Summary

A proposal for significantly and continuously improving the security of the Aave platform and the dApps built on top of it, by offering our formal verification and path coverage tooling service to the Aave Platform contributors and the Aave Protocol dApp developers. The initial proposal is for 6 months starting January 2022. A discount price is given for an annual contract.

Background

Aave Security

The Aave Protocol is a fully decentralized system that provides sophisticated tools for accessing liquidity. The protocol's ongoing management is controlled by a governance protocol that allows external contributions and voting by stakeholders. Such a system opens up the possibility of creating powerful new DeFi protocols built on top of it, without giving up on decentralization.

One of the major risks in managing a complex system of smart contracts is that it is harder to ensure that changes introduced via governance are safe, and that they do not break the behavior of the protocol. While those problems are common to every piece of evolving software, decentralization introduces additional risks.

These risks were highlighted by a recent incident in which a bug was introduced in a Compound governance proposal, leading to huge nonrecoverable financial losses. Of course, such bugs are not exclusive to Compound— they have been affecting many DeFi protocols.

Detecting vulnerabilities before they are deployed is difficult because of the lack of good security tools for smart contract development. Smart contract developers often rely on manual auditing to prevent bugs, but audits are difficult to employ in the setting of ongoing, time-controlled governance proposals. Moreover, even the best auditor can miss critical bugs due to the complexity of the code.

About Certora

Our team consists of 31 experts in smart contract security, formal verification methods, and compilation techniques. 9 of our team members have PhD in formal verification. We have built a world-class and unique developer tool that seamlessly integrates into CI/CD, allowing continuous verification of contract correctness.

We enable companies to "move fast and break nothing", taking months off of the time to market, by decreasing code audit time. Our product, the Certora Prover, allows both pre- and post-deployment code verification: it statically analyzes the code before it is deployed but also runs on the EVM bytecode of the deployed contracts. The product verifies code by checking that it obeys high-level semantic rules. For example, a rule could assert that the sum of token balances remains unchanged by all operations that do not mint new tokens. A free demo of the Certora Prover can be found here.

Our product is used by the industry's leading companies (Aave, Balancer, Benqi, Compound, MakerDAO, OpenZeppelin, Sushi and more) and has prevented more than 100 safety-critical bugs, including 20 "solvency" bugs (a bug in which a user can steal money from the contract). Each bug can lead to tens or even hundreds of millions of dollars in losses. The Certora technology has also uncovered critical security bugs in the Solidity compiler itself and in deployed contracts of major DeFi organizations.

Certora and Aave relationship

We have been working with the Aave team since before V2 protocol. We've formally verified the various iterations of the AAVE token, and significant parts of the V2 protocol. We found and prevented 6 high severity issues in V2 before deployment, including a solvency bug. We will soon be working on the next major upgrade to the protocol. Our security rules for Aave are publicly available and serve as a useful tool for contract upgrades and integrations. Protocols that integrate into Aave could use these rules and run their code against them to make sure the integration process is smooth. Making this service more accessible is part of this proposal.

Proposal

We propose two approaches to significantly increase the confidence in the platform itself and in the smart contracts built on top of it.

First, we propose to change the project-based relationship of Aave and Certora, to an ongoing relationship, where we will provide ongoing support and rule-writing for Certora Prover on Aave's code. This service will be provided to all who contribute to Aave's ecosystem: Aave's in-house developers, community contributors and dApp developers. This will ensure that the constantly-evolving code of Aave's platform remains secure, protecting its users' assets.

Second, we will develop a new symbolic execution tool (path coverage) which will significantly increase the coverage of code areas where we look for bugs, complementing the more focused nature of the Certora Prover. This tool's results will be visible to all via a unique dashboard we will build. In addition, it will be open-source, so the community could contribute to its development.

The two approaches are complementary: Our continuous rule-writing for the Certora Prover will mathematically prove that critical code areas are secure, while the symbolic execution tool will be more comprehensive, running 24/7 to continuously increase the coverage for specifications that are too complex to prove using the Certora Prover.

In the following sections, we will specify the deliverables of our proposal.

Continuous High-Level CVL rules specification for the Aave Ecosystem Contributors

We will write high-level correctness rules in English and in CVL, Certora's domain-specific specification language, for DeFi smart contracts built on top of Aave, as well as for the Aave platform itself via its contributors. These rules will be used later for the Certora Prover and the new symbolic execution tool.

