Abstract

Home to some of the best smart contract security researchers in the market and one of the strongest Developer Relations teams in the industry - professionals in Cyfrin come from backgrounds like Chainlink, Compound, Alchemy, Aragon, WorldCoin, Microsoft, Google, and other popular FinTech companies.

Through this proposal, Cyfrin would like to request $2M to improve and foster the security and longevity of the Arbitrum ecosystem.

We will do this through launching the Arbitrum Security Enhancement Fund

dedicated to sponsoring audits for Arbitrum projects.

Motivation

Blockchains solve global issues no other technology today has been able to solve: verifiable accountability, unbiased data exchange, trust without intermediaries, online ownership, permissionless transactions, global identities, to name a few…

Yet, until Web3 is safe, it is not scalable.

In July, total losses in the DeFi sector breached $77B according to a report fromCryptoSlate. In 2022 alone, DeFi experienced hacks resulting in losses of over $3.1B. In 2023, a staggering $2.3B has already been stolen, indicating a trajectory higher than the previous year.

This is a security problem, a best practices problem, and a branding problem - rightfully keeping away institutions and users from a world-changing technology. Not solving this makes any effort of making web3 mainstream, vain.

[

1600×1138 136 KB

](https://global.discourse-cdn.com/standard17/uploads/arbitrum1/original/2X/7/7dbb9b4b71e82d06bc9ed50d172fbd4f740875d5.png)

Every time there is a hack on an Arbitrum project, both the Arbitrum ecosystem and the entire industry, suffer.

Getting this right increases adoption at scale. Value exchange technologies without developers capable of using them appropriately have a hard time succeeding. Value exchange technologies with developers and protocols lacking security best practices create an unsafe environment for everyone participating.

– The future of crypto hinders on projects prioritizing smart contract security.

Cyfrin commits to leveraging our team of industry experts to strengthen, support, and secure Arbitrum's ecosystem and its developers.

Rationale

Leveraging our auditing, engineering, and educational skill sets, the Cyfrin team will keep projects built on Arbitrum and its users safe. Through this proposal, Cyfrin aims to contribute to the long-term success of the Arbitrum ecosystem through attracting incoming TVL for the Arbitrum ecosystem, gain user trust, and show traction to potential future investors.

Laser-focused on Web3 security, Cyfrin is a market leader in smart contract audits. Cyfrin offers everything from private audits to competitive public and private audits, as well as a multi-phase auditing approach we've designed to ensure stronger security guarantees.

[

image

1272×438 18.9 KB

](https://global.discourse-cdn.com/standard17/uploads/arbitrum1/original/2X/e/eef6f8ad9af263c4f7d23396654d6993e05d7dcd.png)

Additionally, you may find case studies for Oku Trade and SudoSwap to learn more about how Cyfrin works.

Some testimonials from clients:

- "It was a pleasure to work with the Cyfrin team. Their approach to security and meticulous testing is exceptionally thorough. Additionally, their intimate knowledge of the Chainlink protocol made them particularly useful for our audit." -

Getty Hill, Oku Trade Founder

- “Working with Cyfrin feels like a true partnership — they are just plain good at what they do and above all are as motivated as anyone to move our industry’s security practices forward” - Beanstalk
- “Working with Cyfrin was a good experience, they kept in touch throughout the entire audit, and also followed up post-launch. Competitive with the best of the firms." - 0xmons from Sudorandom Labs

Through this proposal, we’re asking Arbitrum to fund a Security Enhancement Fund to audit projects built on its infrastructure.

The fund will allocate funds to private, competitive, or multi-phase audits for projects built on Arbitrum.

Cyfrin will power the long-term success of Arbitrum protocols, so protocols feel safer going to market and users more comfortable interacting with the Arbitrum chain.

Key Terms

- Audit:

An audit is a service where a security researcher reviews a codebase in depth with the intent of finding potential vectors for exploitation. Once completed, a report is presented to the protocol to fix any potential vulnerabilities found.

