Abstract:

AIP-134 recently requested budget to support the set up of a bug bounty program for the staking system. This proposal suggests we expand the budget and timeline + build a process that supports all future AIPs who's ongoing operation poses risk to ApeCoin community members. We propose using treasury assets to fund a 1 million $APE bug bounty program with Immunefi, and partner with Solidity.io to help design and implement the program + onboard new AIPs as they launch.

This proposal would unlock the first $20,000 $APE immediately to fundSolidity.io costs for program set up, and the rest made available at program launch to fund white hat hackers until depleted. At this point the community can draft a second proposal to continue funding.

We believe it is very beneficial for the DAO to approve this program since the absence of this infrastructure and process leaves the DAO with only two options:

1. Every new AIP must create a second AIP to request additional bug bounty funding which poorly allocates hacker rewards at scale.

2. Accept the security risk.

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 6, article 2 4). 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 that many new AIPs introduce smart contract risk we believe it is prudent to run a bug bounty program that's available to all future AIPs to tap into. 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-134 recently secured budget and set a process to secure the staking contract, but as we prep to launch the ApeCoin marketplace I personally want to ensure the same level of security for the community. Because we're a start up with limited funding we can't fund massive rewards on our own, and others will face this exact problem in the future so we want to set this up for future proposals as well.

Rationale:

The bug bounty program would allow us to incentivize a community of white hat hackers to find potentially costly bugs with the future AIPs. 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 funds remain and funds are only paid out when vulnerabilities that meaningfully reduce community risk are discovered and addressed.

Specifications:

1 million $APE budgeted for a bounty program.

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

Designing the program specifics. This includes designing the rules and rewards to optimize success. In the interest of time, we recommend Immunefi and Solidity.io be given the flexibility to architect the program specifics.

Launching the program. Communicating the program to the broader ApeCoin ecosystem at launch to explain severity levels, rewards, and rationale for how the program was constructed.

Adding new partners. Onboarding new AIPs that expose ApeCoin community members to smart contracting risk as they launch leveraging the established system.

- As part of this Solidity.io will be responsible for onboarding new vendors along side Immunefi and defining budget and payouts for the AIP-specific BBP.

Community comms on payouts. Sharing updates on payouts from the bug bounty program on a quarterly basis.

Ongoing maintenance, such as reviewing and adjusting the program as appropriate

Operational support in ensuring payout of rewards.

Once the program is designed and live, the bug bounty program will operate in perpetuity, or until funds are depleted, co-managed by Immunefi and Solidity.io . 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. Solidity.io has offered to support the DAO in this effort.

Working with Solidity.io

Solidity.io is a full-stack Web3.0 solutions firm and product incubator focused on providing blockchain development services, smart contract solutions, and audits. Solidity.io is run by MAYC and ApeCoin DAO member Alex McCurry.

To run an effective bug bounty program, the DAO needs an experienced team to represent their interests and coordinate between all the different stakeholders… Solidity.io will collaborate with the Immunefi team to design the parameters and payouts for the bug bounty program and coordinate between all the different stakeholders through implementation at which point AIP authors will be responsible for managing communication with hackers as requests come in.

Steps to Implement:

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

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

Timeline:

When this AIP is approved, Solidity.io and Immunefi will have up to 30 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.

AIPs will be onboarded from there starting with the ApeCoin Marketplace built by Snag Solutions. The program will run from there with new AIPs onboarded as they've been audited and meet requirements for risk (in $$) necessary to justify bounties for their product.

The program will end if the community creates a proposal for it to end and unused funds would be returned.

This proposal will not delay the launch of the ApeCoin marketplace.

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.

The program will end if the community creates a proposal asking to cease and unused funds would be returned.

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 riskSolidity.io and Immunefi will structure the program within the 1 million $APE budget being requested. All budget not listed below will go directly to white hat hackers.

1. 20,000 $APE (~$60,000) paid to Solidity.io upfront, for operating the ongoing program on behalf of the DAO.
2. 20,000 $APE annually for each year the program runs with the first year paid 6-months following launch and every 12-months after.
3. 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)