

Early Observations of Based Rollups : A Case Study of Taiko

Jan Gorzny

Phillip Kemper

Martin Derka

 Zircuit

CAAW 2025, Miyakojima, Japan





Disclaimers

- This is early work, and likely will be continued; should be considered partly as a WIP and subject to limitations at the end of the talk.
- I work for **Zircuit**, not Taiko or Scroll.

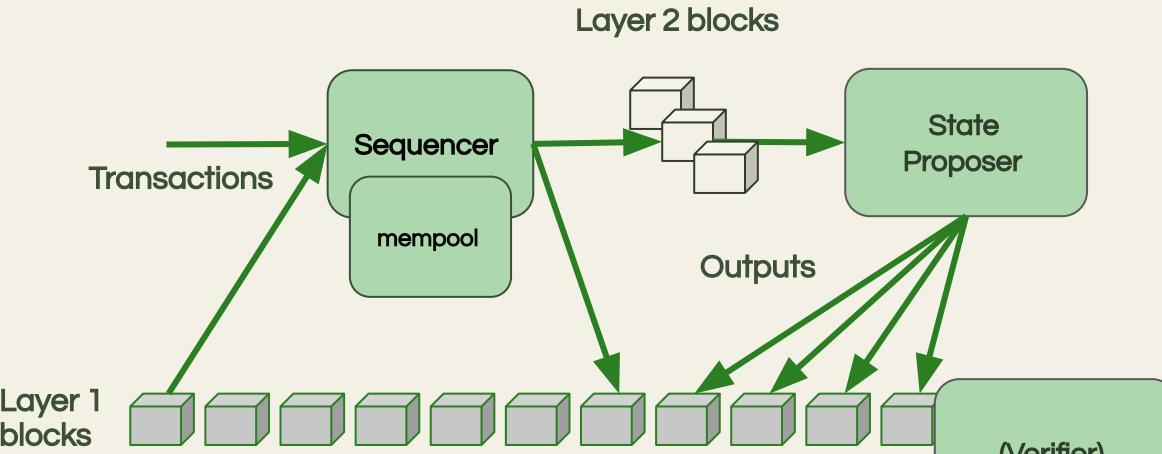




Rollups

Separate execution from consensus and post state summaries to another blockchain for security.

“Layer 2” solution on a
“Layer 1”



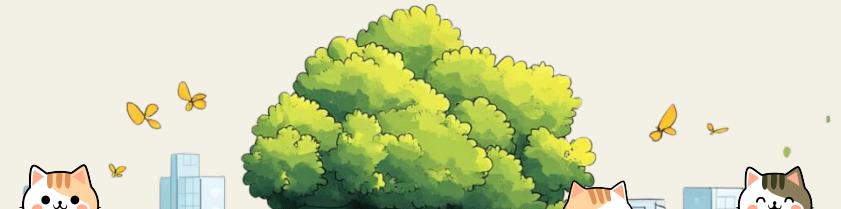
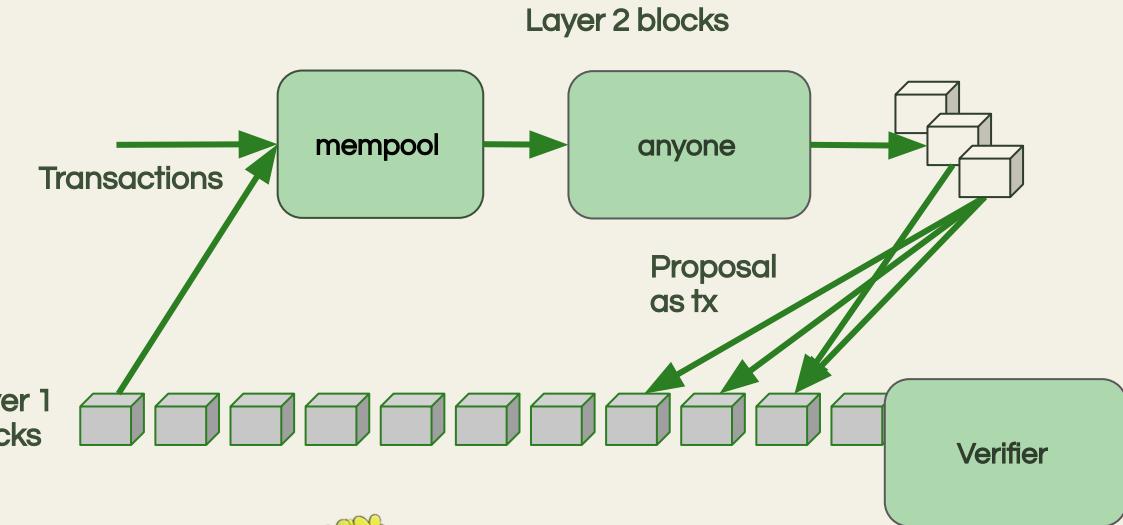