- Private audit

: A team, consisting of usually 2-3 security researchers, spends weeks looking at a protocol’s codebase with the aim of finding the most critical exploit vectors in a codebase, as well as perform architecture analysis, fuzz testing, improvement pull reviews, etc.

- Public Competitive Audit

: An audit where hundreds, if not thousands, of security researchers review a codebase and compete for funds in a set reward pool based on the complexity of vulnerabilities found, its impact, and its uniqueness.

- Private Competitive Audit:

An invite-only audit where a protocol invites top-performing auditors to review their code and compete in community driven audit competition.

- Multi-Phase Audit:

a new, innovative model known as the Diverge-Converge Multi-Phase Model. Crafted to maximize the quality of audits, a critical aspect in the Web3 space, by strategically incentivizing auditors and ensuring that the protocol codebase goes through at least three comprehensive auditing phases, enhancing the protocol’s ultimate security.

Specifications

The entirety of the funds will be allocated towards funding security reviews for protocols, including the costs to run the audits, hire auditors, promote contests, bring judges, do customer support, and competition moderation.

The Fund will match up to 60% for the audit requested. The remaining amount will have to be paid by the project itself requesting for funding. This is mostly to weed out projects just looking for a free audit, ensuring we’re truly enabling long-lasting impact for the ecosystem.

The one exception to this rule is projects who are already deployed on Arbitrum and who can prove a high number of active users, total value locked, or who provide user retention and stickiness across the Arbitrum ecosystem as a whole. Establishing the details of what “high” means in this case will be a task of the Allocation Committee once formed.

These audits may come in the form of competitive audits, through our CodeHawks platform, private audits through our security research team, or through our multi-phased approach combining the above.

Audit Types

Competitive Audits

CodeHawks, one of the leading competitive auditing platforms in the market and home to some of the top security experts in the industry, enhances the security of protocols through community-driven smart contract security reviews.

On CodeHawks, hundreds of auditors study, test, stress, and review the same protocol’s codebase for a defined amount of time - finding bugs and potential exploit vectors. Auditors then submit the findings to the platform for judge review and

monetizing based on the vulnerabilities uncovered.

Private Audits

Private audits, an option tailored to yet-to-be deployed, and already-live protocols. A hand-in-hand relationship between protocol's engineering team and our security research squad is formalized to uncover vulnerabilities and support developers with state-of-the-art best practices guidance.

Through constant communication, the protocol's engineering team is able to revise vulnerabilities as soon as they're found - ensuring the team can start working on fixes immediately. Auditors also provide architecture analysis, fuzz testing, improvement pull reviews, specific knowledge like formal verification, code smells, testing feedback, etc.

Multi-phase Audits

Designed for large and more complex protocols, the Multi-Phase audit approach has the stronger security guarantee of them all since it encourages the protocol to go through several audit phases before completing the final report.

To learn more about the Multi-Phase Audits, review here.

[

1600×531 112 KB

](https://global.discourse-cdn.com/standard17/uploads/arbitrum1/original/2X/9/94de3d610083fec1fdc4d0cd35c1720832865f5b.png)

Allocation Committee

The Allocation Committee is the group responsible for determining which projects should receive audit funding. Cyfrin will lead the charge of setting this Committee up within 2 weeks of proposal approval.

The multisig account for the Allocation Committee will contain 5 people (3 from Arbitrum's side, 2 from Cyfrin). Each team (Cyfrin and Arbitrum) will select who from their organizations will represent them in the Allocation Committee within 10 days of proposal approval.

Once composed, the committee will determine any additional eligibility criteria and share them with the community before opening up the application funnel. The application funnel should open within a maximum of one month post proposal approval.

Additionally, the Allocation Committee is responsible for defining the appropriate application process and reviewing applications on a recurrent basis. The process for reviewing these applications, as well as how often the Committee meets will be determined by the members based on the amount of applications received and their complexity.

