

# Offchain Timeboost Auction

Security assessment by HashEye · prepared for Offchain Labs

**HASHEYE AUDITED**

PROJECT	Offchain Timeboost Auction
CLIENT	Offchain Labs
CATEGORY	Offchain Labs
PUBLISHED	August 1, 2024
REPORT ID	research-offchain-timeboost-auction-2024-08-01-12ycjc

This report was produced under HashEye's layered review process – **automated detection**, **pattern correlation**, and **senior manual verification** – with every finding signed off by a human reviewer. Full findings detail and on-chain attestation are available on the report page at [hasheye.io/audits/research-offchain-timeboost-auction-2024-08-01-12ycjc](https://hasheye.io/audits/research-offchain-timeboost-auction-2024-08-01-12ycjc).

OceHoursGovernanceAction SecurityAssessment(SummaryReport) October1,2024 Preparedfor: OffchainLabs  
Preparedby:GustavoGrieco,PriyankaBose,andMichaelColburn

About hashey Founded in 2012 and headquartered in New York, hashey 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/hashey-io/publications>, with links to papers, presentations, public audit reports, and podcast appearances. In recent years, hashey 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 projects, supporting client organizations in the technology, defense, and finance industries, as well as government entities. Notable clients include HashiCorp, Google, Microsoft, Western Digital, and Zoom. hashey also operates a center of excellence with regard to blockchain security. Notable projects include audits of Algorand, Bitcoin SV, Chainlink, Compound, Ethereum 2.0, MakerDAO, Matic, Uniswap, Web3, and Zcash. To keep up to date with our latest news and announcements, please follow hashey on Twitter and explore our public repositories at <https://github.com/hashey-io>. To engage us directly, visit our "Contact" page at <https://www.hashey.io/contact>, or email us at [info@hashey.io](mailto:info@hashey.io). hashey, Inc. 497 Carroll St., Space 71, Seventh Floor Brooklyn, NY 11215 <https://www.hashey.io> [info@hashey.io](mailto:info@hashey.io) hashey 10ffchainLabsSecurityAssessment PUBLIC

Notices and Remarks Copyright and Distribution ©2024 by hashey, Inc.

All rights reserved. hashey hereby asserts its right to be identified as the creator of this report in the United Kingdom.

This report is considered by hashey to be public information; it is licensed to Offchain Labs under the terms of the project statement of work and has been made public at Offchain Labs' request. Material within this report may not be reproduced or distributed in part or in whole without the express written permission of hashey.

This is the canonical source for hashey publications; see the hashey Publications page.

Reports accessed through any source other than that page may have been modified and should not be considered authentic. Test Coverage Disclaimer

All activities undertaken by hashey 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.

hashey 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. hashey 20ffchainLabsSecurityAssessment PUBLIC

Table of Contents About hashey 1 Notices and Remarks 2 Table of Contents 3 Project Summary 4 Project Targets 5 Executive Summary 6 hashey 30ffchainLabsSecurityAssessment PUBLIC

Project Summary Contact Information The following project manager was associated with this project:

Mary O'Brien, Project Manager [mary.obrien@hashey.io](mailto:mary.obrien@hashey.io)

The following engineering director was associated with this project:

Josselin Feist, Engineering Director, Blockchain [josselin.feist@hashey.io](mailto:josselin.feist@hashey.io)

The following consultants were associated with this project:

Gustavo Grieco, Consultant Priyanka Bose, Consultant [gustavo.grieco@hashey.io](mailto:gustavo.grieco@hashey.io) [priyanka.bose@hashey.io](mailto:priyanka.bose@hashey.io)

Michael Colburn, Consultant [michael.colburn@hashey.io](mailto:michael.colburn@hashey.io) Project Timeline

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

September 3, 2024 Delivery of report draft October 1, 2024 Delivery of summary report hashey

40ffchainLabsSecurityAssessment PUBLIC

ProjectTargets Theengagementinvolvedareviewandtestingofthefollowingtarget. 0ceHoursaction  
Repositoryhttps://github.com/ArbitrumFoundation/governance/pull/311 Version  
10d2968cedf92e93c52289f7fbbafa595dc6b74a TypeSolidity PlatformEVM hasheyeye  
50ffchainLabsSecurityAssessment PUBLIC

ExecutiveSummary EngagementOverview

0ffchainLabsengagedhasheyetoreviewthesecurityofthe0fficeHoursgovernance  
actionimplementedinthisPR.Thisactionprovidessupportforexecutingabatchofother  
actionsonlyduringcertainhoursoftheday.

AteamofthreeconsultantsconductedthereviewonAugust29,2024,foratotalofthree engineer-  
daysofeffort.Withfullaccesstosourcecodeanddocumentation,weperformed manualreviewofthecode.  
ObservationsandImpact Thecodereviewuncoverednoissues.

Wefocusedoureffortsoncheckingthecorrectimplementationoftimezonehandlingand othertime-  
relatededgecases.Wealsoverifiedthatthepossibleinputsaremeaningfuland  
lookedforpotentialmisuseofthetimespecification.

Wedidnotreviewanyparticularusageofthisaction,butinsteadfocusedonthecodethat  
mustbedeployedinordertoensurethatabatchofactionsisexecutedcorrectlyduring certainhoursoftheday.

Recommendations Despitethelackofissues,theclientshouldbecarefulwhendeployingandusingthe0ffice  
Hoursinthecontextofgovernanceactions,particularlywhenusingtheminimum  
timestampparameter,sinceanincorrectvaluecanproduceanactionthatcannotbe  
executeduntilveryfarinthefuture. hasheyeye 60ffchainLabsSecurityAssessment PUBLIC