ackee | blockchain security

School of Solana

BONUS LECTURE

Fuzz testing

Adam Hrazdira

ackee | blockchain security

SW Development Status Quo

- Any software needs to be “properly” verified.
  - Unit tests.
  - Integration tests.
  - Tests based on requirements.
  - High test coverage.
  - Manual code reviews.
  - Security audits.
  - ...

The Problem

- Absence of bugs is still not guaranteed!

ackee | blockchain security

What is Fuzz testing?

- A.k.a. fuzzing.
- Automated software testing method.
- Another testing layer increasing robustness of your program.
- Passes malformed, invalid or unexpected inputs to your program.
- Checks for crashes or invariants violations.
- Automatically generates and runs thousands of test cases.

ackee | blockchain security

Benefits

- Most likely finds bugs missed by other tests.
- “Set it and forget it.”
- Increases tests coverage.
- Easy to scale (test on more machines).

Challenges

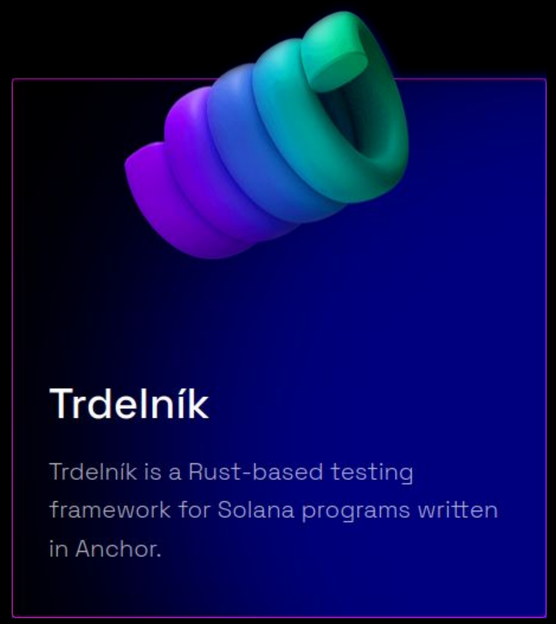
- Complicated environment setup.
- Complex testing harness.
- Data analysis of crashes.

ackee | blockchain security

Trdelnik fuzz testing framework

- Written in Rust.
- Supports Solana Anchor programs.
- Automatically sets up testing environment.
- Generates basic test harness.
- Provides CLI to run and debug fuzz tests.
- Based on Google's Honggfuzz library.

https://github.com/Ackee-Blockchain/trdelnik/



ackee | blockchain security

Fuzzing a Solana (Anchor) program

- Fuzz test can generate “random”:
  - Instruction parameters.
  - Instruction accounts.
  - Instructions invocation order.
  - Combinations of all cases above.

