TL;DR

- Today we are launching OAO, an onchain AI oracle, complementary to our zkOracle offering. The OAO is powered by opML (optimistic machine learning) on Ethereum and brings ML models onchain.
- Currently, OAO supports LlaMA 2 and Stable Diffusion. Users can use these onchain models onchain.
- The future of onchain machine learning is optimistic with opML.

0. opML: Optimistic Machine Learning

a) Onchain ML

Machine Learning and Artificial Intelligence, the trendiest and most talked-about computing paradigms today, have led to an acceleration of innovation.

Implementing ML or AI onchain can give machine learning computation the advantages of current onchain computing, including:

- Fairness
- Verifiability
- Computational Validity
- Transparency

However, the convergence of AI x Crypto is facing challenges. Taking Ethereum as an example, running ML/AI model inference on the blockchain faces the following challenges:

- Network resource: In order to ensure decentralization, it is not reasonable to have all nodes running complex ML computations in 12 seconds.
- Computation limitation: Ethereum's EVM is a domain-specific language for smart contracts, and does not take into account ML and AI-related computational adaptations.

b) opML is All You Need

Some pioneers are trying to implement onchain ML using zkML. The idea is to generate a cryptographic proof for ML computations that is succinct enough to be verified on the blockchain.

However, this approach is not really practical given the restraints of current computing power, here are some examples:

- The zkML framework EZKL takes around 80 minutes to generate a proof of a 1M-nanoGPT model
- According to Modulus Labs, zkML has >>1000 times overhead than pure computation, withthe latest report being 1000 times.
- According to EZKL's benchmark, the average proving time of RISC Zero is of 173 seconds for Random Forest Classification.

In the blockchain field, there is another commonly used form of proof: the fault/fraud proof, that is commonly deployed in optimistic rollups, and that can be serve as a more practical solution to realize onchain ML.

As the inventor of opML and the first open source implementation, we are thrilled to see the growing adoption of opML. opML can run Stable Diffusion and LLaMA 2 directly on Ethereum. You can find the latest and most complete information about opML in the whitepaper.

Compared to zkML or other onchain ML methods, opML is all you need

.

[

zkML can run some small ML models onchain" & "opML can run any ML model onchain"

1876×1054 29.4 KB

](https://ethresear.ch/uploads/default/original/2X/d/d1c2419d53f447441c2def1df1bbba9fdaa22834.png)

[

Comparison between opML and zkML

1115×479 33.6 KB

](https://ethresear.ch/uploads/default/original/2X/f/f6cea93b2062a5f7e13ba725e7320fb9eeebe67b.png)

Comparison between opML and zkML

1. OAO: Onchain AI Oracle

a) Introduction

We are thrilled to announce the deployment of opML on the Ethereum network.

OAO, with opML at its core, allows anyone to use onchain ML inference on the blockchain.

[

OAO

1237×630 383 KB

](https://ethresear.ch/uploads/default/original/2X/a/ac81db5637c1a99e8b34b8454051d622d63c52f0.png)

OAO is a set of smart contracts including:

- opML contract, for fault proofs and challenges to ensure ML is onchain and verifiable
- AIOracle contract, for connecting the opML node with onchain callers to process ML request and introducing any ML model
- User contract, to initiate and receive AI results from OAO. This can be any contract customized by developers

b) Architecture and Workflow

The specific architecture of the OAO is as follows. The user's contract can initiate an AI request by calling the OAO, the OAO will publish the request to the opML node for processing, and then the OAO will return the AI result to the user.

[

Untitled (6)

1328×610 82.3 KB

](https://ethresear.ch/uploads/default/original/2X/6/607e99be7e74da694bf80872bf5d2af172e69939.png)

In terms of workflow, we need to break down the explanation into two parts.

Usage process:

1. The user contract sends the AI request to the OAO on chain, by calling the requestCallback

function on the OAO contract.