In the process of writing the rules, we will perform a code review and identify bugs manually. We will allocate an expert software engineer for the entire period of the contract, dedicated to Aave. Normally, customers wait several months for our services, while here Aave will receive ongoing support. This engineer will update the rules to capture the essential security properties of the Aave Protocol and its derivatives. Also, we will update the rules when bugs are found.

Fitting the DeFi community spirit, we will make the CVL rules open-source, allowing decentralized rule writing and rule auditing. This will allow knowledge-sharing in rule writing between contributors and dApps developers, as different developers could use rules fitting their purposes which were written by others.

Formal Verification of Smart Contracts during CI/CD

The above rules will be used by the Certora Prover, which will be available to all Aave platform developers. Rules can be developed using a new VSCode extension, with tooling to integrate CVL specs to the Solidity code project. The extension will also be able to invoke the Certora Prover, and present an ongoing status of the rules: whether they are proven or violated. When a rule is violated, the extension will return a concrete call-trace showing the input for which the rule is violated, in a view similar to a debugger.

Code Coverage for Smart Contracts

This project is inspired by the Sage Direct Fuzzing Project which prevented million-dollar bugs for Microsoft.

We will develop a new symbolic execution product for increasing code coverage of the Aave smart contracts. For each smart contract, the product will automatically generate inputs, enumerating over time more and more control flow execution paths using SMT solvers, in pre and post-deployment. This complements formal verification when the code is too complex for it or when using it is too labor-intensive.

This is similar to Dynamic Monitoring provided by Forta, however, our tool is different in two aspects: it uses high-level security rules and leverages SMT solvers for triggering rarely executed scenarios. The code developed in this project will be open source to allow contributions from the community. This means that every developer can get access to a security tool for her/his smart contract.

In addition to creating the product, we will create a dashboard that will report the inputs and the paths covered by the different inputs, as well as rule violations that may occur. Also, for each input, we check that every CVL rule holds, which will also be reported.

Measures of Success

Certora Prover takes as input a contract and a specification and formally proves that the contract satisfies the specification in all scenarios. Importantly, the guarantees of Certora Prover are scoped to the provided specification, and any cases not covered by the specification are not currently checked by Certora Prover.

In general, we note that there is no silver bullet in smart contract security and in formal verification specifically. Still, we plan to measure success according to the following KPI: (1) the number of paths covered by the symbolic execution tool, (2) the number of rules formally proved, (3) the number of bugs identified by the Certora Prover before deployment, (4) the number of bugs identified by the path coverage tool, and (5) the number of missed bugs in code analyzed by Certora found by auditors and other means. The numbers will be available on a daily basis.

Certora Services Summary

We offer the following services by the company:

- We will allocate a dedicated expert software engineer for writing rules for the Aave platform contributors and for Aave dApps as needed for the whole period. We will also allocate a full-time security researcher to review all proposed code changes.
- We will offer all Aave platform contributors (registered by Aave) access to the Certora Prover SaaS platform to check new and existing rules, as well as provide support for run analysis and creation of new rules.
- We will develop an open source directed fuzzing engine on top of modernSMT solvers.
- We will create a cloud-based symbolic execution product that will analyze the Aave platform code and the dApps built on top of it in pre and post-deployment.
- We will create a dashboard displaying the results of the symbolic execution product, including rule violations and covered paths, visible to all Aave users. Rule violations will be reported automatically to the Aave security team, but not visible to all users to avoid revealing potential exploits.
- We will create an open-source database of CVL rules and the code they refer to, to decentralize rule writing and promote decentralized contributions to rules.
- We will create a two-week online course on writing rules. The course will be recorded for availability for all developers.
- We will hold 2 weekly support Zoom calls for users of the Certora Prover and the new symbolic execution tool.

Pricing

- The project price is $1,700,000 for 6 months or $3,400,000 for 1 year. For a 6 months period, $1,000,000 is paid in USD and USDC. $700,000 is paid in Aave tokens vested linearly over a year period. A 20% discount is given for an annual contract bringing the total to $2,720,000 for a year.
- An additional sum of $200,000 will be paid to Certora and purposed for paying decentralized community rule writers. This sum will not be used for any other purpose.
- The normal price for our services is $70,000 per week for rule writing subject to availability. We are booked 6 months in advance. The SaaS fees are $2000 per month for each user. Here we allow 52 weeks and an unbounded number of users.