ackee | blockchain security

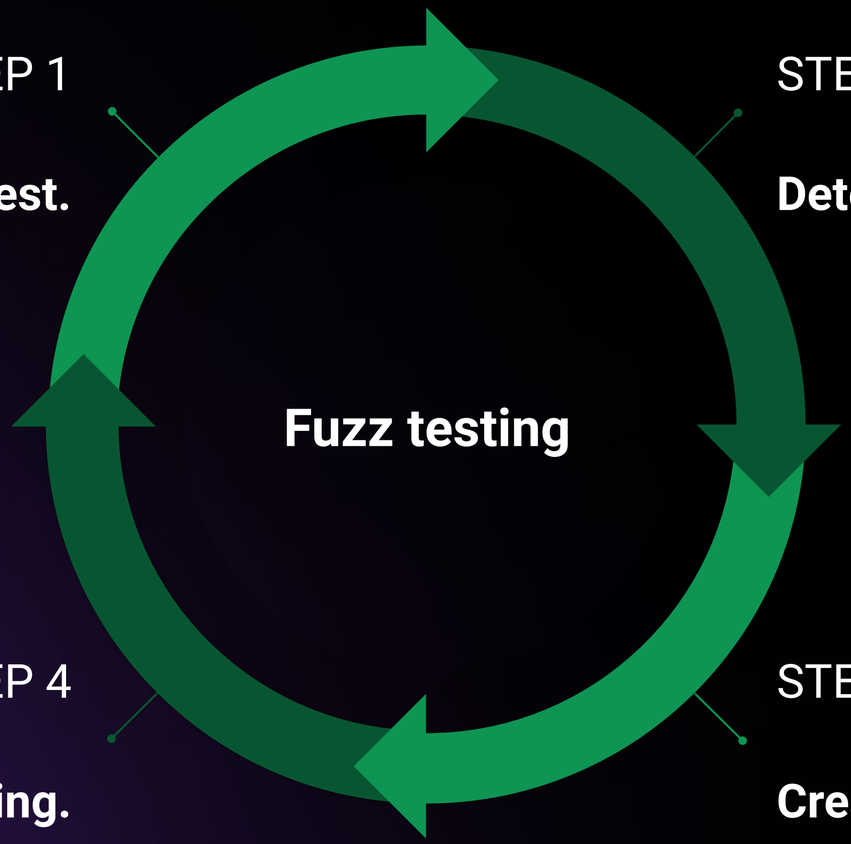
Basic fuzzing workflow

STEP 1

Analysis of the system under test.

STEP 2

Determination of inputs.



STEP 4

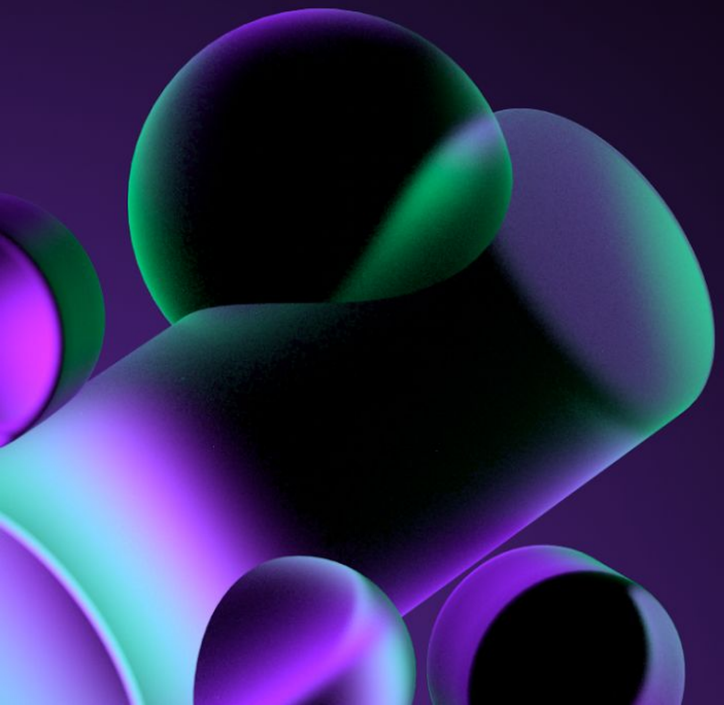
Analysis of crashes and debugging.

