Executive Summary

Aave's success relies partly on its ability to deliver high quality products with a strong security posture. To date, and despite the large TVL potentially attracting a lot of malicious actors, Aave users haven't suffered any losses due to smart contract bugs or vulnerabilities. Lately, it has been increasingly difficult to contract reputable smart contract security auditors, as most of the prominent firms in this space are booked out for months.

The aim of this proposal is to ensure Aave receives high-quality security assessment services to address all upcoming updates to its protocols, including critical upgrades such as the v2 → v3 migration.

Sigma Prime has been providing security assessment services to Aave for the past 2.5 years, reviewing critical components such as Aave v2 and v3, along with various other changes made to the lending platform.

Background

Sigma Prime is an information security consultancy who specialise in Blockchain technology and are mostly based out of Sydney, Australia.

The primary focus of Sigma Prime is to help secure distributed systems through in-depth security assessments of decentralised projects, while concurrently researching and developing core Blockchain infrastructure. Over the past 6 years, we have been working with some of the most prominent organisations in the space: the Ethereum Foundation, Chainlink, SushiSwap, 1inch, the Filecoin Foundation, NEAR, Arbitrum, Lido, Rocket Pool, and plenty of others. Some of the reviews that have been made public and performed recently are featured here.

Sigma Prime is also the founder and maintainer of theLighthouse project, an open-source implementation of the Ethereum Proof-of-Stake Consensus specification, written in Rust. Lighthouse is one of the leading Ethereum consensus client implementations and has a particular focus on performance and security.

Throughout the works performed for Aave, the feedback received from the leadership team has been very positive, as can be seen here. We have gained a high degree of familiarity with the protocol, which we intend to leverage as required for the delivery of this engagement.

Proposal

This section outlines the terms of a master services agreement between Sigma Prime Pty Ltd and Aave for security assessment/consulting services:

- Duration of the Agreement

: 12 months

- Commitment

: 240 person-days + 40 optional person-days

- Start Date

: July 4th, 2022

- Minimum Consultancy Fee

: US$ 1,296,000, to be paid in USDC and/or USDT

- Maximum Consultancy Fee

: US$ 1,512,000, to be paid in USDC and/or USDT

- Payment terms

: * 50% of the Maximum Consultancy Fee at the signing of the MSA

- Remaining Consultancy Fee (either 50% of the Maximum Consultancy Fee, or Minimum Consultancy Fee - 50% of Maximum Consultancy Fee) at the completion of the MSA or at the latest 12 months after the start of this Agreement

- 50% of the Maximum Consultancy Fee at the signing of the MSA

- Remaining Consultancy Fee (either 50% of the Maximum Consultancy Fee, or Minimum Consultancy Fee - 50% of Maximum Consultancy Fee) at the completion of the MSA or at the latest 12 months after the start of this Agreement

- Scope of Services:
- Smart contract security assessments
- Web/API application security assessments
- Mobile application security assessments
- Cloud infrastructure security reviews
- Security awareness trainings
- Social engineering activities
- Security processes and organisation consulting
- Red-teaming exercises
- Smart contract security assessments
- Web/API application security assessments
- Mobile application security assessments
- Cloud infrastructure security reviews
- Security awareness trainings
- Social engineering activities
- Security processes and organisation consulting
- Red-teaming exercises
- Engagement Process:
- For each security assessment, the primary deliverable will be a report-style document listing any vulnerabilities discovered during the security review, along with a test suite, built using Brownie. For security awareness training and security processes and organisation consulting, deliverables will be agreed upon with Aave at the start of the engagement.
- Bored Ghosts Developing (BgD Labs) will facilitate the engagement process by vetting the targets for each testing window, and ensuring that the security assessors have access to the relevant entry criteria (documentation, target commit, etc.)
- Multiple projects can be targeted in a single testing window, if time permits.
- While Sigma Prime expects the vast majority of the allocated effort to be dedicated to smart contract security assessments, other security activities can also be conducted (see Scope of Services).
- For projects requiring a high level of familiarity with the core protocol (e.g. v2 → v3 migration), Sigma Prime will utilise the same resources allocated to Aave on previous engagements.
- As part of this agreement, one testing window will be made “optional”, meaning that if no targets are available, that allocated effort will not be charged to Aave. This provides some degree of flexibility, while guaranteeing availability of security assessors throughout the duration of the agreement.
- For each security assessment, the primary deliverable will be a report-style document listing any vulnerabilities discovered during the security review, along with a test suite, built using Brownie. For security awareness training and security processes and organisation consulting, deliverables will be agreed upon with Aave at the start of the engagement.
- Bored Ghosts Developing (BgD Labs) will facilitate the engagement process by vetting the targets for each testing window, and ensuring that the security assessors have access to the relevant entry criteria (documentation, target commit, etc.)
- Multiple projects can be targeted in a single testing window, if time permits.
- While Sigma Prime expects the vast majority of the allocated effort to be dedicated to smart contract security assessments, other security activities can also be conducted (see Scope of Services).
- For projects requiring a high level of familiarity with the core protocol (e.g. v2 → v3 migration), Sigma Prime will utilise the same resources allocated to Aave on previous engagements.

