

Ethereum Protocol Attackathon Sponsorship

Non-Constitutional

Abstract

This proposal seeks funding from the Arbitrum DAO to support an “Attackathon,” a large-scale security audit event organized by the Ethereum Foundation and hosted on the Immunefi platform. The Attackathon will focus on enhancing the security of the Ethereum protocol through three phases: education, active code hunting, and result evaluation. The initiative aims to raise over \$2 million, with \$500,000 already committed from the Ethereum Foundation. This effort is crucial for ensuring the stability and security of Ethereum, which is vital for maintaining the reliability of projects on Arbitrum.

Motivation

As a Layer 2 on Ethereum, Arbitrum relies heavily on the security of the Ethereum protocol. Given Arbitrum’s EVM compatibility, vulnerabilities in Ethereum could potentially impact Arbitrum as well. Conducting a comprehensive security audit contest at this time is critical due to the recent major hard forks that have introduced significant changes to Ethereum.

A key component of this Attackathon is the development of educational materials that cater to all levels of security knowledge. This educational program will feature live technical walkthroughs and detailed documentation developed by the Ethereum Foundation, client teams, Solidity developers, and Immunefi, covering a broad scope that includes client, specification, and solidity compiler bugs. By educating security researchers, the Attackathon will cultivate a community of researchers capable of identifying and mitigating vulnerabilities across the Ethereum and Arbitrum ecosystems. This increased awareness and participation in Ethereum’s security ultimately benefits the Arbitrum community by ensuring the continued reliability and safety of the underlying blockchain infrastructure.

Rationale

The Attackathon aligns with the Arbitrum community’s mission to promote a secure and scalable Ethereum ecosystem. By investing in this initiative, Arbitrum will help Ethereum’s security, which directly impacts Arbitrum’s scalability and user trust. Moreover, the educational component of the Attackathon will benefit Arbitrum by upskilling security researchers, providing them with the knowledge and tools needed to conduct thorough audits and improve security across the network.

Additionally, Arbitrum can benefit from the collaborative efforts of the Ethereum Foundation and Immunefi, positioning itself as a proactive leader in the Ethereum community. Participation in the Attackathon provides Arbitrum with the opportunity to engage with top security researchers and improve its security posture. As a sponsor, Arbitrum will gain visibility and credibility among developers and users, further solidifying its reputation as a secure and forward-thinking.

Key Terms

- Attackathon

: A comprehensive and time boxed security audit event involving education, active vulnerability hunting, and result evaluation phases.

- Immunefi

: A leading bug bounty platform specializing in blockchain and smart contract security.

- Hard Fork

: Significant upgrades or changes to the protocol that may introduce new code and, potentially, new vulnerabilities.

- Solidity Compiler

: The tool used to compile Ethereum smart contracts written in Solidity into bytecode, which is executed on the Ethereum Virtual Machine.

Specifications

Platforms and Technologies:

- Ethereum Protocol

: The primary focus of the security audit, with an emphasis on identifying vulnerabilities in core protocol code, client software, and the Solidity compiler.

- ImmuneFi

: The platform hosting the Attackathon, responsible for managing submissions, triaging bug reports, and distributing rewards.

- Ethereum Foundation

: Providing funding and oversight for the Attackathon, including contributions to the reward pool and logistical support.

Design Decisions:

- Scope

: The contest will have a broad scope including specification bugs, client bugs, deposit contract bugs and Solidity compiler vulnerabilities.

- Inclusion of the Solidity Compiler

: By including the Solidity compiler in the scope, the Attackathon directly addresses potential vulnerabilities in the primary programming language for Ethereum smart contracts, which is crucial for both Ethereum and Arbitrum.

Related Work

:

- Ethereum Bug Bounty Program

: The permanent bug bounty program has been effective but lacks visibility. The Attackathon aims to increase participation and awareness through a focused, large-scale event.

Steps to Implement

The primary role of the Arbitrum DAO in this initiative is to provide funding support for the Attackathon. By contributing to the reward pool, Arbitrum will ensure that the event attracts top-tier security researchers and maximizes its impact on the security of the Ethereum protocol. Additionally, the Arbitrum community can assist in promoting the Attackathon to raise awareness and encourage participation.

Estimated Timeline

- July 8-11

: EthCC program announcement

- Aug 19th

: Detailed program announcement and education kickoff

- September 2nd

: Attackathon hunting begins

- October 27th

: Attackathon concludes, and results compilation begins

- October 28th

: Review period begins

- Early January

: Results announced

Overall Cost

The Arbitrum DAO has two options for sponsoring the Attackathon:

Unicorn Partners (+75 ETH Commitment)

(limited to two sponsors)

- 1x Unique NFT with leaderboard rank
- Participation in Attackathon Kick-off Twitter Space as a partner speaker
- Leaderboard Placement on Sponsor page
- Top-tier logo placement on Sponsor and Program Landing Page
- Top-tier logo placement on the Program Education page and program report
- Call out in Press Releases and EF and Immunefi Program Announcement Blogs
- Digital Logo Placement in the results announcement at Devcon or a dedicated virtual event
- An Arbitrum Boost (Audit Contest) on Immunefi with up to a \$100K rewards pool at 100% Immunefi Discount within 180 days of the conclusion of the Ethereum program
- 1x Dedicated Twitter post announcing sponsorship from Immunefi Twitter handle

Panda Partners (+30 ETH Commitment)

- 1x Unique NFT with leaderboard rank
- Leaderboard listing on the sponsor landing page
- Mid-roll logo placement on Sponsor and Program Landing Page
- An Arbitrum Boost (Audit Contest) on Immunefi with up to a \$100K rewards pool at 100% Immunefi Discount within 180 days of the conclusion of the Ethereum program
- 1x Dedicated Twitter post announcing sponsorship from Immunefi Twitter handle

By supporting the Attackathon, Arbitrum can leverage the findings to ensure its network remains robust against vulnerabilities. This initiative not only enhances security but also demonstrates Arbitrum's commitment to the ecosystem.