Abstract

TL: DR this proposal funds continuous formal security analysis for Arbitrum ecosystem projects over 12 months, potentially preventing multiple $m in hacks

Dedaub proposes to provide continuous security analysis for all Arbitrum projects (satisfying criteria), including for the Arbitrum DAO and any other smart contracts critical for the secure operation of Arbitrum. This proposal, lasting 12 months, aims to improve the security and reputation of the ecosystem, and detect Critical vulnerabilities and Governance attacks before they are exploited, using a semi-automated approach ("Security Platform") to achieve economies of scale: an automated system liberally flags potential issues and human auditors inspect and validate in depth. Our proposal is inspired by earlier successful deployments for other EVM-based chains.

Motivation

Over the past year, $Bs worth of crypto assets have been lost due to smart contract vulnerabilities. The intricate financial interdependencies within the Arbitrum ecosystem amplify these threats, suggesting a potential domino effect: one major breach could trigger a cascade, jeopardizing the entire ecosystem. Our team at Dedaub has a proven track record of averting such crises. For example, on the Fantom chain, when its Total Value Locked (TVL) surpassed that of Arbitrum's current ecosystem, we identified and helped rectify a critical flaw in a primary bridge originally flagged via Dedaub security analysis platforms, yielding the team a multi-million dollar bounty. Left unchecked, this vulnerability could have resulted in a staggering ~$1.5B loss in a single transaction, and further indirect losses to the broader Web3 community via systemic risks.

The rising frequency and scale of these security breaches underscore the urgent need for robust smart contract security measures applied to the collective protocol ecosystem. Dedaub, with its expertise and experience, is uniquely positioned to bolster the Arbitrum ecosystem's defenses. We are dedicated to fortifying all protocols deployed on Arbitrum, at scale, ensuring that the revolutionary potential of the chain is not undermined by security oversights of important participants in the ecosystem. Our commitment extends beyond mere detection; we actively engage in remediation, safeguarding the ecosystem's assets and reputation, while respecting a decentralized approach.

Rationale

Arbitrum's DAO enjoys significant autonomy and is pivotal in the protocol's coordination, growth, and protection. Reliance on singular entities, whether Offchain Labs or the Arbitrum Foundation, for the running of the ecosystem is undesirable. At the same time, an each-to-their-own approach towards security neither scales nor does it yield good results, especially since many projects fall through the cracks or don't allocate enough resources to security. Indeed, security is lacking on many protocols: most do not have access to high-quality auditing, experienced war-roomers, formal security analysis platforms, nor on-chain monitoring solutions tailored to their protocol. Dedaub can fill the gap and provide ecosystem developers access to all the above, financed via a relatively small fund from the Arbitrum DAO. The advantage of this approach is that it achieves a much higher economy of scale and yields excellent security that complements each project's own initiatives.

The goals of this proposal may appear to be very challenging; however, our team has already invested heavily in security research that can scale to an entire blockchain ecosystem and has already commercially deployed variations of the services outlined in this proposal for the Ethereum Foundation (security impact studies) and the Fantom Foundation. For instance, throughout the period during which Dedaub's Security Platform has been integrated with Fantom protocols, there have been several vulnerability disclosures and redeployments of vulnerable protocols. Indeed none of the protected protocols were hacked! This high level of security support for multiple protocols by a single organization (Dedaub) is in part enabled by the high degree of automation behind the Dedaub Security Platform. This proposal will, however, aim to advance the state-of-the-art even further.

Finally, Dedaub's role transcends merely security. It aspires to ensure the DAO's smooth operation without interfering in protocol ecosystem operations, reflecting true decentralization in action.

About Dedaub

Dedaub specializes in Smart Contract security, conducting 200+ audits and partnering with blockchain leaders like the Ethereum Foundation, Coinbase, and Chainlink. We set Web3 security standards through our various technological initiatives and are a Founding member of SEAL, assisting protocols with post-hack remediation. We've developed a blockchain code explorer (Contract Library) centered around decompilation and security and a technology-driven continuous auditing & monitoring service, Security Platform (Watchdog), utilizing state-of-the-art static analysis technology. Within the security community, Dedaub tools have become an indispensable resource for reverse-engineering, debugging, and understanding of opaque smart contracts.

The Dedaub Security Platform is a collection of custom vulnerability analyses. The analysis is a combination of ultra-novel techniques - declarative program analysis and bottom-up theorem proving. The Dedaub Security Platform has flagged numerous vulnerabilities in deployed contracts, resulting in several public disclosures and twelve (12) bug bounties (totaling over $3m). The Security Platform offers continuous security monitoring through two main facilities:

- proactive static analysis of deployed code to detect vulnerabilities, which are subsequently inspected and possibly confirmed by a human expert;
- continuous monitoring of transactions via bots specified in WatchdogQL, monitoring transactions in real-time via Dedaub's real-time database of on-chain actions and states.

