Special thanks to Brecht, Archie, and Dave for comments and review.

TL;DR

In this article, we briefly cover a general rollup architecture and the rollup properties required for long-term robustness and safety. Then, we mention the origination history of the based rollup and unpack its architecture. In the FAQ section, we answer questions about based rollups.

Disclaimer: rollup definitions struggle from lack of alignment sometimes. In this article, we refer to the rollup layers taxonomy provided by Celestia. Please check it out to ensure we are on the same page.

Content

- Is based rollup censorship-resistant?
- Is token necessary for a based rollup to operate in good faith?
- Can a based rollup be built on top of a non-based rollup?
- How is MEV handled in a based rollup?
- What do we mean by “L1 sequencing”? Do based rollups increase the load on L1 validators because they do the sequencing?
- Will based rollups be cheaper for users?
- Is based rollup a sovereign rollup?
- Can an optimistic rollup be based?
- Why do based rollups have stronger economic guarantees?
- Are based rollups limited to the L1 block times?
- What's the difference between based and shared sequencers?
- How does being a based rollup impact the design of the rollup?
- How decentralized are based rollups?
- How does a based rollup affect L1 stakers?
- What liveness level do based rollups provide?

- Is based rollup censorship-resistant?
- Is token necessary for a based rollup to operate in good faith?
- Can a based rollup be built on top of a non-based rollup?

Introduction

- How rollups work
- Rollup consists of up to four layers
- The wanted “features” of rollups

How rollups work

Rollup consists of up to four layers

The wanted “features” of rollups

History of a based rollup

Based rollup architecture

- Settlement Layer
- Data Availability
- Consensus
- Execution Layer

Settlement Layer

Data Availability

Consensus

Execution Layer

Based rollup FAQ

- How is MEV handled in a based rollup?

- What do we mean by “L1 sequencing”? Do based rollups increase the load on L1 validators because they do the sequencing?
- Will based rollups be cheaper for users?
- Is based rollup a sovereign rollup?
- Can an optimistic rollup be based?
- Why do based rollups have stronger economic guarantees?
- Are based rollups limited to the L1 block times?
- What's the difference between based and shared sequencers?
- How does being a based rollup impact the design of the rollup?
- How decentralized are based rollups?
- How does a based rollup affect L1 stakers?
- What liveness level do based rollups provide?
- Is based rollup censorship-resistant?
- Is token necessary for a based rollup to operate in good faith?
- Can a based rollup be built on top of a non-based rollup?

How is MEV handled in a based rollup?

What do we mean by “L1 sequencing”? Do based rollups increase the load on L1 validators because they do the sequencing?

Will based rollups be cheaper for users?

Is based rollup a sovereign rollup?

Can an optimistic rollup be based?

Why do based rollups have stronger economic guarantees?

Are based rollups limited to the L1 block times?

What's the difference between based and shared sequencers?

How does being a based rollup impact the design of the rollup?

How decentralized are based rollups?

How does a based rollup affect L1 stakers?

What liveness level do based rollups provide?

Is based rollup censorship-resistant?

Is token necessary for a based rollup to operate in good faith?

Can a based rollup be built on top of a non-based rollup?

Introduction

Disclaimer: there are a lot of articles and videos explaining what a rollup is and what is not. However, we have to briefly define the core components of a rollup in this article, as well as it is necessary for an explanation of how each rollup core component works in a based rollup. If you’re fluent in rollups, feel free to skip the introduction.

How rollups work

- A rollup is a scaling solution for Ethereum (L1).
- It performs transaction execution off-chain, packing transactions in blocks.

- For each block, rollups post the data required for reconstructing the chain state (as a source of Data Availability) to the Data Availability Layer and a proof that the off-chain execution was performed correctly to the Settlement Layer (in the case of ZK-rollup, for each block, in case of an optimistic rollup, only if there is a dispute). Note: After EIP-4844, when data posting will switch to the blobs, one might call this layer “Data Publishing Layer”. For more information on how EIP-4844 will impact rollups, check our article “Why EIP-4844 matters for rollups and how it works for ZK-EVM.”

