Setting up the Certora Prover

Michael George

Stanford, August 2022

Workshop overview

Today: using the Certora Prover

- Installation
- Basic rules
- Lunch
- Invariants
- Ghosts

Tomorrow: Background and practical use

- How the Prover works
- Introduction to AAVE Governance token
- Lunch
- Systematic specification design
- Work session
- Closing

Logistics

For synchronous watchers (in person / streaming):

- Ask questions! In person or on our Discord in `#stanford-certora-workshop`
- Slides are dense; we'll post on discord
- Follow along; finished examples are in the repository
- We'll do lots of exercises
- Recordings will be available on Certora youtube channel

For asynchronous watchers:

- Ask questions! On the forum: `https://forum.certora.com/`
- Slides and repository are linked in the comments

Installing the Prover and Examples

1. Clone and update the Examples repo
   - `https://github.com/Certora/Examples`
2. Update the submodules
   - `git submodule update --init`
3. Install the Certora Prover

   Option 1: VSCode + Docker

   3.1 Install VSCode

   3.2 Install Docker Desktop

   3.3 Install “Remote - Containers” VSCode extension

   3.4 Open the ERC20Example folder in VSCode

   3.5 View → Command Palette → Reopen In Container

   Option 2: Local install

   3.1 Install Python

   3.2 Install Java JRE

   3.3 Install solc-select

   3.4 `pip install certora-cli`

4. Set your `CERTORAKEY` to the key we sent you
   - in a terminal, run “`export CERTORAKEY=<key we sent you>`”
5. Verify the ERC20 example
   - in a terminal, change to `ERC20Examples` directory
   - `sh certora/scripts/verifyERC20.spec`
   - view the report link that is printed

certora