First of all, this is just a wild idea. Please don’t really use it or consider using it in practice except hackathon.

Proof in Rollup

For proving that “Rollup’s program” is executing correctly, we need to provide some commitments. These commitments can be Fault Proof and Validity Proof in Optimistic and ZK Rollup.

In order to prove and convince, we haveseveral ways other than Fault proof and validity proof:

- Authority (eg. Coinbase)
- Multi-sig (or multi-authority)
- Light Client

AI as Proof in Rollup

Current AI models, such as GPT-4, are very much like aHypercomputation or super-Turing computation model. More specifically, they are like an Oracle machine that can solve certain complex problems in a single operation, like a black box.

Thus, we can use the AI as something like an Authority, and let it reveal whether the Rollup program was executed correctly.

Rollup: Here's pre_state... Here's rollup programs... Here's transactions... Here's my output... Evaluate whether it's correct.

ChatGPT: ....

Different Styles of AI Oracle Proof

Besides the commitments should be proving that rollup program is executing correctly, we may still need to show that the commitment is generated correctly.

Optimistic Style

When challenge is submitted on the claim, we play interactive game and figure out who’s correct.

Interactive game would be executed on the chain with approximately ten back-and-forth steps (something like five questions, five ChatGPT answers).

ZK Style

We need to make the entire AI model ZK, so that the commitment itself can be executed correctly and the model can be guaranteed.

Limitations

- Accuracy of AI itself: It is difficult to test the accuracy of a generative model like ChatGPT. If we can’t guarantee the accuracy of the AI itself or go further and make the accuracy 100%, then we can’t never really use a similar solution in practice. Or we can only include AI Oracle Proof into multi-prover rollup architecture, so we can have a 3/4 multi-sig…
- Development of On-chain AI and zkML: zkML and on-chain AI can be combined together, and there is alreadyzkML that can do GPT-2. In the future, if GPT-5 zkML can be implemented with a similar high-performance solution, then different styles of AI Oracle Proof will be possible.