- There are two types of rollups: Zero-Knowledge rollups (ZK-rollups) and optimistic rollups. They differ by the types of proofs they use: ZK-rollups use Zero-Knowledge Proofs, and optimistic rollups use fraud proofs. While ZK-rollups post a ZK proof to the Settlement Layer for each

block, optimistic rollups post fraud proof only if there is a dispute.

- A rollup’s smart contract on L1 verifies the posted proofs.

- Each rollup has a bridge (or bridges) to transfer data between chains (including deposits and withdrawals). Deposits and withdrawals allow users to permissionlessly

transfer their assets between L1 (Ethereum) and L2 (a rollup).

A rollup is a scaling solution for Ethereum (L1).

It performs transaction execution off-chain, packing transactions in blocks.

For each block, rollups post the data required for reconstructing the chain state (as a source of Data Availability) to the Data Availability Layer and a proof that the off-chain execution was performed correctly to the Settlement Layer (in the case of ZK-rollup, for each block, in case of an optimistic rollup, only if there is a dispute). Note: After EIP-4844, when data posting will switch to the blobs, one might call this layer “Data Publishing Layer”. For more information on how EIP-4844 will impact rollups, check our article “Why EIP-4844 matters for rollups and how it works for ZK-EVM.”

There are two types of rollups: Zero-Knowledge rollups (ZK-rollups) and optimistic rollups. They differ by the types of proofs they use: ZK-rollups use Zero-Knowledge Proofs, and optimistic rollups use fraud proofs. While ZK-rollups post a ZK proof to the Settlement Layer for each

block, optimistic rollups post fraud proof only if there is a dispute.

A rollup’s smart contract on L1 verifies the posted proofs.

Each rollup has a bridge (or bridges) to transfer data between chains (including deposits and withdrawals). Deposits and withdrawals allow users to permissionlessly

transfer their assets between L1 (Ethereum) and L2 (a rollup).

Rollup consists of up to four layers:

- Settlement Layer

– provides objective onchain finality. For classical optimistic rollups and ZK-rollups, Ethereum is a Settlement Layer as they post the proofs to L1. Hence, if there is a dispute, the proof can be checked on L1.

Settlement Layer is optional. A rollup without the Settlement Layer is called a “sovereign rollup.” Imagine a social app-chain. The proof of correct execution is important only in two cases: (i) one needs to know the L2 state on L1 (e.g., for withdrawals), (ii) one wants to allow faster trustless syncing against a verified state root that is proven. If the social app is not one – neither the first case nor the second one are applicable. Hence, the social app-chain can live without the Settlement Layer (i.e., be a Sovereign Rollup).

- Data Availability Layer

– guarantees that everyone can access data required to reconstruct the rollup state.

- Consensus Layer

– a network of sequencers (or just a single sequencer) agrees on the order of transactions in a block before posting the data required to reconstruct the chain state to the Data Availability Layer.

The Consensus Layer is optional as (i) not all rollups have their own consensus layer and (ii) not all rollups have a network of sequencers (some have only one sequencer). Note: as by Consensus Layer we mean sequencers, one might also refer to it as a “Sequencing Layer”.

- Execution Layer

– executes transactions off-chain, that is, fetches the posted transaction data and construct the state of the rollup.

Settlement Layer

– provides objective onchain finality. For classical optimistic rollups and ZK-rollups, Ethereum is a Settlement Layer as they post the proofs to L1. Hence, if there is a dispute, the proof can be checked on L1.

Settlement Layer is optional. A rollup without the Settlement Layer is called a “sovereign rollup.” Imagine a social app-chain. The proof of correct execution is important only in two cases: (i) one needs to know the L2 state on L1 (e.g., for withdrawals), (ii) one wants to allow faster trustless syncing against a verified state root that is proven. If the social app is not one – neither the first case nor the second one are applicable. Hence, the social app-chain can live without the Settlement Layer (i.e., be a Sovereign Rollup).

Data Availability Layer

– guarantees that everyone can access data required to reconstruct the rollup state.

