

Abstract

When Arbitrum protocols look for audits, they look to [Sherlock](#).

In the past year, Sherlock has conducted 47 audits for protocol teams that have either deployed on Arbitrum or publicly plan to deploy on Arbitrum including GMX, KyberSwap, and Lyra. Sherlock has prevented 183 Critical severity vulnerabilities from reaching Arbitrum mainnet across protocols representing \$470M of Arbitrum's TVL.

[

Stats

1920x717 123 KB

](https://global.discourse-cdn.com/standard17/uploads/arbitrum1/original/2X/f/ffefd15a35136b8558e79a44eba2999c923f7732.jpeg)

Sherlock is requesting \$4M — not for Sherlock — but for Arbitrum protocols, so they can access reduced-cost audits from Sherlock through the Ecosystem Security Fund. This initiative will enhance the security of the Arbitrum ecosystem for the long term as well as entice up-and-coming protocol teams to build on Arbitrum.

Motivation

Arbitrum has one of the most vibrant developer communities and dedicated user bases in the entire Web3 space. The recent STIP is proof that the Arbitrum Foundation always takes the long-term well-being of their projects into account. However, there is one aspect that can pose a great threat to any ecosystem and requires constant vigilance: security.

Arbitrum projects' success depends on their commitment to security. Exploits can tarnish user trust and attract significant negative media coverage. Moreover, due to smart contracts' composability, vulnerabilities can spread easily.

As [Pew Research Center](#) highlights, distrust in the security and reliability of Web3 projects is a major barrier to crypto adoption.

Without adequate security, scaling and long-lasting adoption is not possible.

Sherlock's primary mission since Day 1 has been protecting end-users, who usually are the most affected by hacks and exploits. Sherlock aims to fortify the broader crypto industry, where Arbitrum plays a significant role.

The Ecosystem Security Fund proposal will enhance the security of the Arbitrum ecosystem, one project at a time.

Rationale

The Ecosystem Security Fund as well as Sherlock's own values directly align with the Arbitrum Community Values described in [Section 6](#) of the Arbitrum DAO Constitution.

- Ethereum-aligned:

The most innovative projects with the highest usage and TVL have tended to be on Ethereum-based chains, so that's where Sherlock has focused 100% of its time so far and honed its skills.

- Sustainable:

Sherlock will leverage its extensive experience securing Arbitrum projects alongside a great community of security experts to ensure the long-term success of the Arbitrum ecosystem as a whole.

- Secure and user-focused:

Sherlock makes every decision through the lens of "What maximizes security for users?" which is why Sherlock prides itself on being the "final exam" before mainnet due to the proven effectiveness of Sherlock audits.

- Socially inclusive:

Just as anyone can build on Arbitrum, anyone in the world is welcome to participate in both public audit contests and judging on Sherlock.

- Technically inclusive:

Sherlock pioneered decentralized judging which is widely known as one of the best ways to learn auditing and has made Sherlock a valuable platform for beginners and experts alike.

- Neutral and open:

Sherlock attempts to be maximally inclusive when it comes to which protocols can receive audits on the platform.

Encouraging and subsidizing audits would not only attract far more protocols to Arbitrum (audits are expensive), but it would also be a very commendable move by the Arbitrum DAO which will enhance the security of crypto as a whole, no matter which chains a protocol ends up on.

From Sherlock's perspective, Arbitrum has become a very popular chain for builders. Sherlock is very grateful to have been able to help many protocols that have either deployed on Arbitrum or declared to Sherlock's auditors that they plan to do so in the future. Here's a list of Arbitrum-aligned projects that Sherlock has audited in the past year:

[

Companies 26

1920×1080 103 KB

](https://global.discourse-cdn.com/standard17/uploads/arbitrum1/original/2X/4/4e42d084bbda653371a0f1bfaece003253268c80.jpeg)

References

A high percentage of these protocols have come back for multiple audits from Sherlock. Here are a few things they've said about Sherlock:

Notional

[\(V3 is committed to Arbitrum\)](#): "Notional has gotten 14 audits from 6 different firms, and ever since we first used Sherlock in October of 2022 they have been, and will continue to be for the foreseeable future, our exclusive audit provider. Sherlock is the best audit experience we've ever had, hands down."