- As part of this agreement, one testing window will be made “optional”, meaning that if no targets are available, that allocated effort will not be charged to Aave. This provides some degree of flexibility, while guaranteeing availability of security assessors throughout the duration of the agreement.
- Timeline:
- This agreement provisions the following testing windows for Aave:
- Review #1:

40 person-days | July 4th to July 29th (v3 Migration)

- Review #2:

40 person-days | August 8th to September 2nd

- Review #3:

40 person-days | September 19th to October 14th

- Review #4:

40 person-days | November 14th to December 16th

- Review #5:

40 person-days | January 16th to February 10th

- Review #6:

40 person-days | March 13th to April 10th

- Review #7:

40 person-days | May 8th to June 2nd

- Review #1:

40 person-days | July 4th to July 29th (v3 Migration)

- Review #2:

40 person-days | August 8th to September 2nd

- Review #3:

40 person-days | September 19th to October 14th

- Review #4:

40 person-days | November 14th to December 16th

- Review #5:

40 person-days | January 16th to February 10th

- Review #6:

40 person-days | March 13th to April 10th

- Review #7:

40 person-days | May 8th to June 2nd

- If one (or more) of these testing windows is not used by Aave, the Minimum Consultancy Fee will apply. If all testing windows are consumed, the Maximum Consultancy Fee will be charged.
- This agreement provisions the following testing windows for Aave:
- Review #1:

40 person-days | July 4th to July 29th (v3 Migration)

- Review #2:

40 person-days | August 8th to September 2nd

- Review #3:

40 person-days | September 19th to October 14th

- Review #4:

40 person-days | November 14th to December 16th

- Review #5:

40 person-days | January 16th to February 10th

- Review #6:

40 person-days | March 13th to April 10th

- Review #7:

40 person-days | May 8th to June 2nd

- Review #1:

40 person-days | July 4th to July 29th (v3 Migration)

- Review #2:

40 person-days | August 8th to September 2nd

- Review #3:

40 person-days | September 19th to October 14th

- Review #4:

40 person-days | November 14th to December 16th

- Review #5:

40 person-days | January 16th to February 10th

- Review #6:

40 person-days | March 13th to April 10th

- Review #7:

40 person-days | May 8th to June 2nd

- If one (or more) of these testing windows is not used by Aave, the Minimum Consultancy Fee will apply. If all testing windows are consumed, the Maximum Consultancy Fee will be charged.
- Example of targets:
- Aave v2 → v3 migration on Ethereum
- A new version of the AAVE token, mainly reducing code and changing delegation
- A new version of the staticAToken, a wrapper that makes the aToken increasing in value via exchange rate, instead of balance
- A new iteration of the Aave governance, based on storage proof voting on a different chain
- A migration of the AAVE/ETH Balancer pool from Balancer v1 to Balancer v2

- Aave v2 → v3 migration on Ethereum
- A new version of the AAVE token, mainly reducing code and changing delegation
- A new version of the staticAToken, a wrapper that makes the aToken increasing in value via exchange rate, instead of balance
- A new iteration of the Aave governance, based on storage proof voting on a different chain

- A migration of the AAVE/ETH Balancer pool from Balancer v1 to Balancer v2

Next Steps

We’re very excited about this proposal and look forward to hearing from the community! Massive thanks to the BgD team who reached out to us and provided feedback as we crafted this proposal. Here are the following steps we anticipate:

- Step 1:

Governance Forum Discussions (5 days)

- Step 2

: Creation of Snapshot Proposal (6 days)

- Step 3

: Creation of on-chain proposal if outcome of Step 2 is positive

- Step 4

: Project kick off if outcome of Step 3 is positive