
- Radius utilizes a **zk-based cryptography scheme, PVDE<sup>(28)</sup>, to create its encrypted mempool.**
- User transactions are temporarily encrypted based on a time-lock puzzle. The sequencer then orders the encrypted transactions. The sequencer needs to solve the time-lock puzzle to obtain decryption keys. This takes time and computational resources and prevents the sequencer from decrypting transactions prematurely (i.e., before they are ordered).
- To prevent attacks, the users generate a ZK proof to prove the validity of their transactions and decryption keys. The sequencer can then verify these proofs before ordering, effectively preventing meaningless decryptions (i.e., attacks) and the wasting of resources.

#### ❖ MEV marketplace

- Radius has also **proposed an optimized blockspace design.** They seek to create an **auction-based marketplace<sup>(29)</sup> for traders to submit bundles of cross-rollup MEV transactions.** The highest bidder will have their transactions included in a block by the sequencer, helping maximize rollup profits from cross-rollup arbitrage and also creating a more efficient rollup market.

#### ❖ Latest updates

- In June 2023, Radius announced their US\$1.7M pre-seed round.
- Roadmap:



Source: Radius documentation, Binance Research

## Others

While we have covered some of the larger and most prominent projects in the shared sequencing space, there are also others working on similar or closely related solutions.

- ❖ **NodeKit:** The NodeKit team is building **NodeKit SEQ**, a **decentralized shared sequencer** built into a custom L1 blockchain.
  - They are also building **NodeKit Chain**, an **EVM-based rollup**.
  - Their Twitter page also indicates that their solution will launch on an **Avalanche Subnet**<sup>(30)</sup>.
- ❖ **AltLayer:** AltLayer is a **rollup-as-a-service platform** that allows developers to launch highly scalable L2 rollups with multi-VM support.
  - While rollup-as-a-service companies are their own sector and not a space we are covering in this report, **AltLayer is important to mention here because of its decentralized sequencer network**<sup>(31)</sup>.
  - AltLayer's shared sequencer network is called the **Beacon Layer, and it is a permissionless middleware blockchain**. The nodes in the blockchain are called validators (similar to any PoS network).
  - When a user wants to create a rollup using Altlayer's platform, they can specify the number of sequencers needed to operate their rollup, the minimum amount of collateral required from each sequencer, and a set of tokens the collateral could be denominated in. AltLayer recommends at least five distinct sequencers for each rollup.
  - **Once a validator joins the Beacon Layer and puts up the minimum collateral, they can take on the role of a sequencer for different rollups.** The Beacon Layer selects validators to become sequencers for individual rollups based on their stake and some randomness. Analogous to any PoS blockchain, the validator stakes are at risk of stake slashing in the event of misbehavior.
  - This process means that developers can deploy a rollup relatively quickly using AltLayer's infrastructure and then ensure that it is decentralized using the Beacon Layer. If you subscribe to the idea of a rollup-centric future, services like AltLayer are definitely worth keeping a close eye on.



It appears that existing L2 rollups have to make a choice. On the one hand, they can maintain the status quo and continue to operate with sole, centralized sequencers. On the other hand, they can start integrating with third-party shared sequencing networks or develop their own in-house solutions.

## 1. Continue to operate as usual with a sole, centralized sequencer:

- a. This is the simplest course of action and one that is likely to be the most financially prudent. **Monetization of the sequencer is a significant revenue source<sup>(32)</sup>** for all of the major rollups and, undoubtedly, an important part of the business model. In fact, the new L2 rollup, **Base, recently confirmed their intention to monetize the sequencer in the Coinbase Q2 earnings call<sup>(33)</sup>**.
- b. Other than the fact that **maintaining a centralized sequencer creates issues in the form of censorship, MEV extraction, and single point of failure risks, it also goes against the very ethos of crypto**. Imagine a scenario where key members of a major rollup mysteriously disappear or get into serious trouble. If they run a centralized sequencer, this is likely to impact their rollup, its day-to-day operations, and the user experience. If such a situation occurs, it is likely that many of the other players in the industry will start to seriously work on decentralizing their sequencers, as outlined in their roadmaps. This is a simple example of why sequencer decentralization might be more important than it initially seems.

## 2. Integrate with third-party shared sequencing networks:

- a. As shared sequencing networks like Espresso and Astria continue to develop and move toward mainnet launch, this becomes a great option for existing rollups. In fact, keeping in mind **Espresso's integration with the Polygon zkEVM fork, it would appear that some of the major rollups are actively exploring** this option.
- b. When compared to the risks of keeping the sequencer centralized or the effort and cost required to develop an in-house solution, outsourcing sequencing to a specialist could be a sensible idea for many rollups.
- c. One of the most important factors to consider here is **rollup interoperability**. This is **potentially one of the clearest benefits of L2s that run on a shared sequencer** compared to those that run in their own proprietary silos. As

[highlighted](#) earlier in the report, running on a shared sequencer and the interoperability it brings can unlock all sorts of new possibilities, including **cross-rollup arbitrage, conditional transaction inclusion**, etc.