Consensus Layer

– a network of sequencers (or just a single sequencer) agrees on the order of transactions in a block before posting the data required to reconstruct the chain state to the Data Availability Layer.

The Consensus Layer is optional as (i) not all rollups have their own consensus layer and (ii) not all rollups have a network of sequencers (some have only one sequencer). Note: as by Consensus Layer we mean sequencers, one might also refer to it as a “Sequencing Layer”.

Execution Layer

– executes transactions off-chain, that is, fetches the posted transaction data and construct the state of the rollup.

The desired “features” of rollups

- Expected behaviour

– transactions are executed according to the specs, and everyone agrees on the state of the blockchain.

- Censorship resistance

– any user can force any transaction to be executed by the rollup within a reasonable time period at a reasonable cost.

- Liveness

– the rollup prover, smart contract, and sequencer must all be live and functioning.

- Decentralization

– different rollup components (e.g., sequencer, prover, and data availability) are handled by a decentralized network of operators.

- Cheap transactions

– transactions are as cheap as possible (in an ideal case, almost free).

Expected behaviour

– transactions are executed according to the specs, and everyone agrees on the state of the blockchain.

Censorship resistance

– any user can force any transaction to be executed by the rollup within a reasonable time period at a reasonable cost.

Liveness

– the rollup prover, smart contract, and sequencer must all be live and functioning.

Decentralization

– different rollup components (e.g., sequencer, prover, and data availability) are handled by a decentralized network of operators.

Cheap transactions

– transactions are as cheap as possible (in an ideal case, almost free).

History of a based rollup

The idea

The idea of the based rollup was first introduced as “Total Anarchy” by Vitalik in thearticle “An Incomplete Guide to Rollups” from 2021:

”Total anarchy: anyone can submit a batch at any time.

”

The definition

The definition of a based rollup and formal design description were later introduced by Justin Drake in March 2023 in the ethresearch post “Based rollups—superpowers from L1 sequencing”:

”A rollup is said to be based, or L1-sequenced, when its sequencing is driven by the base L1. More concretely, a based rollup is one where the next L1 proposer may, in collaboration with L1 searchers and builders, permissionlessly include the next rollup block as part of the next L1 block.

”

Based rollup

By design, Taiko has been building towards being a based rollup since the winter of 2023. By name, Taiko started introducing itself as a based rollup after the name “based rollup” was proposed by Justin in his ethresearch post in March 2023.

Based rollup architecture

- Settlement Layer

– since based rollup posts proofs to Ethereum, its Settlement is Ethereum. One can always get access to the verified L2 chain state on Ethereum.

- Data Availability Layer

– since based rollup posts the data required to reconstruct the chain state to Ethereum, Ethereum is its Data Availability Layer. Anyone can check the posted block hash and use it to retrieve the data about transactions executed in this block.

- Consensus Layer

– based rollup doesn’t have a separate consensus, which is why it doesn’t have a Consensus Layer. Instead, it uses the Ethereum Consensus Layer as the transaction ordering is determined by L1 validators.

- Execution Layer

– based rollup executes transactions off-chain on its own. Hence, based rollup is its own Execution Layer.

Settlement Layer

– since based rollup posts proofs to Ethereum, its Settlement is Ethereum. One can always get access to the verified L2 chain state on Ethereum.

Data Availability Layer

– since based rollup posts the data required to reconstruct the chain state to Ethereum, Ethereum is its Data Availability Layer. Anyone can check the posted block hash and use it to retrieve the data about transactions executed in this block.

Consensus Layer

– based rollup doesn’t have a separate consensus, which is why it doesn’t have a Consensus Layer. Instead, it uses the Ethereum Consensus Layer as the transaction ordering is determined by L1 validators.

Execution Layer

– based rollup executes transactions off-chain on its own. Hence, based rollup is its own Execution Layer.

Based Rollup FAQ

How is MEV handled in a based rollup?

Most based rollup MEV flows to L1 validators. L1 searchers and block builders are incentivized to extract rollup MEV by including rollup blocks within their L1 bundles and L1 blocks. This then incentivizes L1 proposers to include rollup blocks on the L1.