Perennial

[\(live on Arbitrum and the next version is in a Sherlock audit\)](#): "Perennial has done multiple audits with Sherlock and has been continually impressed with the process, from scheduling to onboarding to operation the Sherlock team makes it extremely easy to get audits done. Having used both audit firms and other contest audit platforms, we have found the auditors in Sherlock's contests to be exceptional - finding numerous complex and subtle bugs that had otherwise gone unnoticed. We are excited to continue to use Sherlock for future protocol upgrades."

Index Coop

[\(latest version is planned for Arbitrum\)](#): "Index Coop has had many audits performed by top-tier firms and independent security researchers, but none of them compare to Sherlock in terms of coverage, comprehension, and collaboration. The contest model paired with a dedicated security researcher has led to the highest impact outcomes for our protocol and we consistently recommend Sherlock to other protocols regardless of what stage they are in."

See [here](#) for a supplementary list of Arbitrum-aligned teams that have spoken about Sherlock.

Key Terms

- Audit:

A detailed analysis of a smart contract's code to identify existing and potential vulnerabilities, specifically those causing a loss of funds or comprised functionality.

- Audit Contest:

A competition where any number of security experts (usually ~300) compete to find the most severe vulnerabilities in a codebase and earn money based on their findings.

- Fix Review:

Sherlock includes a half-day fix review which ensures that patches made after a Sherlock audit resolve the initial problem and don't introduce new vulnerabilities.

- nSLOC:

Number of source lines of code. Sherlock uses the nSLOC of a smart contract in combination with qualitative analysis from Sherlock's scoping team to price audits.

- Critical Vulnerability:

A bug in smart contract code that can cause a significantly degraded experience for users (loss of funds, etc.) and is easily exploited. Sherlock refers to “High” severity vulnerabilities and “Critical” severity vulnerabilities synonymously.

- Lead Senior Watson (LSW):

A dedicated and battle-hardened security expert who is part of an elite group at the very top of [Sherlock's leaderboard](#). Each Sherlock audit reserves at least one top Senior Watson to lead the audit before the audit can take place. The Lead Senior Watson also explains vulnerabilities, suggests fixes, and reviews changes made after the audit.

Specifications

Sherlock's “best of both worlds” approach

One of the main reasons why so many Arbitrum-aligned projects elect to trust Sherlock with their codebase security is Sherlock's “best of both worlds” approach. The section below will focus on briefly exploring why it's a superior model, supported by raw data.

Currently, there are 2 main approaches to audits: Traditional and Contest.

Traditional:

2-4 security experts pore over the codebase for a few weeks and flag any vulnerabilities they see.

[

Traditional Audit

1956×662 179 KB

](<https://global.discourse-cdn.com/standard17/uploads/arbitrum1/original/2X/8/80bbc729dbcd4a02781b8233058f72285759e852.jpeg>)

Contest:

A protocol team creates a prize pool (\$30k-\$200k usually), and anyone in the world can submit vulnerabilities. The higher the severity, the more of the prize pool the security expert is awarded.

[

Contest Audit

1956×662 214 KB

](<https://global.discourse-cdn.com/standard17/uploads/arbitrum1/original/2X/0/03278d0641811537700de4e5905acf14874b4c5e.jpeg>)

Sherlock:

Sherlock's approach provides a protocol with the focus, collaboration, and assurance of a traditional audit, alongside the breadth of security expert participation from an audit contest.

Benefits of Sherlock's approach:

- Each contest has an assigned Lead Senior Watson who is heavily incentivized (through fixed pay and an [ELO-style ranking system](#)) to find as many bugs as possible over the entire length of the audit.
- A significant contest prize pool attracts anywhere from 200-400 independent auditors who get paid based on the severity of their findings. Sherlock specifically rewards only High and Medium severity threats.
- The Lead Senior Watson comes back to help the protocol team with fixes (provides a half-day complimentary fix review).
- Sherlock's decentralized judging process takes hundreds of raw, duplicate issues and turns them into a digestible report, saving the protocol team days of work and reducing the possibility of overlooked vulnerabilities.
- Sherlock charges the lowest fees in the industry. 80% of what you pay to Sherlock goes directly to security experts.
- Sherlock is the only auditor to offer exploit and/or bug bounty coverage after the audit is conducted (once the fix review is finished), ensuring that Sherlock's incentives are aligned in shipping the most secure protocol possible.

How does Sherlock know the model is effective?