Based Rollups

"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."

Justin Drake

L2 blocks are L1 transactions.





Advantages & Disadvantages



+/-	Trait	Short Justification
+	Live ness	L2 continues to function as long as the underlying L1 continues to function.
+	Decentralization	Permissionless inclusion of the next L2 block.
+	Simplicity	No need for escape hatches (see, e.g. [24]), additional consensus, or signature verification.
+	L1 economic alignment	MEV [25] extraction on based rollups is performed by actors building L2 blocks – namely, L1 actors – and therefore any extracted value stays within the L1.
+	Sovereignty	Based rollups can still issue a governance token and use it to make decisions about the network
-	No MEV income	Block builders (L1 actors) will not necessarily be motivated to maximize L2 fees
-	Constrained sequencing	Pre-confirmations [20] are hard and the actual ordering of transactions may not be enforced by the L1 actors building the blocks.

Table 1: Advantages (+) and disadvantages (-) of based rollups according to Drake [4], along with a short justification of the trait.

Based rollups—superpowers from L1 sequencing

Layer 2



JustinDrake

1 Mar 2023

Mar 2023

1 / 26
Mar 2023

TLDR: We highlight a special subset of rollups we call “based” or “L1-sequenced”. The



Taiko

- Taiko is a zero-knowledge rollup that describes itself as a “**based contestable rollup**”,
 - “based” is as described;
 - “contestable” means that some proofs can be contested – in fact, there are tiers:
 - TEE-generated proofs can be contested by a “stronger” ZK-generated proof
 - This is not a requirement of general based rollups
- Taiko was chosen as it has the largest Total Value Locked (TVL) among based rollups at the time of writing (**\$295 million** USD on 6 January 2025)
- **Initial version** (pre-“Ontake”) **studied** due to time limitations