To further talk about MEV, let's assume an MEV taxonomysuggested by Justin Drake: "Blockspace fundamentally provides both transaction inclusion and transaction ordering services. Competition for inclusion leads to congestion, and competition for ordering leads to contention."

That is, MEV = congestion

- contention

, where congestion stands for transaction inclusion using the EIP-1559 mechanism and contention stands for transaction ordering, a.k.a. "bad MEV" extraction, such as sandwich attacks or front-running. As for now, circa 80% of Ethereum MEV is congestion MEV, and only 20% is "bad MEV." If L2 MEV follows the same logic, some substantial share of L2 MEV might stay on L2.

For more details on how MEV is handled by different L2s, check ourarticle "L2 MEV wat".

What do we mean by "L1 sequencing"? Do based rollups increase the load on L1 validators because they do the sequencing?

When we say "L1-sequenced", we mean that the next L1 proposer may, in collaboration with L1 searchers and builders, permissionlessly include the next rollup block as part of the next L1 block. That is, the sequence of included L2 blocks (and, as a consequence, the final ordering of transactions) is determined by L1 proposers (i.e. validators who were given a right to propose a block for a specific slot).

One should note that by default L1 validators do not build L2 blocks on their own. Instead, each based rollup block is built by an L2 builder. That is, L1-sequenced rollups do not increase the load on L1 validators.

Will based rollups be cheaper for users?

Using an L1 proposer as an L2 sequencer allows to remove one layer from the supply chain that might

lead to cheaper transactions (e.g., no need to verify signatures from centralized or decentralized sequencers.)

It is fair to note that not only based rollup but rollups with shared sequencing, in general, might reduce the transaction cost for the same reason. As block proposing is permissionless, there is fair competition to build blocks, which might also decrease user fees.

Is based rollup a sovereign rollup?

By default, based rollup and sovereign rollup are not related at all, as based rollup is mostly about the way of block proposal while sovereign rollup is mostly about the way of block proving. But formally, if based rollup, for example, gets rid of the proofs (i.e. only data messaging without transaction execution), it will become a sovereign rollup.

Can an optimistic rollup be based?

Yes, if the decision on block inclusion is "outsourced" to L1 validators (exactly the same mechanism as for general based rollup case described in this article).

Why do based rollups strengthen Ethereum's economic guarantees? (a.k.a. L1 economic alignment)

MEV originating from based rollups naturally flows to the base L1. These flows strengthen L1 economic security (and, as a consequence, the economic security of the whole Ethereum ecosystem) and, in the case of MEV burn, improve the economic scarcity of the L1 native token.

Are based rollups limited to the L1 block times?

By default, yes. The based rollup transaction confirmation time directly depends on the L1 block time (i.e., 12s for Ethereum today).

However, one should note that instant pre-confirmations are possible for based rollup. It can be designed using re-staking

where a share of L1 validators commit (through re-staking) to include based rollup blocks in L1 blocks they'll propose in the future (this idea was suggested by Justin Drake in summer 2023). It is possible, as validators know at least 32 blocks in advance, who is assigned as a proposer to which block.

What's the difference between based and shared sequencers?

Shared Sequencer functions as middleware between rollups and their underlying L1, sequencing transactions for a number of rollups. That is, transactions of different rollups can be included in one superblock.

The goal of Shared Sequencer is to build the most economically profitable block. It extrapolates the idea of Based Sequencing aiming at higher (than L1) throughput and faster (than L1 block time) confirmation of transactions while maintaining decentralization.

However, while based rollup relies on Ethereum, Shared Sequencer relies on a separate new set of operators handling decentralized sequencing with its own consensus. That is, as a system, SS is more complex than based rollup. Furthermore, it doesn't inherit 100% Ethereum liveness.

How does being a based rollup impact the design of the rollup?

Based sequencing is maximally simple, significantly simpler than even centralized sequencing, because of reusing Ethereum infrastructure. Based sequencing requires no sequencer signature verification, no escape hatch, and no external PoS consensus.

How decentralized are based rollups?

Based sequencing inherits the decentralization of the L1 and naturally reuses L1 searcher-builder-proposer infrastructure.