On the auditing front, none of the protocols we've audited have beenhacked.

The Dedaub team consists of whitehat hackers, static analysis experts, security engineers, cryptographers, and researchers. We have successfully worked with many teams, such as the Ethereum Foundation, Chainlink, Fantom Foundation, Coinbase, Uniswap, Lido, Blur, TrueFi, Base, and others.

Here's a collection of public, unsolicited quotes on our work:

"I've only seen the Dedaub team ship amazing reports, … As an ex-Chainlink engineer myself (ex-DevRel technically), I've witnessed the good this team can do on an audit."

- Patrick Collins, Founder, Cyfrin Audits

"nice job, the tools look really useful!"

- Dr. Christian Reitwiessner, Creator of Solidity

"I'm really pumped up about seeing all the different use cases here… Yannis [from Dedaub] always makes really cool security tools, which I'm excited for."

- Steve Ellis, co-Founder & CTO of Chainlink

"… It is one of the most sophisticated security tools available, finding even the most subtle exploits… Both Neville and Yannis are some of the smartest security professionals in this space…"

- Michael Kong, CEO, Fantom Foundation

"There are tools nowadays like this one [Dedaub Security Platform] which find, in unpublished code, what the vulnerabilities are. Very direct…"

- Matthias Egli, Principal Auditor & Founding Partner at Chainsecurity

"… I always have great discussions with the folks from Dedaub…"

- Josselin Feist, Director of Engineering, Trail of Bits

"Dedaub officially goated security chads, wud endorse"

- Fully Allocated, Olympus DAO

"This is how it should be! You are doing Gods work! Keep watching and protecting us sers!"

- fable.eth

Specifications

As background, Dedaub Security Platform brings together four major elements for smart contract security:

- Automated, deep static analysis of contract code. Our team has published numerous research papers in static analysis techniques over the course of more than 15 years, with significant applications in smart contracts.
- Dynamic monitoring of protocols. Monitoring covers all interacting/newly deployed contracts, current on-chain state, past and current transactions. This component admits significant customization: we offer a language for writing monitoring bots based on the needs and API of a protocol, in just a few lines, using our fast indexed schema of transactions and holdings.
- Statistical learning over code patterns. The Security Platform learns from all contracts ever deployed in EVM networks. Some of its most important warning types come from observing that the way of using a third-party service differs from past patterns.
- Human inspection of warnings raised. The automated analyses of the Security Platform are tuned (at the default level of confidence) to flag suspicious computation and interaction, to focus the effort of human inspectors. Human auditors are responsible for analyzing the code in depth and escalating issue reports.

We propose the following services:

1. Develop & deploy a security-focused blockchain explorer for Arbitrum chains, as well as an accessible database of smart contract code, simplifying the job of whitehat hackers, and developers to dive deep into potential security issues.
2. Develop and deploy Dedaub the Security Platform on Arbitrum chains, and integrate with all protocols at least $5m TVL, prioritizing strategically important projects. This allows security researchers to formally analyze these projects.
3. Allocate Dedaub auditor time to support the deployed protocols on Arbitrum, i.e., inspect flagged vulnerabilities and assist projects with developing their own monitoring bots for suspicious transactions using Dedaub tools.
4. Create competitive auditing contests with the help of our partners that introduce a novel, but more effective way of leveraging multiple security inspectors. These will be incentivized to inspect security vulnerabilities flagged via the Security Platform and create monitoring bots in WatchdogQL.
5. Education - develop and make available educational content for using the formal analysis toolchains, monitoring, and also on how to interpret the security issues of DAO proposals.
6. Check DAO proposals - each DAO proposal will be immediately screened for security vulnerabilities the moment it is queued. In addition, a team of auditors from Dedaub will collectively spend 10 auditing weeks scrutinizing these for vulnerabilities, and deviations from the spec. The security issues will be communicated both to the proposer and the public.

A high level of security support for multiple protocols by a single organization (Dedaub) is in part enabled by the high degree of automation behind the Security Platform. For instance, all contracts that are part of each protocol get grouped automatically (under human supervision). Subsequently, the Security Platform can analyze the contracts and display warnings of vulnerabilities (or proto-vulnerabilities, i.e., components that when put together can make a service vulnerable). The static warnings are then combined with queries on environmental conditions (e.g., approvals and balances in past transactions, state of initialization of a contract, storage contents) to produce reports that can point to security issues.