We saw the community gather together under the STIP proposal and would like the same community participatory process to guide the direction of how the fund allocates the distribution. It's a discovery process that we will run, partnering with Arbitrum to validate findings and iterate repeatedly.

Eligibility criteria for protocols applying to the Security Enhancement Fund

The Security Enhancement Fund aims at improving the security of all projects that have already deployed or will be deploying into the Arbitrum chain.

Any protocol that adds value to the Arbitrum ecosystem across DeFi, Gaming, DAOs, or social projects, real world assets tokenization, track and trace solutions, or any other track, bringing a healthy and sustainable contribution to the ecosystem, is welcomed to apply.

Projects should have already deployed to Arbitrum mainnet to apply, although exceptions can be made for:

- Protocols who commit to deploying on Arbitrum within 6 months of the audit - if this is the case, the code being audited must be deployed exclusively on Arbitrum for 6 months before launching elsewhere. The Allocation Committee will determine when taking such a risk is worth the assessment.
- Protocols who already have deployed and gained traction on other chains, looking to deploy to Arbitrum as well - if this is the case, information regarding the protocol's TVL, active user base, and Arbitrum strategy should be shared in the application for review by the Allocation Committee.

Ineligible Projects

In an effort to keep the Arbitrum ecosystem secure and sustainable, we comply and leverage Arbitrum's guidelines to determine which projects are ineligible to apply for the Security Enhancement Fund.

Additionally, the Allocation Committee may establish additional guidelines for ineligible projects.

Security Enhancement Fund Distribution

The 100% of the funds from the Security Enhancement Fund will be used to audit Arbitrum projects.

The fund allocation per project will cover 60% of the protocol audit, expecting the protocol to cover the rest. The reasoning behind this is to ensure only protocols serious about their long-term growth get audited. However, an exception of sponsoring 80% of the audit could be made for unique situations as established by the Allocation Committee, like for a protocol amounting for large ecosystem growth or a large protocol deploying to Arbitrum.

This makes it extremely convenient for protocols built on Arbitrum to enhance the security of their codebase and protect users' assets.

Audit prices are aligned with industry standards and calculated based on the complexity of the codebase under review.

- For competitive audits

, the prize pool is calculated as approximately $30 multiplied by the number of lines of code in the code base.

- For private audits

, the cost is calculated as $60,000 multiplied by the number of weeks required by the auditors to read, understand, and review the code base in scope. The time required for each audit is evaluated before the security review by the lead auditor assigned to the project and will be made publicly available to the community.

Protocols are permitted to undergo one or multiple smart contract security reviews per protocol update. The number of reviews is determined based on the codebase size, as indicated below:

- For codebases or protocol updates with less than 5000 nSloc, security reviews will be limited to 1 per type.
- For codebases or protocol updates with more than 5000 nSloc, security reviews will be limited to 2 per type.

nSloc is an objective measure and industry that stands for Normalized Source Code. Calculated reducing all multiline functions declarations to a single line, removing all comments and empty lines and counting the remaining number of lines of code.

Whatever allocation we don't spend, at the end of the year we will return to the DAO for further use.

Steps to implement

Within the next year, the Cyfrin team commits to:

1. Technical implementation of creating the Allocation Committee's multisig and define its members
2. Allocation Committee details eligibility requirements and allocation criteria
3. Define and implement process for protocols to apply for audits alongside the Allocation Committee
4. Review applications and start distributing funds strategically for protocols who meet the criteria
5. Pair auditors with protocols
6. Kick-off auditing process
7. Amplify the Security Enhancement Fund as a great reason for projects to choose Arbitrum as their L2 of choice, as well as promotion of the protocols Cyfrin audits
8. Final report to protocols

– Keep in mind, this process may vary depending on whether the protocol is undergoing a private, competitive or multi-phase audit.