### 3. Develop in-house proprietary solutions:

- a. As this is likely to be the most time-consuming and costly option of the three, it will be interesting to see which rollups decide to go down this path.
- b. One of the key issues we have seen so far with the larger rollups is that of **token value accrual**. Most top Ethereum L2 rollups already use ETH as the token for gas fees, and this has prevented their own native tokens from accruing value. A **possible solution is for rollups to develop in-house sequencing solutions that can be secured by token holders**; e.g., users can stake their native rollup token to become sequencers and receive fees for their services.
- c. A **drawback of this approach is its effect on interoperability**. Rollups running on shared sequencers will have better interoperability with one another when compared to those running their own proprietary sequencing solutions.
- d. A recent development to consider is **Optimism's [announcement](#) regarding its Law of Chains**. The Law of Chains is a **set of guiding principles for chains in the OP Stack Superchain ecosystem**. It is essentially setting up a framework for these chains to work in a more homogeneous manner. This might very well extend itself to a shared sequencing solution for OP Stack-based chains, which could be a possible solution to the interoperability problem discussed above (at least for OP Stack chains).

As L2 rollups continue to proliferate in the crypto world, growing in size and transaction volume, **questions around centralization and interoperability will continue to get louder**. This topic has been gaining attention over the past year, and we anticipate it will continue to grow as the major rollups approach their one- and two-year anniversaries and more rollups launch.

While we imagine that at least some rollups will choose to integrate with third-party sequencer networks like those of Espresso and Astria, we can also see a scenario where others choose to develop their own in-house solutions. It is likely that **some of the larger rollups, especially those who have already launched native tokens, might see value in developing their own solutions in order to maximize profits and add utility to their tokens**. Whatever happens, it remains a very important aspect of the rollup world to keep an eye on and something we will monitor closely with great interest.

## 6 Closing Thoughts

Users want and prefer faster transaction confirmations and cheaper fees. While centralized sequencers have been the solution to this for the major L2 rollups so far, rollups and users should ideally have the choice to use the best decentralized version of this technology. This is the crucial role that companies like Espresso Systems, Astria, Radius, and others are playing in the L2 story.

The two key drivers here are decentralization and rollup interoperability. Decentralization is crucial for a number of different reasons. The fact that it is very much the philosophical underpinnings of crypto is just one of these. On a more practical level, centralized sequencers represent a single point of failure in terms of rollup liveness and are a threat to rollup resiliency. This is not to mention the potential for large amounts of MEV extraction, some of which might be hidden from the user and extracted in a private mempool. The potential for censorship, even if temporary, and delayed transactions is also an issue and important to keep in mind, especially when considering the industry's strong growth aspirations. Rollup interoperability is similarly crucial, especially if one subscribes to the rollup-centric view of the future of the crypto industry. If the market is to become more and more saturated with rollups, whether app-specific or otherwise, then they should be able to communicate and work seamlessly with each other. How else are we to achieve a Web2-type user experience?

There are certainly challenges in the future, and some of the bigger rollups might be tempted to create their own proprietary solutions rather than use a shared sequencing network. One way to combat this would be for shared sequencing networks to address value accrual and revenue allocation through economic mechanisms, because ultimately, there is a strong network effect to be realized if many rollups share a common sequencer.

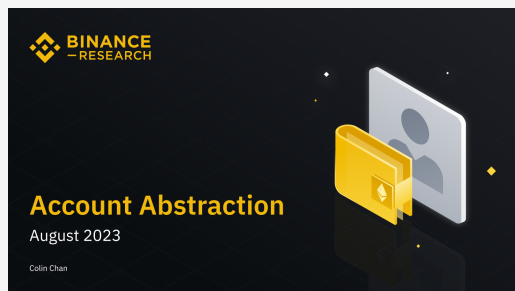
This is a topic that will continue to get more heated in the coming months, and we are sure many new players will join the market, both in the rollup space and in the shared sequencer space. It will be interesting to observe what choices different projects make. We look forward to keeping our ears close to the ground and following this narrative closely.