Sherlock's claims are supported by [data

](<https://docs.google.com/spreadsheets/d/1OwWgBwU3jYoyT8EAbt43Kqg8VCh-3tqg0Z9f6gWujeo/edit?usp=sharing>) gathered from 94 contests, where over 1000 vulnerabilities were found. The image below showcases how many bugs are missed if an audit is done without a reserved auditor (such as a Senior Watson) or without a community contest.

Can you afford to NOT include both?

[

Approach

1947×662 166 KB

](<https://global.discourse-cdn.com/standard17/uploads/arbitrum1/original/2X/5/5461bab04c2f984b0ae62959a3544130f6906625.jpeg>)

Sherlock appoints a lead auditor from a roster of elite senior security experts, known as Senior Watsons who are identified by a [pink crown

](<https://audits.sherlock.xyz/leaderboard>). Notable experts on this list among many others include [Xiaoming90](#), [hyh](#), [WatchPug](#), and [0x52](#). They earn attractive fixed pay for leading the contest along with the ability to compete for the entire prize pool.

The Lead Senior Watson's fixed role ensures that each contest will have at least one expert auditor thoroughly reviewing the codebase, consulting the protocol team, and conducting a complimentary half-day fix review to ensure any fixes have been implemented securely.

The talents of this one individual will be enhanced by competing against an unlimited number of independent security experts / teams striving to win a greater portion of the prize pool. The Senior Watson only keeps their "senior" status as long as they outperform the other auditors in the field, pushing them to give maximum effort.

At the core of this model is Sherlock's continuous commitment to incentive alignment.

Audit Council

As advised by the delegates that Sherlock worked with to craft this proposal, Sherlock will create an Audit Council. The role of the Audit Council is to be the final gatekeeper/decision-maker to determine which projects building on Arbitrum (or planning to build on Arbitrum) are eligible to get discounted audits as part of the program. Sherlock will form this council and the associated on-chain Gnosis multisig within 1 week of the proposal passing to allow projects to take advantage of the program as soon as possible.

5 people will be elected to the multisig (3 representatives from Arbitrum, and 2 representatives from Sherlock). The Arbitrum members will be 2 representatives from the Arbitrum DAO and 1 member of the Arbitrum Security Council. Both Sherlock and Arbitrum will finalize their list of members for the Gnosis multisig within 7 days of proposal approval.

The council will have the ability to add/remove any extra eligibility criteria as deemed appropriate to make this initiative as successful as possible for Arbitrum and protocol teams before the requests from protocol teams start coming in.

The main responsibilities of this council will be:

1. Adding/removing any extra eligibility criteria for protocol requests as deemed appropriate
2. Defining the appropriate request criteria and process so that protocol teams can begin requesting audits
3. Reviewing requests by protocol teams and deciding if each team is eligible to be a part of the program or not

Protocol team requests will begin evaluation within two weeks of this proposal's approval. The council will conduct continuous reviews for audit requests, prioritizing rapid access to quality audits. Sherlock pledges to provide a quote within 72 hours of receiving the relevant codebase, considering its size and complexity. Further procedures for request management will be determined by council consensus.

Additionally, Sherlock commits to community involvement in refining this partnership. Gaining consensus from protocols on Arbitrum is essential to ensure the council's procedures are effective.

Sherlock will consistently seek feedback from Arbitrum's protocol teams to confirm the request process is manageable and that the provided timelines and results meet protocol teams' needs, aiming to make Arbitrum an attractive platform for developers.

Protocol Eligibility Criteria

The Ecosystem Security Fund aims to provide premium security audits for protocols on Arbitrum with substantial TVL/users, or those planning to join that are expected to attract substantial TVL/users. The Audit Council will require data on TVL, user statistics, and deployment strategy to make their assessment.

Prioritization is given to protocols that substantially benefit the Arbitrum ecosystem and there is no favouritism for certain categories (DeFi, Gaming, SocialFi, etc.) over others.

Protocols must meet one of the following criteria for consideration:

1. Has deployed on Arbitrum with significant TVL or user base.
2. Intends to exclusively

launch on Arbitrum within six months of receiving an audit and maintain exclusivity for six months thereafter.

1. Has notoriety on another chain (by TVL or users) and is planning to expand to Arbitrum.

Note:

Compliance with any or all of the 3 criteria does not guarantee acceptance into the Ecosystem Security Fund.