The Security Platform maintains a contact database for each protocol. If a vulnerability is detected in a live system, we will automatically notify the appropriate project team. Furthermore, since many protocols deployed on Arbitrum are forks of existing (battle-tested) protocols, they are an excellent fit for Dedaub's dynamic monitoring solution, which, when configured by one of our experienced auditors in conjunction with the protocol team can ascertain that the protocol operating on Arbitrum is properly configured and not malfunctioning. Finally, special emphasis can be given to protocols that are strategically important for the security of Arbitrum, such as bridges (including related contracts on Ethereum), fraud proof contracts, or sequencers.

Costs

The proposed price for the project over one year would be:

Integration & Tooling, including licensing, development & hosting: $200k per quarter.

Auditor Support: $299k per quarter, comprised of:

(i) 50 weeks of Dedaub expert auditor/analysis developers' time (at our standard rate of $17.5k / week)

(ii) one audit competitions with a minimum of 20 participants (including Dedaub's time spent triaging issues) at $150k

(iii) 4 weeks of Dedaub quantitative analyst's time to check DAO proposals economic considerations (at our standard rate of $17.5k / week)

Dedaub proposes to allocate approximately 15% of the auditor time to review governance proposals, on a best-effort basis. However, the DAO will be given a quarterly option to remove the costs associated with this ($30k / quarter), or allocate this time to ecosystem projects instead.

Limitations: only protocols matching TVL and other criteria will have access to auditing support, however all known protocols will have access to the tooling (in the case of the Security Platform, with access credentials—valid for a year—provided to protocol maintainers) but will be fully responsible for inspecting warnings and setting up security monitoring. Security credentials will be verified on-chain.

The stream of funds will remain in DAO control and can be cut off at any time through an onchain DAO proposal. As of the ARB price on November 4th, this proposal is estimated to cost the DAO approximately 1.88M ARB over the year.

Timeline

The project can start 1 month following the successful execution of the Snapshot vote.

Transparency & Success Measures

Dedaub, through the technology behind the Security Platform, has been able to disclose what was most likelythe largest vulnerability in Web3. In addition, none of the protocols safeguarded by Dedaub, either through the Security Platform, or formally audited, have been hacked. Despite this success, the techniques, tools and effort proposed does not guarantee that hacks will be preempted in the future. In general, there is no silver bullet in smart contract security, and any technique including manual auditing, formal verification and program analysis has its blind spots. Moreover, success is also predicated by transparency to be tenable to the Arbitrum DAO.

The rest of this proposal contemplates measures to ensure the success and transparency of the project. We've preemptively identified 3 main items here: (i) ensuring transparency to the DAO and wider community, (ii) establishing a fair process to allow ecosystem protocols to avail of the security support, and (iii) ensuring optimal allocation of the limited number of professional service days that this proposal is seeking.

Ensuring transparency to the DAO.

Each month, a designated member of the Dedaub team will post updates about projects onboarded and actively being analyzed on the forum, and other activities performed. This update will have a section containing KPIs, which include:

1. the number of smart contracts & projects monitored
2. the number of Arbitrum transactions monitored
3. the number of escalated warnings and bugs identified by the Security Platform deployment 4) project hacks and bugs missed or not successfully preempted by the project
4. the number of Arbitrum proposals inspected

Dedaub will also consult with the security council, to prioritize activities proposed.

Availability of professional auditing support

will depend on a project's TVL, as calculated by the approach established by DeFi Llama, or funds at risk in the case of other smart contracts. The latter metric will be calculated by Dedaub. These metrics will be published publicly as a dashboard. Protocols with > $5m in TVL for more than a week will automatically be included in the program, and excluded once TVL drops below $2m. All visible protocols will be identified before the project starts. Dedaub will consult with the security council to make adjustments to these criteria.

Dedaub will provide in-app support on the Security Platform, and Discord channels for support.

All protocols will have access to the Security Platform, and anyone to participate in regular "office hours'' with the protocol teams.

Optimal allocation of (scarce) auditing resources.

The allocation of professional resources to vulnerability inspections in the Dedaub Security Platform program will be optimally allocated by considering the following metrics:

- Confidence: The likelihood that a flagged issue is a true positive. This measurement is calculated algorithmically.
- Funds at risk: The absolute amount of funds at risk in a smart contract.
- Recency of smart contract: Older battle-tested smart contracts are likely to be susceptible to hacks.

All of these metrics are easily calculated through the Dedaub Security Platform.