Dataset

From Ethereum block

19773965 (**May-01-2024** 08:03:47 AM +UTC) [Taiko contract deployed]
to

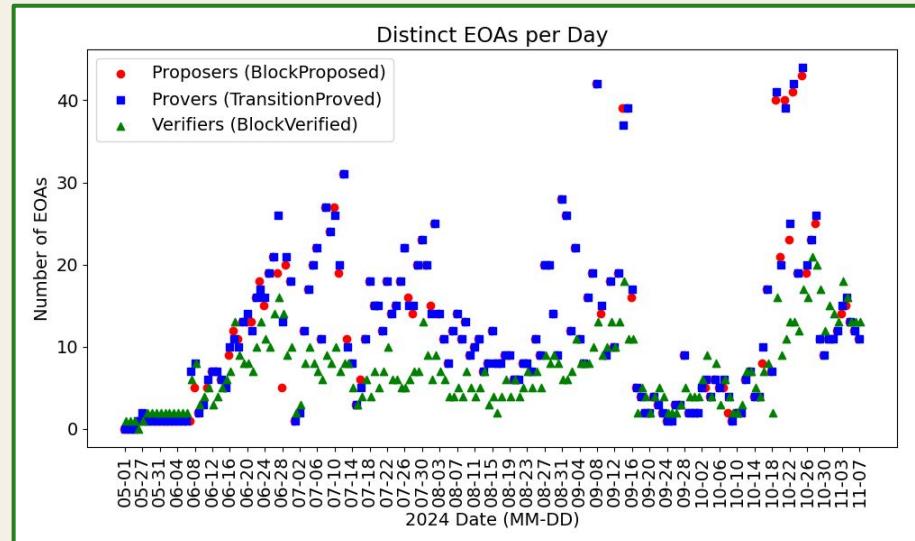
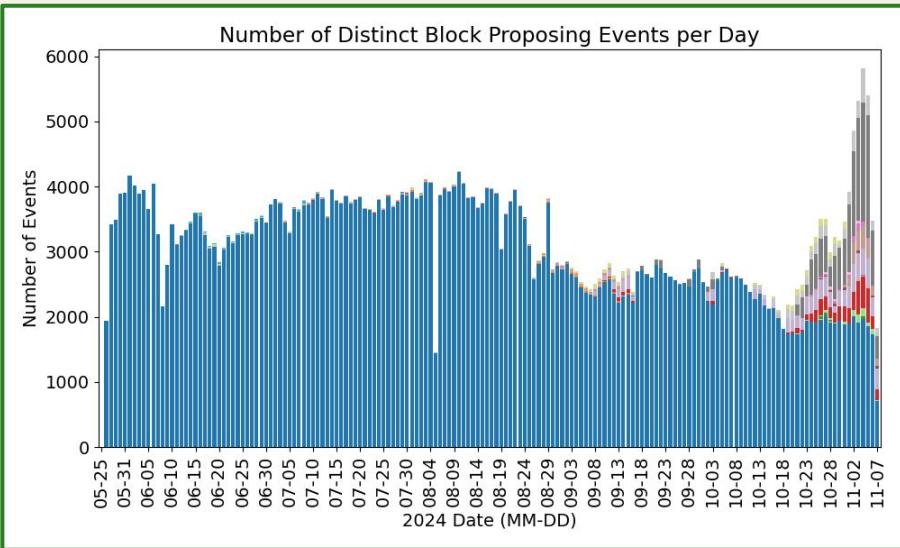
21136529 (**Nov-07-2024** 03:00:23 PM +UTC) [Taiko upgrades]

⇒ more than 6 months of blocks (1362564 blocks)



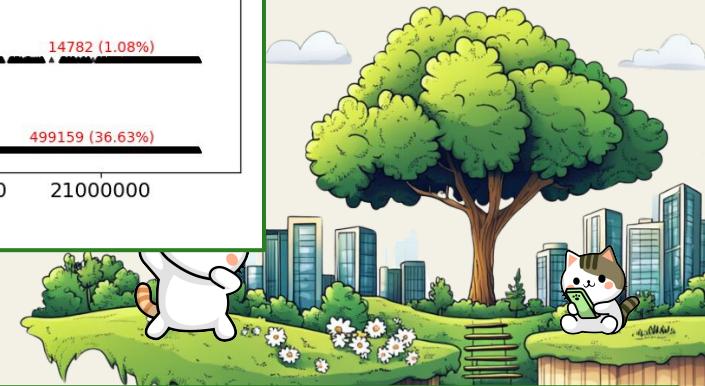
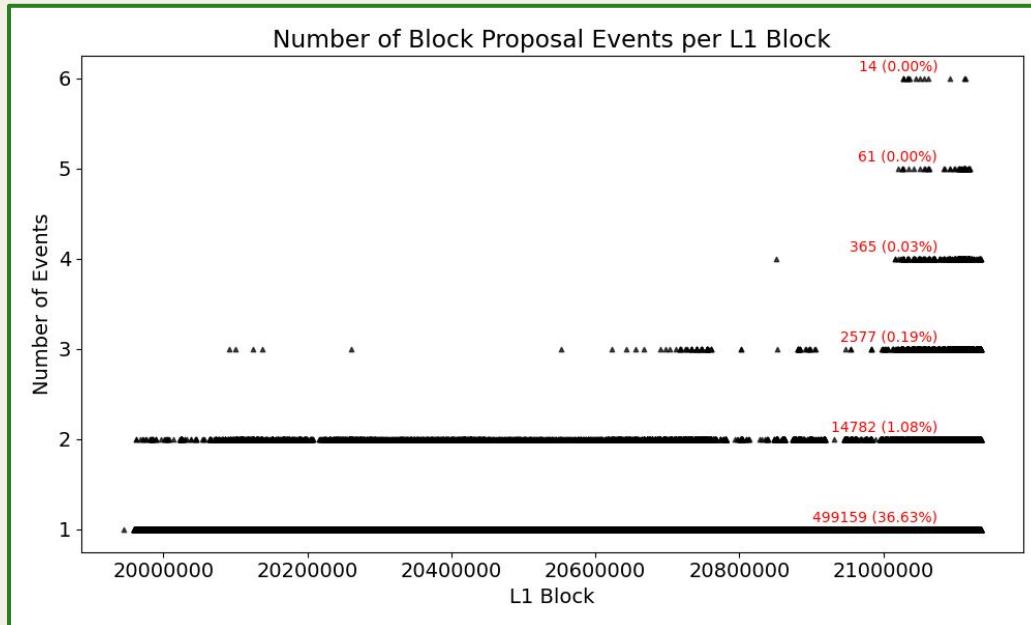