Team

- Patrick Collins

: Cyfrin's CEO and former Lead of Chainlink DevRel, Patrick revolutionized the industry onboarding hundreds of thousands of developers into web3 with its courses and speeches, with more than 3 million views on his courses and ~160.000 subscribers across platforms.

- Alex Roan:

Cyfrin's CTO, Alex is a veteran Web3 developer who has contributed to core DeFi infrastructure such as Chainlink and Compound - securing billions of dollars in value.

- Hans Friese

: Cyfrin Lead Auditor and Co-founder, Hans is one of the world's top auditors,consistently ranking at the top within competitive auditor leaderboards. He is also the founder and Lead Engineer ofSolodit, the most used vulnerability aggregator tool for auditors.

- Don Dodge

: tech veteran with a past in Google, Microsoft, Groove, Napster, AltaVista, and more. Startup investor, advisor, and board member.

- Mark Scrine

: previously the Strategic Lead for Proof of Reserve at Chainlink Labs and led a number of their biggest integrations. These included protocols such as TUSD, Matrix Port, Avalanche Bridge, BackedFi, and Swell Network.

- Developer Relations & Marketing

: Our industry leading DevRel team will work together with the Arbitrum's community to promote, educate, and onboard auditors into the Cyfrin ecosystem, advocating for audit quality for protocols. Additionally, through Cyfrin's Education platform, our DevRel team is brewing the next generation of software engineers into the space with Arbitrum as their L2 of choice. Composed of 6 people total, here's an example of some of the leaders in our team: * Vitto Rivabella

, formerly leading Developers Experience at Alchemy, the popular Web3 infrastructure provider, and Alchemy University, educating tens of thousands of Web3 developers. Web3 educator, investor, developer, public speaker and a former VFX supervisor.

- Juliette Chevalier

, former Lead of Developer Relations at Aragon and Co-founder of Surge Women, an organization bridging the educational gap between women and crypto products. She is also a key contributor to various DAOs, angel investor, software engineer, and public speaker.

- Vitto Rivabella

, formerly leading Developers Experience at Alchemy, the popular Web3 infrastructure provider, and Alchemy University, educating tens of thousands of Web3 developers. Web3 educator, investor, developer, public speaker and a former VFX supervisor.

- Juliette Chevalier

, former Lead of Developer Relations at Aragon and Co-founder of Surge Women, an organization bridging the educational gap between women and crypto products. She is also a key contributor to various DAOs, angel investor, software engineer, and public speaker.

- Community Manager

: Our Community Manager will foster peer-to-peer relationships and manage technical support for the students going through the Arbitrum courses - a vital resource for community members seeking assistance and supporting CodeHawks auditors to do their best work.

- Design

: Our design team will create visually engaging and user-friendly materials, enhancing the overall learning experience for the Abitrum developer community and CodeHawks auditors.

- CodeHawks Team

: The CodeHawks team together with Cyfrin will run, promote, judge, support and moderate the competitions and the community, onboarding and assisting the protocols looking to onboard on Arbitrum. Once the team has made sure the protocol respects the eligibility criteria, they will manage the entire cycle from start to finish. This includes sales (answering to active inbounds, and protocols suggested by the community), contest details, marketing, judging, and final report submission.

- Audit Team

: Our team of security researchers are experts across a variety of fields like DeFi, oracles, Web3 social, and more. They

come from the industry’s top auditor leaderboard and are dedicated entirely to the private audits.

Cost

The budget for this proposition totals $2 million.

The entirety of the funds is dedicated towards the sponsoring of audits for protocols deployed or deploying on Arbitrum.

The entirety of the funds will be expected upon proposal approval to maintain a rapid response to audit requests and safeguard protocol integrity.

Upon the onchain approval of the proposal, these funds will be transferred to the Allocation Committee’s multi-sig, as set up by Cyfrin containing the 2 Cyfrin Committee representatives. The multi-sig’s first transaction will then add the 3 Arbitrum representatives before transferring any funds to protocols.

