AIP Idea: Bug Bounty Program for AIP-21

Proposal Name: Bug Bounty Program for AIP-21

Proposal Category: Process

Abstract:

As we near the launch of the ApeCoin staking system outlined in AIP-21 and AIP-22, we propose taking additional measures to ensure the DAO is following smart contract security best practices. This proposal uses treasury assets to fund a 1 million $APE bug bounty program with Immunefi, and partners with Llama to help design, implement, and run operations of these initiatives.

This proposal would go into effect ahead of staking rewards beginning to accrue with AIP-21. The smart contract for AIP-21 is currently live on testnet so the bug bounty program can go into effect shortly after the AIP passes.

This proposal will delay staking rewards by roughly 3 weeks. If this proposal passes, staking rewards would begin accruing on 12/7, rather than 11/14. Though the 3 week delay is unfortunate it is vastly preferable to a security breach as a result of not following security best practices. We believe it is very beneficial for the DAO to approve this program.

Motivation:

We have all seen the headlines around massive protocol hacks. Chainalysis released a report yesterday saying that over $3 billion has been stolen by hackers this year alone (tweet 2, article 2). A couple weeks ago, a vulnerability in the official Binance Smart Chain bridge allowed an attacker to run away with over $100M in stolen funds. Given this staking program uses a new architecture that includes committing NFTs, we believe it is prudent to run a bug bounty program ahead of any rewards being accrued to holders. . Traditional audits can mitigate some of the smart contract risk, but audit contests and bounty programs provide additional layers of security to identify bugs and keep users safe.

AIP-21 is launching soon. The smart contract has already been through at least one audit (link), but we believe a short code4rena audit contest + dedicated bug bounty program is imperative given the expected size of the program (17.5% of APE supply over 3 years).

Rationale:

17.5% of total APE supply will go towards the staking program outlined in AIP-22. Given the significant allocation of treasury resources, we believe an ongoing bug bounty program is a prudent initiative.

The bug bounty program would allow us to incentivize a community of white hat hackers to find potentially costly bugs with the staking program. An ongoing program will allow us to address new vulnerabilities as they are discovered, ensuring APE holders are safe.

The bug bounty program will be funded as long as staking is live, or until the APE requested has been distributed to white hat hackers. Security is an ongoing effort, not a one-time thing.

Specifications:

1 million $APE budgeted for a bounty program for AIP-21.

Implementing a bug bounty program requires upfront setup and ongoing maintenance. This includes:

1. Designing the program specifics. This includes designing the rules and rewards to optimize success. In the interest of time, we recommend Immunefi and Llama be given the flexibility to architect the program specifics.
2. Setting up a team to process reports. We will need to review each bug reported, triage its severity, and escalate as needed. Bugs include minor bugs that are not critical, but still need to be reviewed.
3. The review process will require at least 1-2 engineers (from Horizen Labs' team) as well as a system designed for escalation as needed.
4. Ongoing maintenance, such as reviewing and adjusting the program as appropriate
5. Operational support in ensuring payout of rewards.

Once the program is designed and live, it will run for 2 weeks prior to the smart contract being deployed. Following the smart contract deployment, there will be a 2 week pre-commitment period for staking as originally intended.

After staking goes live, the bug bounty program will operate in perpetuity, co-managed by Immunefi and Llama. After launch, the program may be adjusted from time to time to ensure the most optimal structure.

Ensuring the right incentives and program structure are critical to have an effective bug bounty program. Immunefi is an industry leader in the space, and has the experience to support and implement this program on behalf of the DAO. Operationally, the DAO will need a representative to coordinate between Immunefi and the Horizen smart contract engineers to operationalize the program. Llama has offered to support the DAO in this effort.

Working with Llama

Llama is a DAO that contributes to leading protocols and communities such as Aave, Nouns, Uniswap, dYdX, Lido, FWB, and Maker. They work on smart contract development, treasury strategies, liquidity incentives, grants programs, and analytics dashboards. Their contributors are among the most active in crypto governance and include engineers, data scientists, DeFi strategists, quants, and accountants.

To run an effective bug bounty program, the DAO needs an experienced team to represent their interests and coordinate between all the different stakeholders… Llama will collaborate with the Immunefi team to design the parameters of the bug bounty program and coordinate between all the different stakeholders. Llama will also be the first point of contact as potential vulnerabilities are reported. Llama will make frequent governance forum posts and host twitter spaces to ensure the ApeCoin community stays informed through this process.

A bug bounty program cannot go live until the DAO has secured funding for the rewards. Given the timeline outlined here, we have requested Llama and Immunefi be given discretion to architect the specifics of the program, using a flat fee at the start and transitioning into a scaling reward paradigm once staking formally begins. The $APE will be allocated as the teams see fit to best drive security outcomes with check-ins every 3 months to share the status of rewards.

Designing and implementing the program will take time and effort but Immunefi and Llama are aware of the community timeline.

Steps to Implement:

Once approved, Immunefi and Llama will sign a grant agreement with the Ape Foundation.

Immunefi and Llama will collaborate to design a program that maximizes efficacy and minimizes time required.

Timeline:

- Voting for this AIP will end 11/3. Llama and Immunefi will have up to 7 days to design and implement the bug bounty program. Bug bounty program will take effect as soon as the parameters and scope are agreed upon.
- The bug bounty program for the Goerli testnet staking system smart contract goes live on 11/10.
- Bug bounty program will run for 2 weeks on test net, to ensure no critical vulnerabilities are surfaced.
- Smart contract is deployed to mainnet on 11/24.
- Users will have 2 weeks to pre-commit their tokens and NFT for staking.
- Bugs will be addressed as they arise, but assuming no critical bugs are found, the smart contract should be funded and rewards begin accruing on 12/7.

Bounty program will remain in place until the earlier of: a) the staking program ending; or b) the prize pool being depleted.

- If and when funds in the bounty program are depleted, the program committee will present a new proposal for further funding.

This proposal will delay staking by roughly 3 weeks. Originally, staking rewards were expected to go live on 11/14. Though the 3 week delay is unfortunate it is vastly preferable to a security breach as a result of not following security best practices. We believe it is very beneficial for the DAO to approve this program.

Overall Cost:

A total budget of 1 million $APE (roughly $4.5 million based on 30-day average $APE price).

Operational costs are minimal, and the majority of the budget will be used to fund prizes for the program.

Bounty rewards will only be paid if bugs are found, and any funds unallocated at the end of the staking period will be returned to the DAO.

The funds requested will be allocated as following:

- Bug bounty rewards can be tiered based on the severity of the exploit, or can be based on % of value at risk. Llama and Immunefi will structure the program within the 1 million $APE budget being requested.

- 10,000 $APE (~$45,000) paid to Llama upfront, for operating the ongoing program on behalf of the DAO. Llama commits to not selling their $APE for at least a year, and plans to use these tokens to actively participate in the ApeCoin DAO.
- 10% performance fee paid to Immunefi on any vulnerabilities discovered (i.e. if a white hat hacker is paid $100,000 for a bug they discovered, Immunefi will receive $10,000)