taiko

How restaking improves based rollup UX

Mamy Ratsimbazafy

ZK Engineering @ Taiko

mratsim

m_ratsim

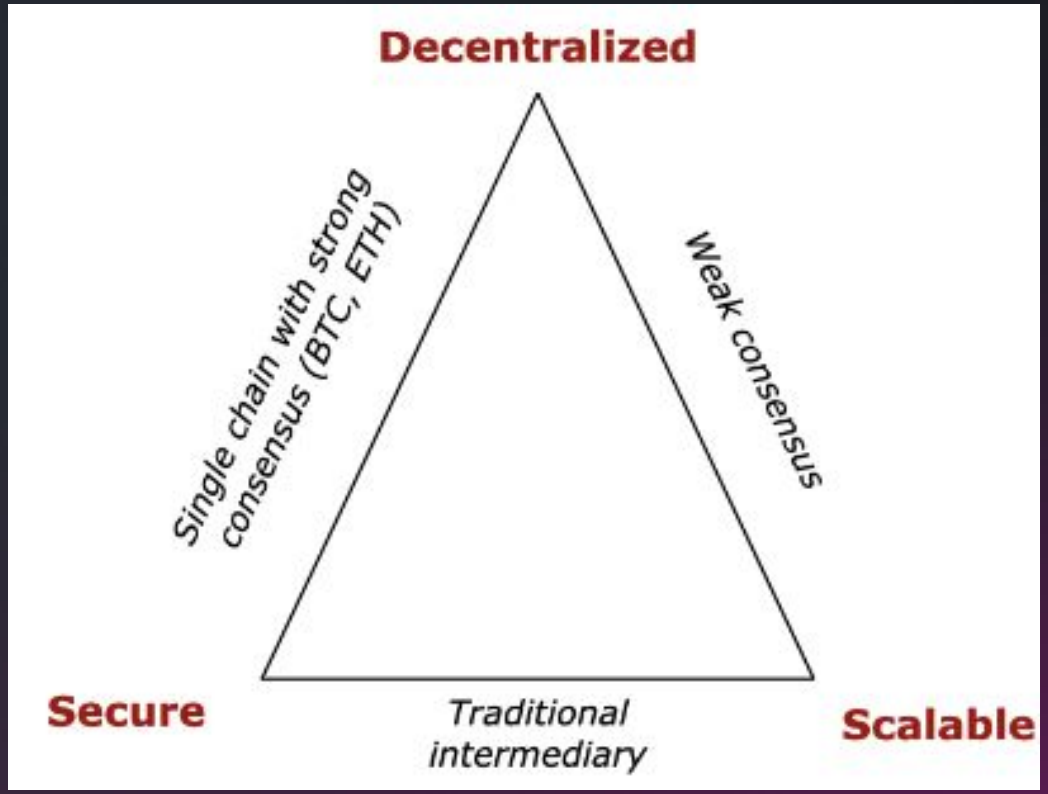
Agenda

- The Challenges of Scaling Ethereum
- Based rollups & Based L1 validators
- Restaking Refresher
- How Restaking Improves Based Rollups UX

The Challenges of Scaling Ethereum

Blockchain trilemma

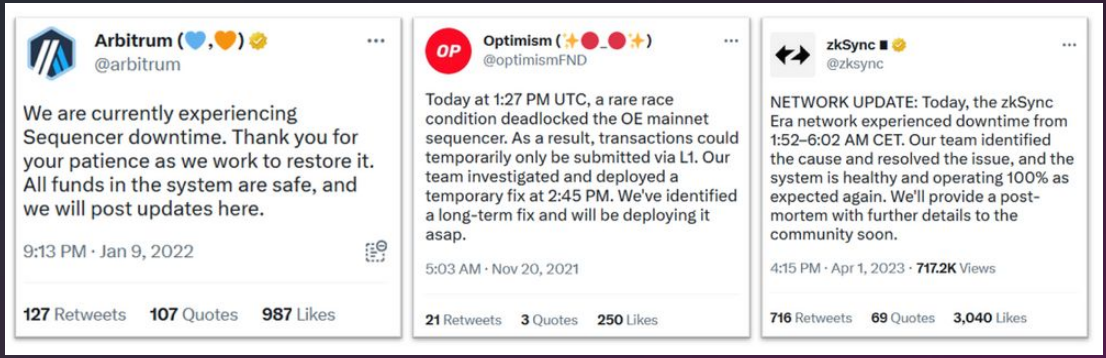
Buterin 2021 (sharding article), Auer-Monnet-Shin 2021 (Bank of international Settlement)



Rollup decentralization

Charbonneau 2023 (SUAVE, Anoma, Shared Sequencers), Bankless 2023 (Will Rollups Ever Decentralize)

- Data Availability
  - uses L1 validators after EIP-4844
- Ordering of transactions
  - Centralized sequencers
  - *Centralized + escape hatch*
  - *Decentralized sequencers*