Additionally, Cyfrin suggests the Allocation Committee reimburses the DAO quarterly in the event that the minimum expected capital for that quarter ($500,000) isn’t spent within that time period. This will also enable a tangible oversight mechanism for the DAO to ensure Cyfrin is doing the expected work.

Why $2M?

At an average cost of $60,000, sponsored at 60%, $2M would cover anywhere from 20-25 audits in the span of a year.

Although the cost of an audit varies widely based on codebase size, complexity, and audit type, audit prices typically range between $30,000-$100,000, with an average audit being ~$60,000.

Assuming the Fund covers 60% of the audit, $2M are estimated to cover anywhere from 20-25 audits within the span of a year. Additionally, 70% of the fund will be used to cover existing protocols on Abitrum, with the remaining 30% used to cover new protocols launching on the chain.

– Important to note that in order to have the best possible security for a protocol, projects often go through 2 or more audits - including private and competitive audits. Particularly for complex projects already holding a high TVL, a multi-phase audit is highly advised to decrease the chances of an exploit to an absolute minimum.

Considering Arbitrum is believed to have 1.2M total commits and over 1,100 Arbitrum repositories, with over 450 active developers, this fund would cover ~10% of Arbitrum’s development.

[

](https://www.developerreport.com/ecosystems/arbitrum)

Framework on payments, reporting, and oversight

Cyfrin pledges to publish financial reports to the DAO to uphold transparency and accountability every quarter, outlining expenditure details, audits funded, decisions made, and progress updates. These reports will be posted in the Arbitrum DAO’s forum for the DAO to periodically review.

Risks and Mitigation

- CodeHawks auditing effectiveness

: The effectiveness of the CodeHawks auditing program in enhancing security for Arbitrum projects may not be guaranteed, as it is dependent upon auditors joining the auditing contests.

— Mitigation

: Cyfrin will focus our efforts in ensuring CodeHawks has a strong track record of successful audits and large enough reward pools that attract the best auditors in the market. Additionally, the Cyfrin team will thoroughly assess projects receiving grants to ensure quality is high.

- Quality of private audits

: There’s always a risk that vulnerabilities are missed during a private audit which may lead to exploits.

— Mitigation

: Cyfrin strictly vets its security researchers and recruits the best from the market. However, when vulnerabilities occur, our auditing team is always on-call to support the project on an emergency basis. Additionally, we also offer the multi-phase audit approach, enabling projects with high TVL and active users to go through an even more in-depth review process as reviewed above.

- Missing funds

: Considering how complex and large some of Arbitrum's codebases already are, we may see a scenario where a few protocols take up the whole dedicated quarterly amount or where more funds are needed than what the quarterly payment can afford.

– Mitigation

: Receiving lots of applications and interest from Arbitrum protocols is generally seen as a positive signal towards increasing ecosystem security. If we encounter such a case, the Allocation Committee may request an earlier dispatch of funds to the DAO in order to serve that specific protocol or wait until the following quarter payment if the audit time is not critical for the project.

- Growth decreases quality

: In the case where the amount of audits requested exceeds the amount of auditors Cyfrin has, there's a risk we decrease quality of audits for quantity.

– Mitigation

: Where Cyfrin cannot do private audits, we will do competitive audits instead – relying on our community of auditors worldwide to support in the security review. We will not hire new auditors just for the sake of hiring, but rather focus always on the best in the industry for long-term recruitment and rely on our additional offering in the case where we don't have bandwidth for more private audits.

- Budget management

: The proposed budget of $2 million is substantial, and there's a risk of misallocation or overspending.

— Mitigation

: The Allocation Committee will be in charge of establishing clear guidelines for budget allocation, with quarterly payments allowing for adjustments based on performance. Periodic financial reports should be provided to the DAO to maintain transparency and accountability. Additionally, if no funds are being spent on a quarter, these funds will be returned to the DAO to further use.