How does based rollup affect L1 stakers?

By default, based rollup almost doesn't affect L1 stakers. The only impact it might have – is increased earnings as MEV from based rollup mostly flows to the L1. However, if based rollup is going to adopt fast-finality through re-staking, then L1 stakers can jump into based rollup re-staking.

What liveness level does based rollup provide?

Based sequencing enjoys the same liveness guarantees as Ethereum. And this is the only type of rollup that inherits 100% of Ethereum's liveness.

Non-based rollups with escape hatches suffer degraded liveness because

- Transactions in the escape hatch have to wait a timeout period before guaranteed settlement;
- Rollups with escape hatches are liable to toxic MEV from short-term sequencer censorship during the timeout period;
- A mass exit triggered by a sequencer liveness failure would disrupt rollup network effects (rollups, unlike the L1, cannot use social consensus to gracefully recover from sequencer liveness failures);

Transactions in the escape hatch have to wait a timeout period before guaranteed settlement;

Rollups with escape hatches are liable to toxic MEV from short-term sequencer censorship during the timeout period;

A mass exit triggered by a sequencer liveness failure would disrupt rollup network effects (rollups, unlike the L1, cannot use social consensus to gracefully recover from sequencer liveness failures);

Even if the liveness degradation seems to be tiny (e.g., 99% instead of 100%), in the adversarial environment, this small delta of 1-5% can be exploited. For example, if one can censor DEX transactions or Oracle activity for an hour – this is a huge position of power to create a lot of disruption and toxic MEV.

Is based rollup censorship-resistant?

Based rollup inherits Ethereum's censorship resistance. That is, as long as Ethereum is censorship resistant – based rollup is censorship resistant as well. While for a traditional rollup, escape hatches are required to provide censorship resistance.

Is token necessary for a based rollup to operate in good faith?

Based sequencing can easily be tokenless (avoiding the regulatory burden of token-based sequencing) as its correctness and fairness are guaranteed by Ethereum.

Can a based rollup be built on top of a non-based rollup?

Based rollups allow building alternatively sequenced applications on top of them (for example, building a Central Limit Order Book on top of Taiko). But the opposite is not possible.

Sources

- https://celestia.org/learn/beginners/the-modular-stack/
- https://medium.com/@espressosys/sequencer-decentralization-and-liveness-e5af7f4b25ca
- https://www.cryptofrens.info/p/settlement-layers-ethereum-rollups
- https://vitalik.ca/general/2021/01/05/rollup.html
- https://ethresear.ch/t/based-rollups-superpowers-from-l1-sequencing/15016
- https://community.taiko.xyz/t/based-rollups-and-decentralized-sequencing-twitter-spaces-wrap-up/1220

https://celestia.org/learn/beginners/the-modular-stack/

https://medium.com/@espressosys/sequencer-decentralization-and-liveness-e5af7f4b25ca

https://www.cryptofrens.info/p/settlement-layers-ethereum-rollups

https://vitalik.ca/general/2021/01/05/rollup.html

https://ethresear.ch/t/based-rollups-superpowers-from-l1-sequencing/15016

https://community.taiko.xyz/t/based-rollups-and-decentralized-sequencing-twitter-spaces-wrap-up/1220

Join us

Explore open positions on our job board.

Follow us

Get the latest from Taiko:

- Website: https://taiko.xyz.
- Discord: https://discord.gg/taikoxyz.
- GitHub: https://github.com/taikoxyz.
- Twitter: https://twitter.com/taikoxyz.
- Community forum: https://community.taiko.xyz.
- Youtube: https://www.youtube.com/@taikoxyz.

Website: https://taiko.xyz.

Discord: https://discord.gg/taikoxyz.

GitHub: https://github.com/taikoxyz.

Twitter: https://twitter.com/taikoxyz.

Community forum: https://community.taiko.xyz.

Youtube: https://www.youtube.com/@taikoxyz.

Contribute

Contribute to Taiko on GitHub and earn a GitPOAP! You will also be featured as a contributor on our README. Get started with the contributing manual.