Protocols with characteristics disallowed by the Arbitrum Foundation, detailed in the [Ineligible Application section](#) of their Submission Guidelines, are ineligible for inclusion. The Audit Council reserves the right to modify eligibility criteria for protocol requests as necessary.

Ecosystem Security Fund Distribution

100% of funds dedicated to this program will be used to audit Arbitrum projects.

Here's the expected breakdown for purchasing an audit through the program:

- 60% of the audit cost for an audit is paid for by the Ecosystem Security Fund
- 40% of the audit cost is paid for by the protocol team

Note:

For protocols that have (or are expected to have) an outsized impact on the Arbitrum ecosystem, the Audit Council will have the ability to increase the % of the audit paid by the Ecosystem Security Fund up to a maximum of 80%.

Requiring the protocol to pay for up to 40% of the audit costs ensures that audits are 2.5x more affordable for eligible protocol teams while still making sure that there is enough cost ("skin in the game") associated with every audit so that protocol teams don't abuse the program.

Sherlock's "final exam" audit approach is best suited to the Ecosystem Security Fund because it offers the greatest capital efficiency while minimizing the possibility of Critical severity vulnerabilities.

Sherlock's audit pricing is substantively based on nSLOC. But Sherlock also has an in-house scoping team that has the authority to add a qualitative aspect to pricing to take into account extra complexity (assembly code, etc.).

Sherlock's pricing is based on years of experience attracting top talent to audits and 80% of the cost of each audit goes directly to security experts (the highest ratio in the audit industry). Sherlock has engineered its pricing to attract a top-ranked Senior Watson to lead each audit. For example, Sherlock has experimented with weekly fixed pay for Senior Watsons from \$7.5k to \$22.5k and has landed on [the current schema](#) as being optimal. Sherlock also ensures the audit will attract hundreds of independent auditors and teams, optimizing for the highest quality audit possible.

The nSLOC (adjusted for qualitative input) drives both the price and length of the audit. Here are some example audit quotes:

- 1,200 nSLOC: \$39,000 (1 week)
- 2,350 nSLOC: \$79,500 (2 weeks)
- 3,450 nSLOC: \$120,500 (3 weeks)
- 4,500 nSLOC: \$160,500 (4 weeks)

Sherlock works closely with top Senior Watsons to ensure the cost and length of each audit are correct. Sherlock's average audit is <2,500 nSLOC and Sherlock finds 13 important issues and 4 Critical severity issues on average for each audit.

A detailed overview of Sherlock's pricing system can be viewed here: [Sherlock Pricing - Google Sheets](#) (use the provided comments to make understanding the table easier)

At the end of every quarter, Sherlock will return any unspent amount (based on a \$1M quarterly allocation) to the Arbitrum DAO.

Steps to Implement

Within three months of proposal acceptance, Sherlock will:

1. Define the members of the Audit Council and create the multi-sig wallet
2. Audit Council details eligibility requirements and allocation criteria
3. Define and implement the process for protocols to create applications for audits which will be reviewed by the Audit Council
4. Review applications and assign percentage allocations (60-80%) to protocols that meet the criteria
5. Quote the dollar cost and length required for each audit
6. Secure at least one highly-ranked Lead Senior Watson for each audit, in consultation with the protocol team
7. Deliver the curated list of vulnerabilities to the protocol team so they can work on the fixes
8. Conduct the fix review to ensure any changes to the smart contracts have the intended effect and do not introduce new vulnerabilities
9. Deliver the audit report to the protocol team, after which they should be ready to deploy to Arbitrum
10. Work with the protocol team throughout the audit process to generate excitement for their launch and extol the benefits of launching on Arbitrum

