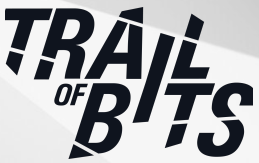

Offchain Labs SetCoreGovernorQuorumAction

Security Assessment (Summary Report)

June 16, 2025

Prepared for:
Harry Kalodner, Steven Goldfeder, and Ed Felten
Offchain Labs

Prepared by: **Jaime Iglesias, Simone Monica, and Nicolas Donboly**

Table of Contents

Project Summary

Contact Information

The following project manager was associated with this project:

Mary O'Brien, Project Manager
mary.obrien@trailofbits.com

The following engineering director was associated with this project:

Benjamin Samuels, Engineering Director, Blockchain
benjamin.samuels@trailofbits.com

The following consultants were associated with this project:

Jaime Iglesias, Consultant
jaime.iglesias@trailofbits.com

Simone Monica, Consultant
simone.monica@trailofbits.com

Nicolas Donboly, Consultant
nicolas.donboly@trailofbits.com

Project Timeline

The significant events and milestones of the project are listed below.

Date	Event
June 9, 2025	Pre-project kickoff call
June 9, 2025	Delivery of report draft
June 16, 2025	Delivery of final summary report

Project Targets

The engagement involved reviewing and testing the following target.

ArbitrumFoundation

Repository	https://github.com/ArbitrumFoundation/governance
Version	d2163adcb6b5415d76bc4d09ec21791749b00c8e 4bf1db4702469d3cd17dcefaf0ffbaa92f880763
Type	Solidity
Platform	Arbitrum

Executive Summary

Engagement Overview

Offchain Labs engaged Trail of Bits to review the security of the `SetCoreGovernorQuorumAction` and `SetConstitutionHashAction` governance proposals, specifically PR #341 and PR #346, respectively.

A team of three consultants conducted the review from June 9 to June 10, 2025, for a total of six engineer-days of effort. With full access to source code and documentation, we performed a manual review of PR #341 and PR #346.

Observations and Impact

PR #341 introduces a new governance action contract (`SetCoreGovernorQuorumAction`) that implements a proposal to reduce the Arbitrum DAO's voting quorum threshold from 5% to 4.5% of all votable tokens. This reduction aims to make governance more accessible and to prevent proposal failures due to insufficient participation, though it also reduces the economic cost of potential governance attacks. This change is motivated by challenges in reaching quorum for important governance decisions due to low voter participation. The contract, deployed at address `0xd5FDDac0BC78C5D7fD1FC0F66B05d697029D9946`, will be executed through Arbitrum's standard governance process.

PR #346 introduces an action contract that changes the on-chain DAO constitution hash to reflect the new quorum parameter.

The review focused on ensuring that the governance proposal follows Arbitrum governance's invariants, that the governance action contract follows Arbitrum's standards and guidelines, and that the action implements the intended behavior. We carefully reviewed the payload generation and the specific actions encoded in the calldata. Finally, we reviewed PR #346.

The review did not reveal any security-relevant issues with the changes made in PR #341 or PR #346.

Recommendations

We recommend implementing the recommendation provided in the Code Quality Findings appendix.

A. Code Quality Findings

The following finding is not associated with any specific vulnerabilities. However, fixing it will enhance code readability and may prevent the introduction of vulnerabilities in the future.

- According to the "Governance Action Contract Standards and Guidelines," the `perform` function should verify that the current quorum numerator is as expected (500) before calling `coreGov.relay` to update it. It must also ensure that the update has been applied correctly (450) after the call to `relay`; if not, the function should revert. We recommend adding at least an after check in the `perform` function of the `SetCoreGovernorQuorumAction` contract.

About Trail of Bits

Founded in 2012 and headquartered in New York, Trail of Bits provides technical security assessment and advisory services to some of the world's most targeted organizations. We combine high-end security research with a real-world attacker mentality to reduce risk and fortify code. With 100+ employees around the globe, we've helped secure critical software elements that support billions of end users, including Kubernetes and the Linux kernel.

We maintain an exhaustive list of publications at https://github.com/trailofbits/publications, with links to papers, presentations, public audit reports, and podcast appearances.

In recent years, Trail of Bits consultants have showcased cutting-edge research through presentations at CanSecWest, HCSS, Devcon, Empire Hacking, GrrCon, LangSec, NorthSec, the O'Reilly Security Conference, PyCon, REcon, Security BSides, and SummerCon.

We specialize in software testing and code review assessments, supporting client organizations in the technology, defense, blockchain, and finance industries, as well as government entities. Notable clients include HashiCorp, Google, Microsoft, Western Digital, Uniswap, Solana, Ethereum Foundation, Linux Foundation, and Zoom.

To keep up to date with our latest news and announcements, please follow @trailofbits on X or LinkedIn, and explore our public repositories at https://github.com/trailofbits. To engage us directly, visit our "Contact" page at https://www.trailofbits.com/contact or email us at info@trailofbits.com.

Trail of Bits, Inc.
228 Park Ave S #80688
New York, NY 10003
https://www.trailofbits.com
info@trailofbits.com

Notices and Remarks

Copyright and Distribution

Test Coverage Disclaimer

All activities undertaken by Trail of Bits in association with this project were performed in accordance with a statement of work and agreed upon project plan.

Security assessment projects are time-boxed and often reliant on information that may be provided by a client, its affiliates, or its partners. As a result, the findings documented in this report should not be considered a comprehensive list of security issues, flaws, or defects in the target system or codebase.

Trail of Bits uses automated testing techniques to rapidly test the controls and security properties of software. These techniques augment our manual security review work, but each has its limitations: for example, a tool may not generate a random edge case that violates a property or may not fully complete its analysis during the allotted time. Their use is also limited by the time and resource constraints of a project.