STEP 3

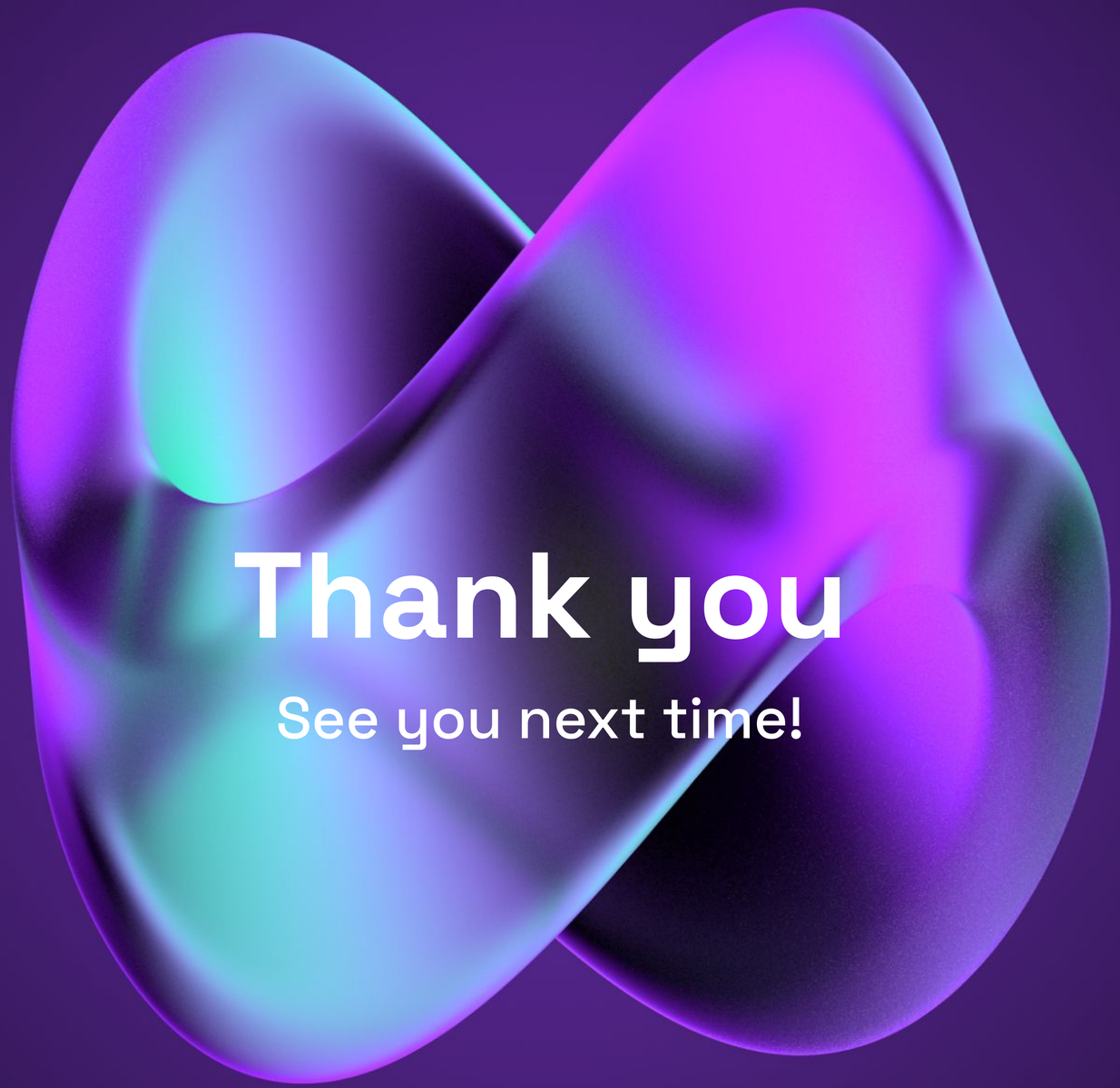
Creation and execution of fuzz tests.

ackee | blockchain security

Hands-on



ackee | blockchain security

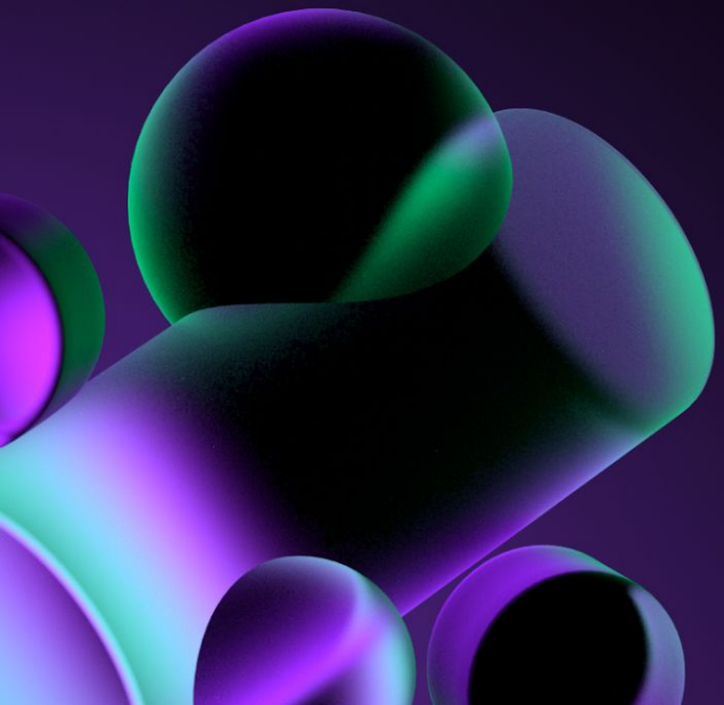


Thank you

See you next time!

ackee | blockchain security

Heading



ackee | blockchain security

Heading

- **List**
  - list item
  - list item 2