1. Each AI request will initiate an opML request.
2. The OAO will emit a requestCallback

event which will be collected by the opML node.

1. The opML node will run the AI inference, and then upload the result onchain.

Challenge process:

1. The challenge window starts right after step 4 in the previous section.
2. During the challenge period, the opML validators (or anyone) will be able to check the result and challenge it if the submitted result is incorrect.
3. If the submitted result is successfully challenged by one of the validators, the submitted result will be updated onchain.
4. After the challenge period, the submitted result onchain is finalized (results can not be mutated).

5. The challenge window starts right after step 4 in the previous section.
6. During the challenge period, the opML validators (or anyone) will be able to check the result and challenge it if the submitted result is incorrect.
7. If the submitted result is successfully challenged by one of the validators, the submitted result will be updated onchain.
8. After the challenge period, the submitted result onchain is finalized (results can not be mutated).
9. When the result is uploaded or updated onchain, the provided result in opML will be dispatched to the user's smart contract via its specific callback function.

Here's the annotated detailed workflow:

[

Untitled (7)

1170×587 91.6 KB

](https://ethresear.ch/uploads/default/original/2X/9/99809b2b16e4232413248ce8add404351b6ee416.png)

c) Deployment and Usage

Here are the OAO contracts deployed onchain:

- AIOracle: https://sepolia.etherscan.io/address/0xb880D47D3894D99157B52A7F869aB3B1E2D4349d
- Prompt (example user contract attached to AIOracle): https://sepolia.etherscan.io/address/0x5d6963003Ad172Fd1D2A2fD18bB3967eA7Aef1a2

Currently, you can use the onchain ML model by initiating an onchain transaction by interacting with the prompt contract. We have uploaded two models to the OAO: LlaMA 2 (LLM model) and Stable Diffusion (Image Generation Model).

Interact on ora.io

You can directly interact with OAO at:ORA.

Interact on Etherscan

Here's the usage guide if you want to play with it directly on Etherscan. You can also check out thevideo guide with all the steps:

1. Initiate AI calculation

Go to the write contract tab, set modelId

as 0 (LlaMA 2), and enter your prompt in human-readable text.

[

screenshot

1382×396 26.4 KB

](https://ethresear.ch/uploads/default/original/2X/4/4b83971991365d970dd364c752a7cd25e1119e47.png)

1. See AI result

Go to the read contract tab, set modelId

as 0 (LlaMA 2), and enter your previous prompt.

[

截屏2024-01-24 上午7.01.27

1382×574 39.2 KB

](https://ethresear.ch/uploads/default/original/2X/e/e88d35df6a87f3b506f6134de67b2e090a250517.png)

2. The future of onchain machine learning is optimistic

.

Partners and Use Cases

At this stage, we are experimenting with OAO and opML together with several projects:

- 7007.studio: The next generation marketplace to secure and govern AI models.
- MyShell: A decentralized and comprehensive platform for discovering, creating, and staking AI-native apps.
- Space Runners: A design tool built for fashion designers, powered by Stable Diffusion.

We are actively exploring the following use cases and directions:

- AIGC NFT (ERC-7007), 7007 Studio won the Story Protocol Hackathon
- zkKYC using facial recognition based on ML
- Onchain AI Games (e.g. Dungeon and Dragons)
- Prediction Market with ML
- Content Authenticity (deepfake verifier)
- Compliant programmable privacy
- Prompt Marketplace
- Reputation/Credit Scoring

Future of Onchain ML

With an OAO, anyone and any contract can experience the magic of onchain ML. An OAO is decentralized and verifiable with the help of opML and its optimistic mechanism.

For our OAO, we'll onboard more ML models. With our opML framework, you can Bing Your Own Model. Anyone is welcome to integrate with the OAO. And we have many more exciting releases coming in the future!

Optimistic machine learning will be the future of onchain machine learning. The future of onchain machine learning is optimistic!