

# Thinking Like an Auditor to Develop Safer Smart Contracts

Dominic Brütsch

Lead Engineer (Founding Partner) | Chainsecurity

#### About ChainSecurity

- We are focused on blockchain security
- Smart contract audits
- Some of our clients:
  - Maker
  - Curve.fi
  - Compound
  - Aave
  - Yearn
  - o / 1inch
  - Lide

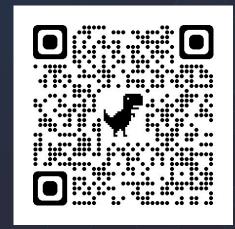


# Development Environment Setup

#### Setup:

- Clone repo https://bit.ly/3RUjnbC
- Follow the instructions in the README.md





# Why it is hard to build DeFi systems

- Composability complexity
- Blockchain is an adversarial environment
- People underestimate secure dev processes benefits













# What we are going to present today

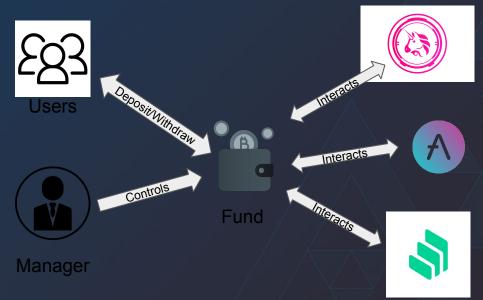
- Secure development practices
  - Writing specification before writing code
  - Writing documentation while writing code
  - Writing code and tests around the invariants
- Testing techniques
  - Property-based testing

## Specification and documentation

- The earlier the specification is written the better
- Thinking about invariants early saves dev and testing efforts.
- Documentation helps to find bugs early
- You want people to trust your code and correctly interact with it

# Building an on-chain Fund

- Fund holds external tokens and mints new erc20 token - "shares"
- Owner controls the fund
- Users / can deposit/withdraw funds, get shares and pay fees
- Fund Interacts with DeFi Protocols via adapters



# Interface - code walkthrough

#### Everyone:

- Deposit
- Withdraw

#### Owner only

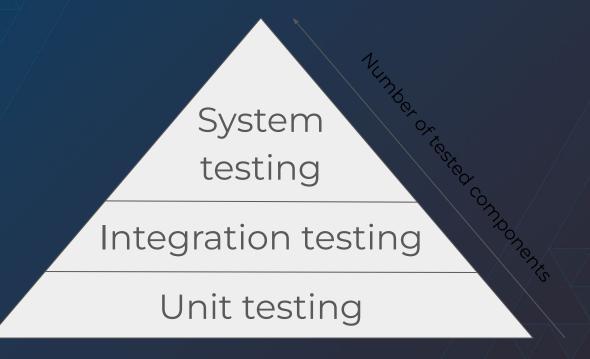
- Manage the fund
- Add/remove price feeds
- Add/remove tracked tokens

# Properties

- Users should pay 3% fee to the owner
- The owner should get fees when users deposit
- Redemption should always work



#### Different kinds of tests



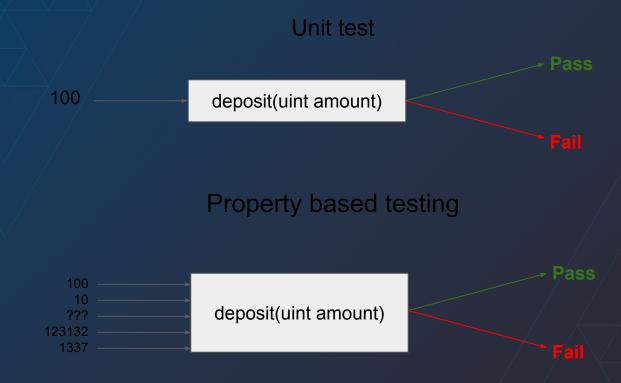
# Warm up exercise

- Users should pay 3% fee to the owner
- Users should get 97% of the value if they withdraw directly after depositing

#### Property Based Testing (Randomized input test)

- Test a property by using many randomly generated inputs
- It is similar to fuzzing but ...
- It is a white-box technique
- The tester describes roughly the shape of the input

#### Property Based Testing (Randomized input test)



## Property Based Testing (Randomized input test)

The owner should get fees when users deposit



#### Mainnet fork

- Why mainnet fork:
  - We test against deployed code
  - No need for mocking
  - Undocumented and unexpected behavior of protocols
- Redemption should always work



# Going Beyond

- Stateful testing
- Not all bugs can be uncovered by tests
- Passing tests are not proofs of correctness
- Formal Verification of code
- Manual inspection (Audit)
- Active monitoring of system invariants
- Test Driven Development (TDD)
- Invariant-based programming



Section 1 title here.

#### Section 1 title here.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

- Sollicitudin
- Consectetur
  - Condimentum
    - Magna
    - Ligula

#### Section 1 details with an image. Enter title here.

Lorem ipsum dolor sit amet, consectetur adipiscing elit sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Enter your main point / statement here.

#### Section 1 details with a main point. Enter title here

Lorem ipsum dolor sit amet, consectetur adipiscing elit sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum



Section 2 title here.

#### Section 2 title here.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

- Sollicitudin
- Consectetur
  - Condimentum
    - Magna
    - Ligula

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

- Sollicitudin
- Consectetur
  - Condimentum
    - Magna
    - Ligula

#### Section 2 details with an image Enter title here.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

#### Section 2 details with a main point Fnter title here.

Lorem ipsum dolor sit amet, consectetur adipiscing elit sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Enter your main point / statement here.

Enter your main point / statement here.

#### Here's the timeline.

Event 1 Event 2 Event 3

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididun ut labore et dolore magna aliqua. Ut enim ad minim veniam.



# Thank you!

#### Your Name

Your title, your organization email@emailaddress.com