Findings - Activity



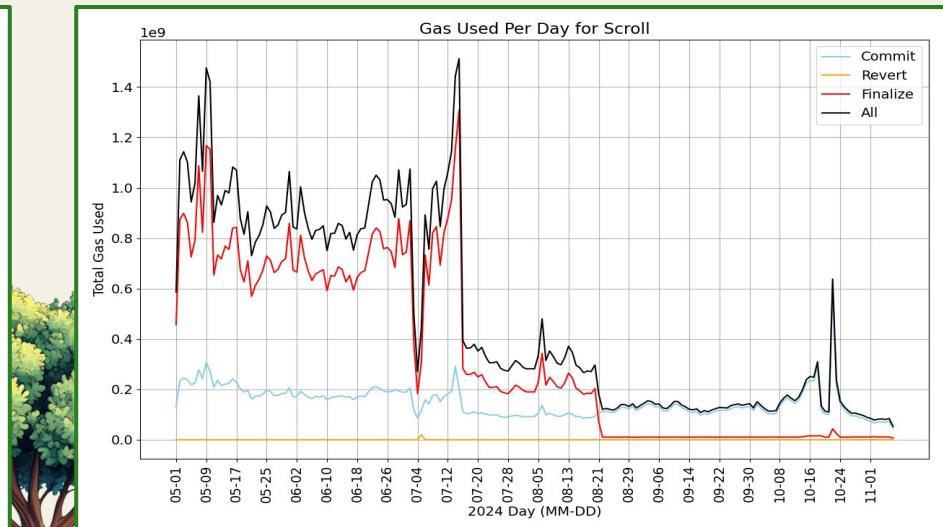
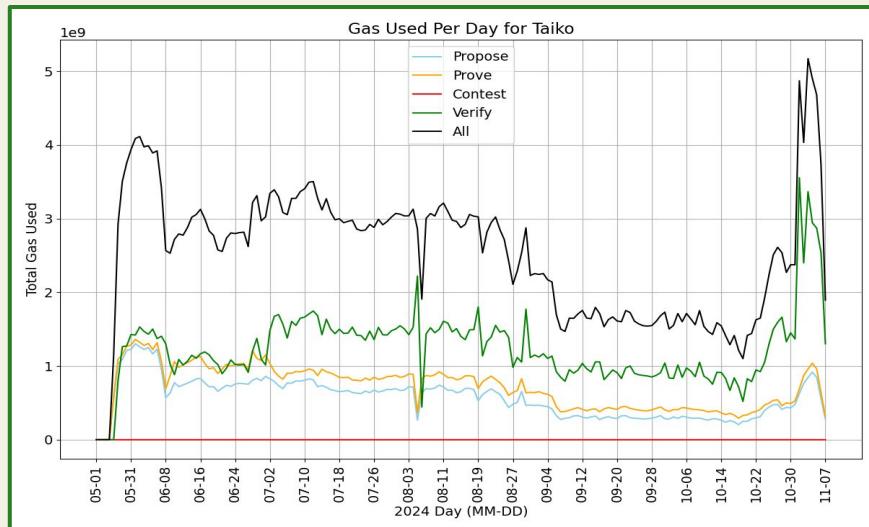