Timeline

1. Within 1 week of proposal acceptance
2. Members of the 5-person Audit Council are selected
3. Gnosis multi-sig is initialized on-chain with the respective Audit Council members
4. Members of the 5-person Audit Council are selected
5. Gnosis multi-sig is initialized on-chain with the respective Audit Council members
6. Within 2 weeks of proposal acceptance
7. Eligibility requirements and allocation criteria will be finalized by the Audit Council
8. Applications by protocol teams will start getting evaluated by the Audit Council
9. Eligibility requirements and allocation criteria will be finalized by the Audit Council
10. Applications by protocol teams will start getting evaluated by the Audit Council
11. Within 3 months of proposal acceptance
12. The earliest audits from the Ecosystem Security Fund will have progressed through every step and had their audit reports delivered
13. Feedback will be collected from early protocol team participants and the Audit Council will make improvements to the process where possible
14. The quarterly "run-rate" for the fund will be known, and any unused funds (out of the \$1M quarterly allocation) will be returned to the Arbitrum treasury
15. The earliest audits from the Ecosystem Security Fund will have progressed through every step and had their audit reports delivered
16. Feedback will be collected from early protocol team participants and the Audit Council will make improvements to the process where possible
17. The quarterly "run-rate" for the fund will be known, and any unused funds (out of the \$1M quarterly allocation) will be returned to the Arbitrum treasury

18. Within 12 months of proposal acceptance
19. Sherlock will create another AIP which will allow the Arbitrum community to decide if the program should be ended or extended (during this process, other audit firms should be given a chance to submit competing/complementary proposals)
20. Sherlock will create another AIP which will allow the Arbitrum community to decide if the program should be ended or extended (during this process, other audit firms should be given a chance to submit competing/complementary proposals)

Overall Cost

\$4M will be allocated to the Ecosystem Security Fund, but any unused funds will be returned every quarter if \$1M is not spent on audits in that quarter.

These funds will be 100% reserved for Sherlock audits done on qualifying protocols building on Arbitrum or planning to build on Arbitrum.

The Audit Council's multisig will be the steward of the funds. For ease of implementation, the entire \$4M amount can be sent to the Audit Council's multisig on acceptance of this proposal. And the Audit Council will remit any unused portion of \$1M every quarter.

The \$4M should not be sent to the Audit Council multisig until all 5 members of the multisig have been successfully added and have completed a test transaction using the multisig. This is to reduce any chance for error and ensure that Arbitrum's 3 council members have a voting majority with respect to the \$4M at all times.

Impact Estimation

Sherlock completed 47 audits for Arbitrum-aligned protocols in the past year. This can serve as a baseline for audit demand prior to the Ecosystem Security Fund's 60% subsidy. With this incentive, the annual demand for Sherlock audits on Arbitrum protocols is expected to be significantly higher.

How many audits can this initiative fund?

To determine this, audits are categorized into three complexity levels, which primarily influence cost. Below are the criteria for each category with a short description.

[

Audit Types

1947x540 152 KB

](https://global.discourse-cdn.com/standard17/uploads/arbitrum1/original/2X/c/ce9665f5429ace982320710df929f82767345509.jpeg)

Size: Size of the codebase; Cost: Average cost of the audit

Why \$4M for the Ecosystem Security Fund?

In the past 12 months, Sherlock has done 47 audits for Arbitrum-aligned projects, many of whom could fit the eligibility criteria for the Ecosystem Security Fund. According to [historic data](#) Sherlock did 5 High, 15 Medium and 27 Low Complexity audits which amount to:

- High Complexity: 5 audits x Average Cost (\$144,000) = \$720,000
- Medium Complexity: 15 audits x Average Cost (\$48,000) = \$720,000
- Low Complexity: 27 audits x Average Cost (\$23,000) = \$621,000
- Total = \$2,061,000

This \$2M serves as an estimate of the past year's audit demand from eligible projects. Sherlock reached this volume without any significant discounts. A 60% discount could potentially triple the number of interested projects. If audit volume reaches \$6M (a 3x increase) and the fund subsidizes an average of 67% (since some projects can be eligible for an 80% discount) of the audit costs, a \$4M fund would be fully utilized.

The \$4M fund could provide an estimated 141 audits

(47 last year x 3) for approved protocols over the course of a year. Given that last year's 47 audits secured 27 projects (57%), Sherlock projects that 141 audits could secure approximately 80 Arbitrum projects

in total.

What KPIs can be used to determine the Ecosystem Security Fund's success?

