DAY 1: USING THE CERTORA PROVER

MICHAEL GEORGE
CERTORA

Certora AAVE Training

WELCOME!

CERTORA

Getting started:

- Please clone Tutorials and switch to AAVE branch

```
git clone https://github.com/Certora/Tutorials
cd Tutorials
git checkout AAVE
```

- I want this to be interactive — follow along, play, and ask questions
  - Please jump in with questions on discord or zoom

- If you haven't yet installed certoraRun, you can use the demo for today
  - https://demo.certora.com
  - Click ERC20Basic
  - Delete everything in the spec window
  - This won't work for tomorrow's session, so install certoraRun tonight

THE PLAN

- Today: using the Prover
  - We'll build some ERC20 specs
  - We'll analyze counterexamples
  - I'm planning one or two 10m breaks (with short exercises to ponder)
- Exercise (between sessions)
  - Use specs to find bugs in two ERC20 contracts (bytecode only!)
- Office hours (later today)
  - We're here to help
- Tomorrow: Designing specifications systematically
- Friday: Real-world examples

Demo

RECAP

CERTORA

Basic Prover usage

- require, assert, mathint, env, envfree, method, calldataarg, withrevert, and lastReverted
- navigating the call trace and understanding counterexamples

Unit-test style rules

- e.g. “`transfer` must increase recipient’s balance by amount”

High-level rules (parametric rules)

- e.g. “`allowance(owner,spender)` can only be increased by `owner`”

Invariants

- e.g. “a user’s balance is at most the `totalSupply`”

RECAP

Basic Prover usage

- require, assert, mathint, env, envfree, method, calldataarg, withrevert, and lastReverted
- navigating the call trace and understanding counterexamples

Unit-test style rules

- e.g. “`transfer` must increase recipient’s balance by amount”

High-level rules (parametric rules)

- e.g. “`allowance(owner,spender)` can only be increased by `owner`”

Invariants

- e.g. “a user’s balance is at most the `totalSupply`”

Exercise for tonight:

- Add properties, verify other tokens (scripts/verify*)
- Challenge: use specs to find the bugs in bytecode tokens (bytecode/*)
- Get help in discord, office hours, forum.certora.com, or docs.certora.com
- I’ll push in the specs we developed today