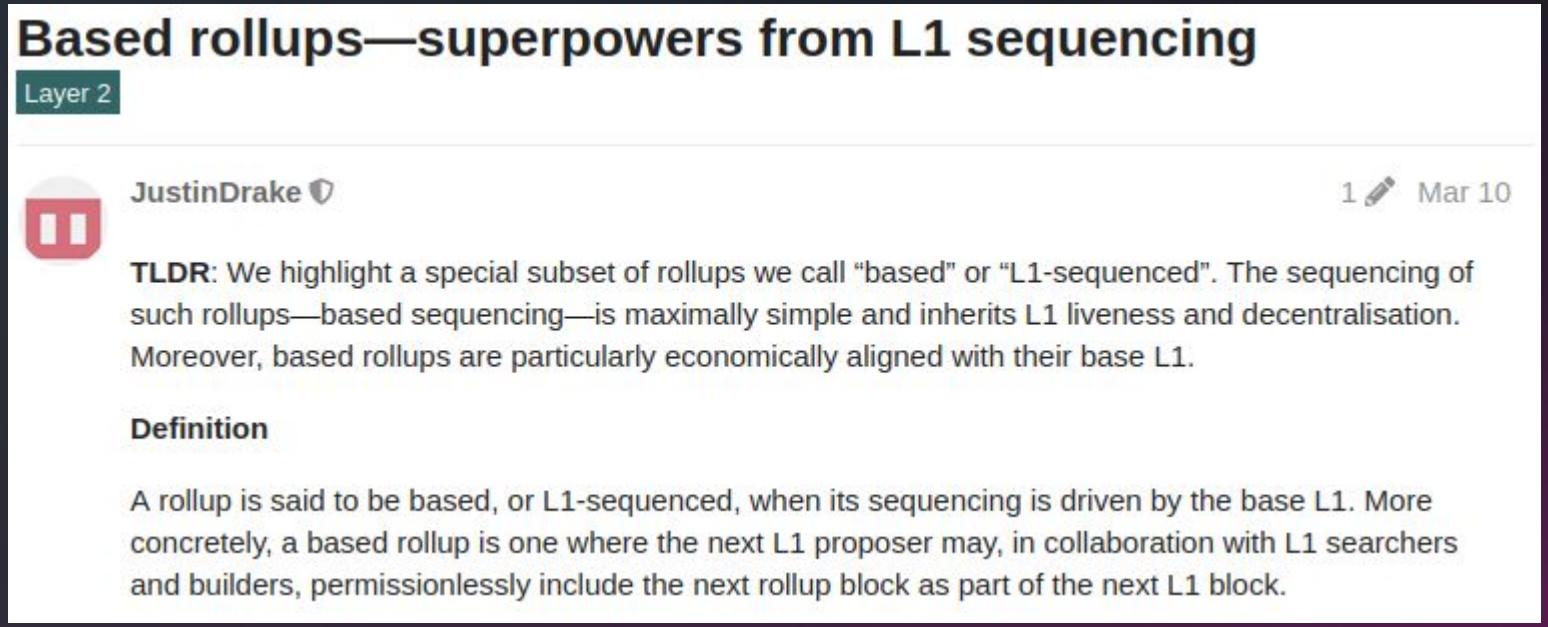
Rollup security

- Liveness
  - Need a custom validator set?
    - Easier to compromise than the 881K L1 validators
- Economic security
  - Need a custom token for sequencing?
    - Less economic security than Ethereum

Based Rollups
& Based Validators

Based Rollups - The TLDR;

Drake 2023 (ethresear.ch)



Based rollups—superpowers from L1 sequencing

Layer 2

JustinDrake 1 Mar 10

TLDR: We highlight a special subset of rollups we call “based” or “L1-sequenced”. The sequencing of such rollups—based sequencing—is maximally simple and inherits L1 liveness and decentralisation. Moreover, based rollups are particularly economically aligned with their base L1.

Definition

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 Rollups

Drake 2023 (ethresear.ch),
Espresso, Ethereum Foundation, Flashbots, Nethermind, Taiko 2023 (Twitter Space)

- Decentralization:
  - as decentralized as L1 validators
  - ~~Centralized sequencer, decentralized sequencer~~
    No sequencer, No external consensus, No escape hatch
    No single point of failure

- Liveness
  - As live as L1 validators

- Credible neutrality: no doubt about decentralization, censoring power or MEV extraction

- Allow building custom sequenced app (order book)

- Most Ethereum aligned

Based Rollups

Drake 2023 (ethresear.ch),
Espresso, Ethereum Foundation, Flashbots, Nethermind, Taiko 2023 (Twitter Space)

- MEV
  - Congestion fees (EIP-1559): L2
  - Front-running (toxic MEV): L1
  - Arbitrage: L1

- Economic security depends on ETH and not on the rollup token

Based Rollups

Drake 2023 (ethresear.ch),
Espresso, Ethereum Foundation, Flashbots, Nethermind, Taiko 2023 (Twitter Space)

Restaking

Staking refresher

- L1 stakers can reuse their stake
  - Either node runners via changing the withdrawal address
  - Or through LSTs (Liquid Staking Tokens)
- With additional rules and slashing conditions
- For extra rewards for securing a rollup

Restaking for based rollups

Restaking for based rollups

Wen TX?

Based Preconfirmations

Drake, Taiko 2023 (Twitter Space),
Drake 2023 (ethresear.ch)

- L1 proposers commit to include a transaction in a block
- Slashed if they don’t, rewarded if they do.
- Rollup app can now display a transaction ETA

What next?

Drake, Taiko 2023 (Twitter Space),
Drake 2023 (ethresear.ch)

- PreconfBoost: A preconfirmation market
- SSLE: Secret Shared Leader Election, with secret proposers/preconfirmer
- MEV
  - Frontrunning toxic MEV is going down anyway
    (Uniswap X, encrypted TX pools, ...)

The End

taiko

How restaking improves based rollup UX

Mamy Ratsimbazafy

ZK Engineering @ Taiko

mratsim

m_ratsim