Audits Approved

Audits Scheduled

Audits Completed

Protocols Deployed on Arbitrum

On-Chain Exploits

KPI

25 audits approved by the Audit Council

20 audits scheduled with Sherlock

20 audit reports delivered

20 protocols deployed to Arbitrum

0 on-chain exploits for audited protocols

Deadline

3 months after the proposal passes

3 months after the proposal passes

4 months after the proposal passes

4 months after the proposal passes

6 months after the proposal passes

Source of Truth

Quarterly report linking on-chain payments with projects

[Sherlock - Contests](#)

[Sherlock Audit Archives](#)

Arbitrum deployment addresses

TVL drops (on-chain) & media (off-chain)

Financial Reporting

Starting 13 weeks after this proposal is approved, Sherlock will issue quarterly financial reports to the Arbitrum DAO forum. These reports will contain key metrics enabling DAO members to evaluate the program's effectiveness. A sample report with dummy data is available [here](#).

[

Financial Report

1920x751 204 KB

](<https://global.discourse-cdn.com/standard17/uploads/arbitrum1/original/2X/5/5902c116dfa06f4bc24bd24c4f205c7da31107ee.jpeg>)

Operational Updates

For complete transparency, Sherlock has set up a Telegram channel and bot specifically dedicated to the Ecosystem Security Fund. To stay updated, you can [join the channel](#). The bot will disseminate real-time information about protocol teams navigating the audit process.

Click [here](#) for a preview. The table below outlines the types of updates the bot provides. Additionally, Sherlock will accommodate any extra update requests from the Audit Council.

Trigger

Announcement

New Audit Request

{Project Name} Requested an Audit. Link: {Website/Twitter}; Size: {nSLOC}; Cost: {Total Price}

Audit Approved/Rejected

The request made by {Project Name} has been approved/rejected by the Audit Council. Confirmation Link: {ArbiScan Link}

Senior Selected

Sherlock has selected {name} to be the Lead Senior Watson for {Project Name}! Here's more info about their background: {Senior Watson profile link}

Contest Announcement

{Project Name} audit contest has been announced! {link to twitter}

Contest Started

{Project Name} audit contest is officially live!

Contest Finalized

{Project Name} final audit and judging contest rewards for Watsons have been announced!

On-chain Address verification

The Audit Council multisig should ONLY ever send funds to Sherlock's multisig address on Arbitrum and back to the address from the Arbitrum DAO that initially funds it.

Sherlock's multisig address on Arbitrum: 0xBe427a7fA085B22fF4928815DF3c2948509d36D3

Risks and Mitigation

Risk

Mitigation

The Arbitrum DAO faces the potential of investing millions in a product that protocol teams may not desire or deem valuable.

Sherlock is one of the most in-demand auditors in the industry (measured by \$ volume of audits) and among Arbitrum-aligned projects. Sherlock's audits with a Security Fund is a powerful combination, and Sherlock's exceptional BD team will ensure widespread awareness among relevant projects.

Sherlock audits may not be effective enough at preventing vulnerabilities.

To gauge Sherlock's effectiveness in identifying critical vulnerabilities compared to other auditors, consider consulting with protocol teams like Ajna, Index Coop, and Tokemak who have undergone multiple concurrent audits by Sherlock.

The \$4M budget for this proposal may be excessive with limited interest from protocol teams.

If the \$4M budget proves excessive, Sherlock will refund any unutilized funds within the quarter (\$1M allocated per quarter). Further returns of funds may be considered if future quarters indicate a low probability of reaching \$1M.

The \$4M budget may prove insufficient, limiting participation from protocol teams.

In a positive light, this suggests strong builder engagement with the program. Arbitrum DAO can opt to maintain the current budget or increase quarterly allocations after hitting the \$1M cap for two or more quarters.

Sherlock may struggle to uphold top-tier audit quality as demand from protocols increases.

Sherlock boasts a highly scalable audit model, consistently drawing over 300 experts per audit. Nevertheless, Sherlock maintains a designated list of Senior Watsons, and no audits occur without their involvement, which has not occurred thus far despite sustained increased demand.

A potential conflict of interest arises as Sherlock both conducts audits and participates in audit approval decisions through the Audit Council.

The Audit Council will consist of 2 signers from Sherlock and 3 signers selected by Arbitrum. This arrangement ensures Sherlock will never be able to “force” an approval decision with its 2 signers.

Conclusion

In the past year, Sherlock has conducted 47 audits and surfaced 183 Critical severity vulnerabilities for protocols building on Arbitrum, including \$470M of the current TVL on Arbitrum. There is likely no other auditor that Arbitrum protocols trust more than Sherlock.

The advent of the Ecosystem Security Fund signals a step-change commitment to security by Arbitrum, and Sherlock is excited to be at the forefront of such an initiative.