Introduction:

Solidity.io is proud to support the ApeCoin community in facilitating an ongoing bug bounty program for all AIPs. Given our experience with leading the audit for the ApeCoin DAO marketplace, as well as our deep expertise in end-to-end web3 solutions, we, as fellow apes and ApeCoin holders, look forward to serving this critically needed role as a proactive preventative measure.

As our community's holders are often targets for social engineering, exploits, and hacks, we know that security is critical to enable the growth of ApeCoin usage and holders.

We know that AIP 134 was an effort at a fix for this, however, we were disappointed in how limited it was in scope (specific to staking only) and the lack of access for other AIPs to receive funding and resourcing to run key preventative security programs to protect their software infrastructure and communities. We believe our role can help enable efficiencies to operationalize the bug bounty program in terms of onboarding, bug identification, bug remediation, bug reward payout, and ultimately return of unused pooled funds across all existing and future AIPs.

Key Roles and Responsibilities

This Bug Bounty Program is a shared responsibility between AIP authors, Immunefi,Solidity.io, white hat hackers, and the broader ApeCoin community.

Solidity.io will be responsible for the following:

1. Initial setup of the program and coordination between AIP authors onboarded, Immunefi, and the community
2. Onboarding of future ApeCoin DAO-approved AIP authors
3. Monthly communication (via Twitter Space or similar) on example bugs, latest bug findings, and general bug bounty program Q&A
4. Coordination of quarterly reporting, which includes bug status, findings, and payouts.
5. Review bug payouts prior to communication with white hat hackers, to ensure a balanced view of technical severity (as defined by Immunefi and Solidity.io standards) and community impact. Solidity.io has the final decision on payouts.

AIP authors will be responsible for:

1. Self-identifying and requesting onboarding via the Solidity.io website contact form. (A specific page will be added to the Solidity.io site in Q1 with information on BBP applications)
2. Definition, Scope, and Program oversight of bug bounty program specific to their AIP.
3. Time availability with Solidity.io for onboarding, including walkthrough and review of AIP-specific program(s).
4. Onboarding (with solidity.io guidance) to the Immunefi platform, including "targets" for bug bounty
5. Review of all identified bugs for associated applicable AIPs and facilitate timely remediation
6. SLA requirement of 48-hour response to any questions or requests raised bySolidity.io or Immunefi.
7. SLA requirement of 72-hour lead time to provide status updates for monthly updates and quarterly reporting
8. Failure to align to #6

and #7

SLAs will result in removal from the bug bounty program. AIP authors can request to be re-onboarding with a trial period.

Immunefi is responsible for:

1. Bug Bounty platform to facilitate the metadata and data capture for program criteria, targets, and impact.
2. Consumption of targets from AIP authors
3. Definitions and standards for impact based on existing standards defined by Immunefi (with opportunity for input from Solidity.io to adjust) and provide clear communication to community on types of bugs and rewards
4. Management of 1M $APE funds
5. Providing timely and relevant information to the Solidity.io team prior to any reward communication
6. Acceptance of Solidity.io decision to override or adjust payout with reasonable reasoning and commentary provided.

7. SLA requirement of 72-hour lead time to provide bug bounty program reporting for monthly updates and quarterly reporting to ApeCoin DAO community. Ideally, if there are major bugs found, Immunefi, AIP authors, and Solidity will collaborate to provide clear and concise communications to the community.

Who can participate:

Overall, anyone is able to participate in the bug bounty program. Those interested in participating will need to set up an account on Immunefi. Individual AIP owners will provide a framework that allows for participation by all, but also the ability to protect IP, proprietary processes, and non-public code blocks. Solidity.io will report on any instances where access is limited and provide recommendations for either formal audit (excluded from bug bounty funding) or for recommendations on white hat hackers willing to test under NDA.

Link to AIP 155: AIP-155: Should we fund an ongoing bug bounty program for all AIP's that introduce security risk?