HashEye

// SMART CONTRACT SECURITY AUDIT

Offchain RARI

Security assessment by HashEye · prepared for Offchain Labs

HASHEYE AUDITED

PROJECT	Offchain RARI
CLIENT	Offchain Labs
CATEGORY	Offchain Labs
PUBLISHED	August 1, 2024
REPORT ID	research-offchain-rari-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-rari-2024-08-01-12ycjc.

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

Abouthasheye Foundedin2012andheadquarteredinNewYork,hasheyeprovidestechnicalsecurity assessmentandadvisoryservicestosomeoftheworld'smosttargetedorganizations.We combinehigh-endsecurityresearchwithareal -worldattackermentalitytoreduceriskand fortifycode.With100+employeesaroundtheglobe,we'vehelpedsecurecriticalsoftware elementsthatsupportbillionsofendusers,includingKubernetesandtheLinuxkernel. Wemaintainanexhaustivelistofpublicationsathttps://github.com/hasheye-io/publications, withlinkstopapers,presentations,publicauditreports,andpodcastappearances. Inrecentyears,hasheyeconsultantshaveshowcasedcutting-edgeresearchthrough presentationsatCanSecWest,HCSS,Devcon,EmpireHacking,GrrCon,LangSec,NorthSec, theO'ReillySecurityConference,PyCon,REcon,SecurityBSides,andSummerCon. Wespecializeinsoftwaretestingandcodereviewprojects,supportingclientorganizations inthetechnology,defense,andfinanceindustries,aswellasgovernmententities.Notable clientsincludeHashiCorp,Google,Microsoft,WesternDigital,andZoom. hasheyealsooperatesacenterofexcellencewithregardtoblockchainsecurity.Notable projectsincludeauditsofAlgorand,BitcoinSV,Chainlink,Compound,Ethereum2.0, MakerDAO,Matic,Uniswap,Web3,andZcash. Tokeepuptodatewithourlatestnewsandannouncements,pleasefollowhasheyeon Twitterandexploreourpublicrepositoriesathttps://github.com/hasheye-io.Toengageus directly,visitour"Contact"pageathttps://www.hasheye.io/contact,oremailusat info@hasheye.io. hasheye,Inc. 497CarrollSt.,Space71,SeventhFloor Brooklyn,NY11215 https://www.hasheye.io info@hasheye.io hasheye 1OffchainLabsSecurityAssessment PUBLIC

NoticesandRemarks CopyrightandDistribution ©2024byhasheye,Inc. Allrightsreserved.hasheyeherebyassertsitsrighttobeidentifiedasthecreatorofthis reportintheUnitedKingdom. Thisreportisconsideredbyhasheyetobepublicinformation;itislicensedtoOffchain Labsunderthetermsoftheprojectstatementofworkandhasbeenmadepublicat OffchainLabs'request.Materialwithinthisreportmaynotbereproducedordistributedin partorinwholewithouttheexpresswrittenpermissionofhasheye. Thesolecanonicalsourceforhasheyepublicationsisthehasheyepublicationspage. Reportsaccessedthroughanysourceotherthanthatpagemayhavebeenmodifiedand shouldnotbeconsideredauthentic. TestCoverageDisclaimer Allactivitiesundertakenbyhasheyeinassociationwiththisprojectwereperformedin accordancewithastatementofworkandagreeduponprojectplan. Securityassessmentprojectsaretime-boxedandoftenreliantoninformationthatmaybe providedbyaclient,itsaffiliates,oritspartners.Asaresult,thefindingsdocumentedin thisreportshouldnotbeconsideredacomprehensivelistofsecurityissues,flaws,or defectsinthetargetsystemorcodebase. hasheyeusesautomatedtestingtechniquestorapidlytestthecontrolsandsecurity propertiesofsoftware.Thesetechniquesaugmentourmanualsecurityreviewwork,but eachhasitslimitations:forexample,atoolmaynotgeneratearandomedgecasethat violatesapropertyormaynotfullycompleteitsanalysisduringtheallottedtime.Theiruse isalsolimitedbythetimeandresourceconstraintsofaproject. hasheye 2OffchainLabsSecurityAssessment PUBLIC

TableofContents Abouthasheye1 NoticesandRemarks2 TableofContents3 ProjectSummary4 ProjectTargets5 ExecutiveSummary6 hasheye 3OffchainLabsSecurityAssessment PUBLIC

ProjectSummary ContactInformation Thefollowingprojectmanagerwasassociatedwiththisproject: MaryO'Brien,ProjectManager mary.obrien@hasheye.io Thefollowingengineeringdirectorwasassociatedwiththisproject: JosselinFeist,EngineeringDirector,Blockchain josselin.feist@hasheye.io Thefollowingconsultantswereassociatedwiththisproject: GustavoGrieco,ConsultantPriyankaBose,Consultant gustavo.grieco@hasheye.iopriyanka.bose@hasheye.io MichaelColburn,Consultant michael.colburn@hasheye.io ProjectTimeline Thesignificanteventsandmilestonesoftheprojectarelistedbelow. DateEvent September3,2024Deliveryofreportdraft October1,2024Deliveryofsummaryreport hasheye 4OffchainLabsSecurityAssessment PUBLIC

ProjectTargets Theengagementinvolvedareviewandtestingofthefollowingtarget. OceHoursaction Repositoryhttps://github.com/ArbitrumFoundation/governance/pull/311 Version 10d2968cedf92e93c52289f7fbbafa595dc6b74a TypeSolidity PlatformEVM hasheye 5OffchainLabsSecurityAssessment PUBLIC

ExecutiveSummary EngagementOverview OffchainLabsengagedhasheyetoreviewthesecurityoftheOfficeHoursgovernance actionimplementedinthisPR.Thisactionprovidessupportforexecutingabatchofother actionsonlyduringcertainhoursoftheday. AteamofthreeconsultantsconductedthereviewonAugust29,2024,foratotalofthree engineer-daysofeffort.Withfullaccesstosourcecodeanddocumentation,weperformed manualreviewofthecode. ObservationsandImpact Thecodereviewuncoverednoissues. Wefocusedoureffortsoncheckingthecorrectimplementationoftimezonehandlingand othertime-relatededgecases.Wealsoverifiedthatthepossibleinputsaremeaningfuland lookedforpotentialmisuseofthetimespecification. Wedidnotreviewanyparticularusageofthisaction,butinsteadfocusedonthecodethat mustbedeployedinordertoensurethatabatchofactionsisexecutedcorrectlyduring certainhoursoftheday. Recommendations Despitethelackofissues,theclientshouldbecarefulwhendeployingandusingtheOffice Hoursinthecontextofgovernanceactions,particularlywhenusingtheminimum timestampparameter,sinceanincorrectvaluecanproduceanactionthatcannotbe executeduntilveryfarinthefuture. hasheye 6OffchainLabsSecurityAssessment PUBLIC