Results of RetroPGF 3 were published on January 11th . This post is providing more insights into the results calculation process as well as next steps to generate insights on the outcomes of the third round of Retroactive Funding.

Results calculation

RetroPGF 3 votes are private, and are not revealed to the public. This is designed to protect the integrity of badgeholders' voting choices, free from external pressures or influence.

Each badgeholder signs the collection of their votes (i.e. ballot) with their private key, so that only authentic votes are counted. To calculate results, the signatures are verified and the relevant voting algorithm is applied. To verify the correct implementation of the voting algorithm, the Agora and OP Labs teams both developed independent implementations of the results calculator.

You can find Agora's implementation here and OP Labs implementation here.

Analyse results

To allow for insights into the voting behaviour of RetroPGF 3 and the impact of different voting algorithms on the results, anonymized voting data has been published. The dataset includes the individual votes that were submitted on each project, while not revealing which badgeholder casted them or which ballot they belonged to. This approach was preferred over anonymised ballots, as they could possibly compromise the badgeholder identity. To safeguard against malicious activities, votes have been rounded to the nearest thousand.

Existing analyses of the results:

- @amy and @ccerv1 have published a post on simulating the impact of different voting algorithms
- @ccerv1 from OS Observer has published a blog post looking into different characteristics of the results and another post on evaluating the anonymised voting data

-@Pr0 has published a post with visuals on the distribution of votes and examined the difference between a median and a mean (used in RetroPGF 2) based results calculation

- Your Analysis here!

Verify the results soon™!

EZKL has received a grant to create ZK proofs on the correctness of RetroPGF results. This "ZK audit" proves the fairness and correctness of voting outcomes for all stakeholders while preserving all desired confidentiality properties. This offers new affordances for governance around necessarily private data or models.

The final proofs will be published to a website (coming shortly) that enables badgeholders, recipients, and Optimism community members to verify them using the public information associated to the round. The proof, verifiable by everyone, includes:

- Checking badgeholder signatures and that each vote was counted exactly once,
- Extracting the data from the ballots,
- Running the allocation algorithm to show the final results are correctly derived,
- Using ZK to preserve the privacy of the badgeholders, and to prevent badgeholders from proving that they voted a certain way.

@LauNaMu was essential in getting this initiative off the ground by approaching relevant teams with the requirements for a ZK-proof of the RetroPGF results, identifying possible candidates and introducing the Foundation to the EZKL team.

Grant delivery

The delivery of RetroPGF grants has started. You can follow the progress on Superfluid or gain more insights via this dedicated dune dashboard created by 0xkhmer.

Following KYC approval and address confirmation, tokens are streamed to RetroPGF recipients over a 90 day period, beginning on the 3rd working day of the month following KYC approval and address confirmation. Recipients have til the end of January 2025 to complete the process. Failure to complete the process in time will lead to the awarded OP tokens being returned to the RetroPGF token allocation.

If you're a recipient, you received an email with guidance on how to claim your grant. If you experience any problems, please email retropgf@optimism.io