Original Proposal

Original Proposal here.

Reason for Return

In January we submitted AIP-155 without identifying and addressing concerns from some large voters which led to a failed vote despite 80%+ of individual wallets supporting the proposal. In the process we talked to many community members and heard:

1. Multiple 1 million $APE budgets for separate security proposals is too costly.
2. The full budget isn't needed based on current assets at risk given the smaller scale of current DAO funded programs outside of staking.
3. Mid-term, everything should be combined into a single program.
4. An 'ongoing' proposal that never ends & returns funds doesn't set up the DAO to optimize the spend/program in the future based on success of the initial pilot.

Resubmission Updates

1. We're reducing the request to 500k $APE to fund all non-staking programs, with a commitment to submit a follow up proposal after May when AIP-134 can be modified.
2. The new request will be submitted by Alex McCurry andSolidity.io as the administrators of the unified bug bounty program within 60-days of AIP-134 becoming eligible for modification.
3. This proposal will create a single funding source for the program without requesting additional funding.
4. We're modifying the initial proposal to a one-year term after which point any unused funds will be returned to the DAO unless the DAO decides to extend via vote.

Abstract:

This proposal expands on AIP-134 which sets up a bug bounty program for staking to fund a scalable bug bounty program and onboarding process that supports all AIPs that create smart contract risk for the ApeCoin community. We propose using treasury assets to fund a (50%) reduced, 500k $APE bug bounty program with Immunefi as a tech partner and Solidity.io designing and implementing the program + onboarding new AIPs.

After incorporating community feedback from our previous proposal, we've cut the budget by 50%, reduced the term from ongoing to 1-year, and will propose an amendment to AIP-134 when it becomes modifiable in May to combine budgets and return excess funds to the DAO. This delivers a total budget reduction of up to 500k $APE to the DAO while ensuring critical security infrastructure for all AIPs is established.

This proposal requires a total cost of 30,000 $APE to fundSolidity.io costs for program set up, as well as 1 year of program operations and administration, with the Bounty Reserve being made available at program launch to fund white hat hackers. The community can draft a second proposal to continue funding after the initial 1 year pilot program or return funds.

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 several negative outcomes:

1. Every new AIP must create a second AIP to request additional bug bounty funding, which poorly allocates hacker rewards at scale, and poorly allocates $APE. (ie. 1M $APE in the staking bounty program without use)
2. DAO and community users accept security risks across ANY AIP-backed infrastructure without a BBP in place.

Motivation:

We have all seen the headlines around massive protocol hacks. Chainalysis released a report saying that over $3 billion was stolen by hackers last year alone. 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. If we truly want to set up the DAO to incubate successful projects and build key infrastructure this program is critical to implement. We've seen strong resonance from other successful AIP-authors that this proposal is critical infrastructure for them to scale while mitigating risk to the community.

AIP-134 previously received funding to secure the staking contract, but we want to ensure the same level of security for the community on all other proposals that earn the ApeCoin community's trust. Because we're a start up with limited funding we can't fund massive rewards on our own, and others like NiftyKit, ThriveCoin, and many future authors will face this exact problem so we want to set this up once to scale for everyone.

[

602×782 84.9 KB

](https://global.discourse-cdn.com/apecoin/original/2X/9/9a32471c44c4b18b3cbe07ece7befc1be69dbfe3.png)

Q4 2022 hacks incident report. Over $1.2bn lost - CertiK

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.

[

1600×897 479 KB

](https://global.discourse-cdn.com/apecoin/original/2X/6/6811e27a521a681dee6030f01b811e2b3fa02e86.png)

Specifications:

500k $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.

Further implementation plan detail included here: AIP - 155 Informational: Planned Implementation Process

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 BAYC and ApeCoin DAO member @alexmccurry and will be personally managed and administered by long-time community member and Solidity.io CSO @8uddha.

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.

Bounty program will remain in place until the prize pool is 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 not delay the launch of the ApeCoin marketplace.

Launch Partners

As a testament to the demand for the program and our commitment to deliver utility to the DAO, the BBP team has already identified the programs initial launch partners. Three of which include passed AIPs that are introducing software infrastructure into the DAO, with the remaining being Boring Security, a trusted resource and security ally of ApeCoin DAO.

Examples of initially support AIP's planning to use the program:

1. ApeCoin Marketplace led by Snag Solutions built by us
2. NiftyKit and their token minting platform built by @4437
3. Thrivecoin with their Thank $APE rewards program for community participation built by@thrivegiraffe

[

1600×900 409 KB

](https://global.discourse-cdn.com/apecoin/original/2X/8/809c484d2a994c02bc06fd4b3143ef87bd4e01a5.png)

Overall Cost:

A total budget of 500k $APE (50% reduction)

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 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 riskSolidity.io and Immunefi will structure the program within the .5 million $APE budget being requested. All budgets not listed below will go directly to white hat hackers.

1. 30,000 $APE paid to Solidity.io, for program set up, as well as 1 year of program operations and administration for operating the ongoing program on behalf of the DAO.
2. 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)

Proposals submitted to the AIP Ideas category can be vague, incomplete ideas. Topics submitted here are not required to be submitted as a formal AIP Draft Template, however, you may still use the template if you wish.