I finally realized it when I made a prototype … the bottleneck of zkRollup isn't in L1 but in L2, to say, in proof generation.

On my laptop (Dell XPS13 9370), it takes ≈1 second to generate zkRollup proof per transaction.

So zkRollup seems not to be suitable to improve "throughputs" unless you use a very expensive EC2 instance or use many instances or invent something smarter…

However, it's still useful for "gas savings", to say, batch operations.

You can aggregate 10,000 L2 txs into a single L1 tx after ≈3 hours-long proof generation.

I have a question about this here.

In zkRollup, anyone can be an aggregator.

In other words, anyone can invalidate other aggregators' ongoing proof generation by executing valid submission to L1, even if other aggregators already spend a long time and much money to aggregate many transactions.

Is there already a workaround for this issue?