Executive Summary

This is a continuation of proposal 6308 to improve the security of smart contracts built on top of Aave using a combination of formal verification and manual code review. In the last six months, Certora has improved the security of the Aave protocol and played a significant role in increasing the security community's involvement in Aave's development. We want to continue to improve Aave's security and enable agile development of new products. This proposal will give a brief overview of Certora and formal verification, outline what we've accomplished in the last six months, and discuss our goals for ensuring Aave's security.

Overview

Certora is a security company focused on delivering tools that enable developers to mathematically prove the correctness of DeFi protocols. In the last six months, Certora worked closely with the Aave community, Aave developers, BGD labs, and external communities, including The Secureum, to guarantee the security of the Aave protocol and enable massive innovation.

We engaged twenty external security researchers who, along with our team of security engineers and researchers, helped Aave safely develop 16 new products and list 12 new tokens. A total of 51 smart contracts were reviewed which contained over 25,000 lines of Solidity code. One critical and two high-severity bugs were prevented using the hundreds of correctness rules written by the community and the Certora team.

As we continue our collaboration, we plan to improve on the current proposal in five significant ways: (1) allocate more resources, (2) improve the Certora Prover, (3) develop new open source technology for automatically checking rules written by the community, (4) drastically improve the collaboration with auditors and the security research community, and (5) develop a monitoring framework for checking the CVL rules before every transaction.

About Certora

Our technical team of over 80 people consists of formal verification experts, compiler experts, static analysis experts, research and development engineers, security engineers, and security researchers. Many have PhDs in their fields, decades of security experience, and a strong history of significantly increasing the security of the most significant protocols in DeFi [Aave, OpenZeppelin, MakerDAO, Euler, Compound, TrueFi].

Project Highlights: March 13, 2022 - September 12, 2022

The Aave protocol is leading DeFi in innovation and security, supported by Certora's technology and the security research community. The Certora team worked closely with BGD labs and the Aave protocol team to ensure code security using funding from the previous continuous verification proposal. We outline the main highlights of Certora's contributions during the six months of the project:

- Certora allocated six R&D personnel and engaged twenty external community security researchers to review protocol contracts, most new to the Aave community. Secureum was very helpful in developing this community.
- 16 new Aave products were developed under our security review, and 12 new tokens were listed, all checked by the Certora Prover for bugs and nonstandard behavior.
- 51 smart contracts were reviewed, totaling 25,000 Solidity lines of checked code (the Certora Prover checks the generated EVM byte code, which is much larger).
- A total of 380 correctness rules were selected out of 600 submitted rules by the Certora team and the Aave community. Unlike traditional security audits, these specifications continue to be useful as protocols continue to evolve.
- Certora provided three workshops to familiarize the community with our tools.
- $283,500 were awarded in grants to the community. $151,000 of these awards came from the grants allocated by Aave in the original proposal; Certora provided the additional $132,500. As of September, twenty security researchers composed over 550 security rules for Aave and won 35 grants.
- One critical, Two high-severity, One medium-severity and Ten low-severity bugs were prevented before the code was deployed.
- No major bugs were identified in manual audits by Chain Security and Sigma Prime after formal verification and in the deployed code.
- A dedicated dashboard for verified smart contracts is maintained here.

- A dedicated dashboard for checked listed tokens is maintained here.
- Three complementary papers are being written by The Secureum, BGD Labs, and Certora which describe the main lessons learned from the three-way collaboration. The first article is titled "Aave-Certora-Secureum: A DeFi Security Collaboration".

The New Proposal: Keeping Aave Agile and Safe

We propose to continue the current engagement. Below are the highlights of what we will accomplish:

- Allocate six R&D personnel to lead the community in specification development for the Aave protocol.
- Write specifications and verify new Aave products and listed tokens.
- Provide free access to our SaaS tooling (Certora Prover) to members of the Aave community.
- Develop and improve our technology to address needs raised by the Aave verification efforts. We will continue to provide new tools to the Aave community as they are developed.
- Develop our education materials and be available to the community to help them learn to use our tools.
- Continue to grow Aave's security community and incentivize the best of this community to engage with Aave more closely. We propose to award several fellowships to the best security researchers to work closely with Aave and Certora. We have identified leading candidates who contributed to this year's program.
- Certora will collaborate with Sigma Prime to help them use the Certora Prover as part of their ongoing security review. We will also collaborate with other third parties such as Secureum, who are working to ensure the security of Aave and building the Aave community. Additionally, Code4rena and Spearbit security researchers are proficient in rule writing. For example, Kurt Barry, who works as an independent security researcher through Spearbit, was able to find a 4 year old bug in the MakeDao tool using the Certora Prover.Therefore, for major code revisions, we will conduct Code4rena competitions for finding bugs and writing correctness rules.

Pricing

The previous proposal cost $1.7M per 6 months. A 20% discount is given for an annual contract ($3.4M), bringing the total to $2,700,000 for a year while maintaining the level of service provided by Certora. In addition, Aave will provide 400,000 USDC for fellowships and community grants. The total cost to AAVE will be $3,100,000.

This community grant will be partially used to support designated fellowships to security engineers who are engaging with the Aave DAO on a part-time basis and potentially long-term collaborations with the DAO. We have identified several candidates who participated in the previous grant program and contributed significant rules throughout the project and expressed interest in participating in the fellowship program.

The price for the project is per annum, and vested linearly over one year. 30-day termination is possible with a vote. $1,890,000 is paid in USDC and $810,000 is paid in Aave tokens. 400,000 USDC are awarded to security researchers from the Aave community for reviewing code and writing security rules, as well as the fellowships. The receivers of the fellowship will be selected by a community with two people from Aave BGD, one person from the Aave team, and two people from Certora. Unutilized grants will be returned to Aave.

UPDATE 30 October 2022:

Following the community's feedback, Certora decided to fund the grant program in the original sum of $400K per year. No fellowships will be awarded as part of the grant.

This reduces the total cost of this proposal to the Aave community to $2.7M.