# References

1. <https://developer.arbitrum.io/tx-lifecycle>
2. <https://arbiscan.io/batches>
3. <https://ethresear.ch/t/based-rollups-superpowers-from-l1-sequencing/15016>
4. <https://community.optimism.io/docs/protocol/#>
5. <https://docs.arbitrum.foundation/state-of-progressive-decentralization>
6. <https://community.optimism.io/docs/protocol/2-rollup-protocol/#block-storage>
7. [https://www.crunchbase.com/organization/offchain-labs/company\\_financials](https://www.crunchbase.com/organization/offchain-labs/company_financials)
8. [https://techcrunch.com/2022/03/17/paradigm-and-a16z-back-ethereum-scaling-startup-optimism-at-1-65b-valuation/?guccounter=1&guce\\_referrer=aHR0cHM6Ly93d3cuZ29vZ2x1LmNvbS8&guce\\_referrer\\_sig=AQAAAH1UUtX3eQktyE-EF3nDiZrSMhHHFCVsn4A-tjzf5NAexyOjflqbpeNImAWEiSi4XC9ioadDK3PMETVRuIJ5Raqek7vcdGvUQ-7i7D2YnQ8Jw\\_4vQiUBqQHZ09u8IqPOpil659OUndLV88EImuQ1nduk-bvFoECgpl0PgZS4j-t](https://techcrunch.com/2022/03/17/paradigm-and-a16z-back-ethereum-scaling-startup-optimism-at-1-65b-valuation/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2x1LmNvbS8&guce_referrer_sig=AQAAAH1UUtX3eQktyE-EF3nDiZrSMhHHFCVsn4A-tjzf5NAexyOjflqbpeNImAWEiSi4XC9ioadDK3PMETVRuIJ5Raqek7vcdGvUQ-7i7D2YnQ8Jw_4vQiUBqQHZ09u8IqPOpil659OUndLV88EImuQ1nduk-bvFoECgpl0PgZS4j-t)
9. <https://techcrunch.com/2022/11/16/matter-labs-the-company-behind-zksync-raises-200-million-to-scale-ethereum/>
10. <https://medium.com/@espressosys/cape-configurable-asset-privacy-for-ethereum-71919935643b>
11. <https://medium.com/@espressosys/releasing-the-jellyfish-cryptography-library-73068138ae14>
12. <https://medium.com/@espressosys/hyperplonk-a-zk-proof-system-for-zkevm-d45fd077bfba>
13. <https://arxiv.org/abs/1803.05069>
14. <https://medium.com/@espressosys/espresso-hotshot-consensus-designed-for-rollups-b080ba7362d1>
15. <https://beaconcha.in/>
16. [https://hackmd.io/@EspressoSystems/HotShot-and-Tiramisu?utm\\_source=preview-mode&utm\\_medium=rec#Introduction](https://hackmd.io/@EspressoSystems/HotShot-and-Tiramisu?utm_source=preview-mode&utm_medium=rec#Introduction)
17. <https://twitter.com/EspressoSys/status/1682425433541816320?s=20>
18. <https://medium.com/@espressosys>
19. <https://tutorials.cosmos.network/academy/3-ibc/1-what-is-ibc.html>
20. <https://medium.com/@espressosys/releasing-the-espresso-sequencer-testnet-ii-doppio-bcc46c315c30>
21. <https://docs.espressosys.com/sequencer/releases/doppio-testnet-release/benchmarks>
22. <https://github.com/ethereum-optimism/ecosystem-contributions/issues/63>
23. <https://github.com/astriaorg/dev-cluster/blob/sb/dev-cluster-overview-doc/docs/astria.md>
24. <https://blog.astria.org/introducing-the-astria-development-cluster/>
25. <https://geth.ethereum.org/>

26. <https://twitter.com/AstriaOrg/status/1643291058623901696?s=20>
27. <https://docs.theradius.xyz/developer/distributed-sequencer-network>
28. <https://ethresear.ch/t/mev-resistant-zk-rollups-with-practical-vde-pvde/12677>
29. <https://docs.theradius.xyz/developer/blockspace-optimization>
30. <https://twitter.com/luigidemeo/status/1679179380856176656?s=20>
31. <https://docs.altlayer.io/altlayer-documentation/beacon-layer/shared-sequencing-layer>
32. <https://dune.com/niftytable/rollup-economics>
33. [https://s27.q4cdn.com/397450999/files/doc\\_financials/2023/q2/Coinbase-Q2-23-Earnings-Call-Transcript.pdf](https://s27.q4cdn.com/397450999/files/doc_financials/2023/q2/Coinbase-Q2-23-Earnings-Call-Transcript.pdf)

# Latest Binance Research Reports



## A Primer on Account Abstraction

An introduction to account abstraction



## Monthly Market Insights: August 2023

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



## Telegram Bots: Exploring the Landscape

An overview of the Telegram Bots landscape



## Navigating DeFi Derivatives

A closer look at the DeFi derivatives market

# 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.