Findings - Duplication



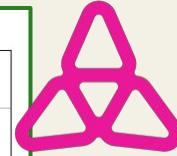
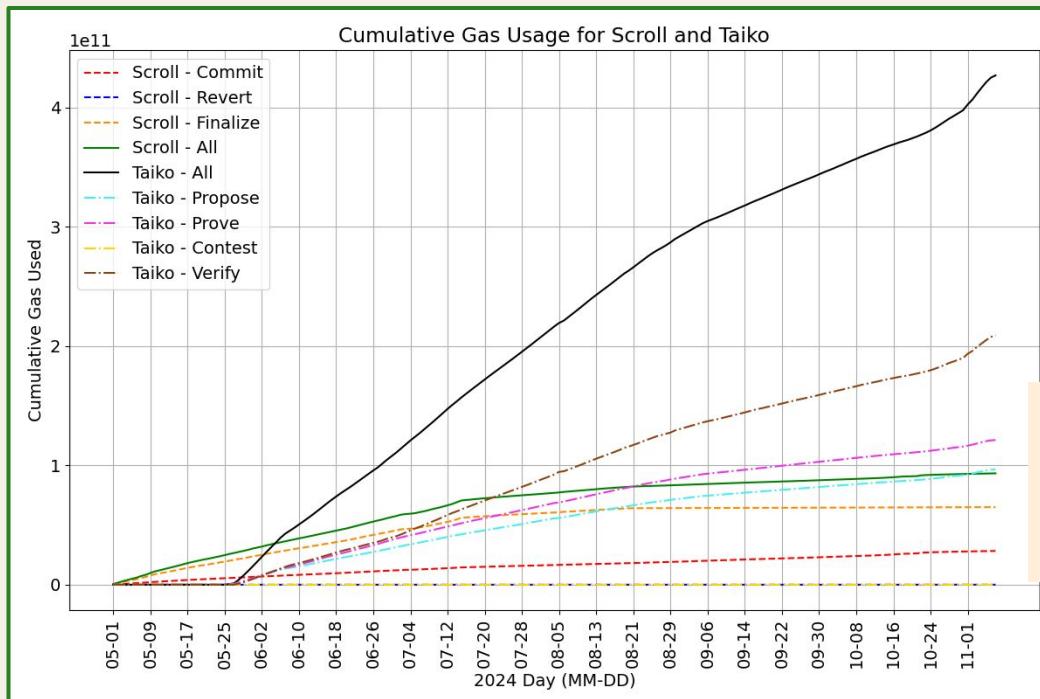