- Lack of applications

: There is a scenario where this Fund doesn't get enough projects applying for funding and audits are not being granted.

– Mitigation

: The sole focus of our Sales team will be dedicated to getting quality Arbitrum projects to apply for audits, as well as the marketing efforts of our industry-leading DevRel team. This means reaching out to existing protocols individually, as well as unleashing the full force of our marketing efforts among Arbitrum circles to ensure the existence of this

Conclusion

More than a blockchain security research firm, Cyfrin is a web3 security powerhouse solving crypto's most fundamental issues: security, education, and developer experience.

Leveraging our joint expertises, the Cyfrin team is beyond excited to partner with Arbitrum and provide our security services to make the Arbitrum ecosystem the go-to choice for engineers and businesses building in Web3.

– For reference, this proposal was made in consultation with Krysztof Urbański (L2Beat), Disruption Joe (Plurality Labs), CLG, Seb (Gains Network), Zer8 PRM, Matt (StableLab), Onkar, Sinkas, Limes.eth, and Frisson. It has gone through several rounds of feedback, ensuring we're building alongside the Arbitrum ecosystem for the longer term.

UPDATE: Upon conversations with the L2Beat delegate, Cyfrin adds the additional details to the proposal:

- L2Beat has suggested the Allocation Committee to be formed by 2 Cyfrin members, 2 Arbitrum DAO members, and 1 member from the Arbitrum Foundation. We find this to be a reasonable composition and would recommend the DAO and the Foundation select their own members to be represented since they know their members best and will have the most context on who's best for the role.

- Additionally, since we understand this can be a complex decision, we're open to extending the timeframe on this selection process to 1 month after proposal approval. Defining the members within the Allocation Committee is a key requirement before any funds are allocated towards audits.

- Additionally, as an additional reporting mechanism, we commit to, at least one member of the Allocation Committee, attending Arbitrum DAO's monthly call to update on the Fund's allocations.

- Aside from what's established in the proposal, the report will also include the amount of protocols which have applied for audits, the number of protocols that have undergone a security audit through the Fund, the total funds distributed within the quarter and how many funds remain for the rest of the year, the qualitative feedback from both private and competitive audits from the protocols who go through this service. Every report from an audit funded via this Fund will also be made publicly available for the DAO to review.

- In terms of payments for the Allocation Committee members, we suggest spending a total of the Fund's 75,000 USD on salaries for the Allocation Committee members within the span of a year. Cyfrin representatives will not receive additional funding, so the 75,000 USD will be divided across the 3 Arbitrum representatives. This translates to 25,000 USD a year for each Arbitrum representative. This means that the Fund's total assets to allocate would instead be 1,925,000 USD.

- We'd also like to add that Allocation Committee members commit to not accepting bribes from protocols in exchange for their vote.

- Another suggestion we received was to set a cap amount of audit funds per quarter. We have defined that as 481,250 USD per quarter - so 25% of the Fund each quarter.

As defined above, all yet-to-launch protocols who receive an audit should commit to deploying on Arbitrum within 8 months of their audit. If they do not accomplish this, there is reasonable expectation that they should refund the money to the DAO.

- The Cyfrin team will lead co-marketing efforts with all the protocols audited, as well as with the Arbitrum DAO to further amplify our brands. This co-marketing will be done through our industry-leading DevRel team including, but not limited to, Patrick Collins.

- While reviewing financial numbers above, we understand the value of these amounts will be in ARB. The conversion rate is determined at the moment when the proposal gets published for onchain vote. Meaning, when 100 USD are mentioned, these should be read as the value of 100 USD in ARB, at the value of ARB at the moment when the proposal is published for the onchain vote.

- This proposal ultimately wishes to provide a signal to the wider Web3 ecosystem that Arbitrum cares deeply about protocols already on Arbitrum or looking to launch on Arbitrum. Getting this approved builds a safer ecosystem longer-term for everyone.