Comparison with Scroll - Gas Usage I



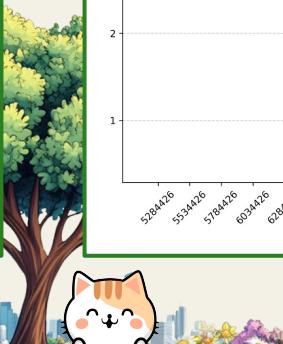
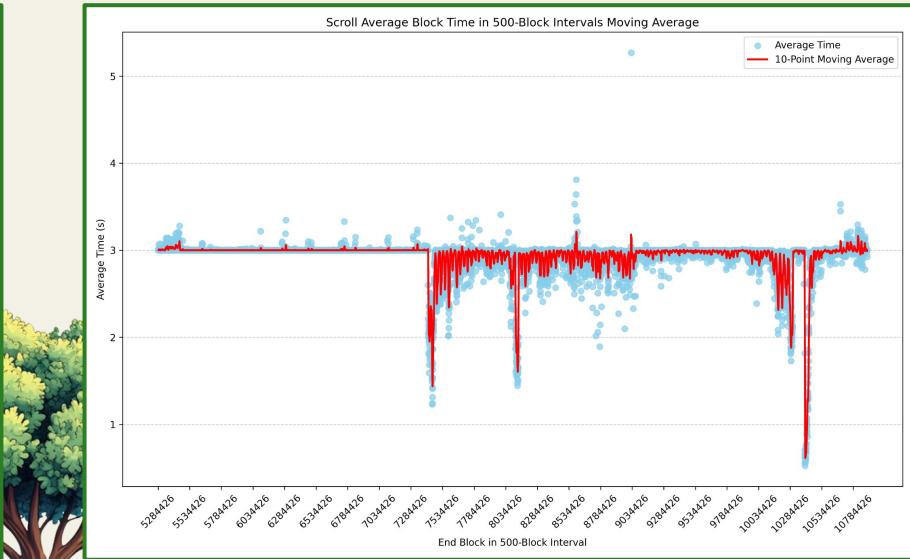
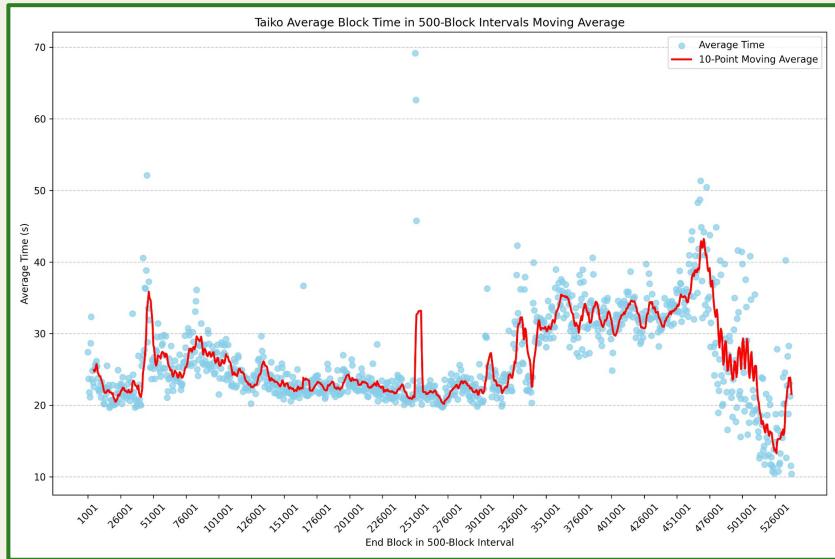


Comparison with Scroll - Gas Usage II





Comparison with Scroll - Block Time





Limitations & Threats to Validity

- Only Taiko was studied, and **only the first version of Taiko was studied** – not subsequent updates to it.
- **Doesn't capture all key metrics:** are Taiko blocks proposed during the same L1 block containing the same L2 tx? (yes: next slide →)
- Comparison may not be fair for **other reasons** (e.g., contestable proofs)
- May not have had enough usage on **Taiko for meaningful data.**





Related Work

Understanding Based Rollups: PGA Challenges, Total Anarchy, and Potential Solutions

Economics mev based-sequencing



DavideRezzoli

2 Dec 2024

Dec 2024

1 / 6

Dec 2024

Many thanks to @linoscope , @donnaoh , @Brecht , @sui414 , @pascalst ,and @cshg for their valuable feedback and comments.

How to Lose \$200K every Two Weeks

<https://ethresear.ch/t/understanding-based-rollups-pga-challenges-total-anarchy-and-potential-solutions/>





Conclusion

- Taiko, as an example of an early based rollup, was **more expensive** to operate from an **on-chain** perspective
- **Liveness and decentralization** advantages of based rollups are real
- Simplicity may be real, but “BCR” design complicates analysis
- Total chaos analysis requires additional work

Refined implementations may change results favorably – need to reiterate on this work!





Thank You

jan@zircuit.com
@igorzny (Telegram/X)

