

About ChainSecurity

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



Development Environment Setup

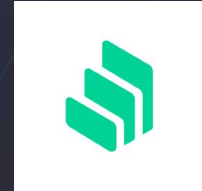
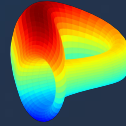
Setup:

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



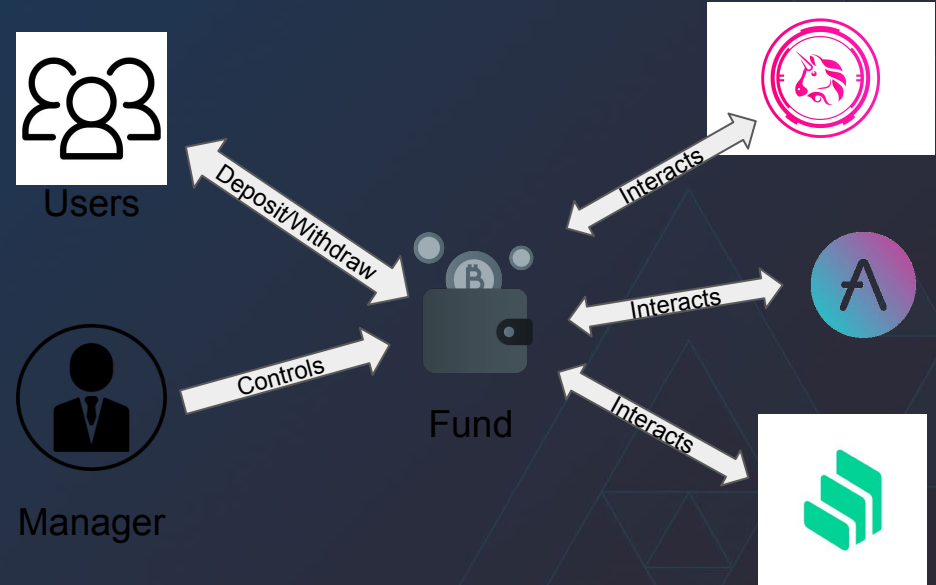
Why it is hard to build DeFi systems

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



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

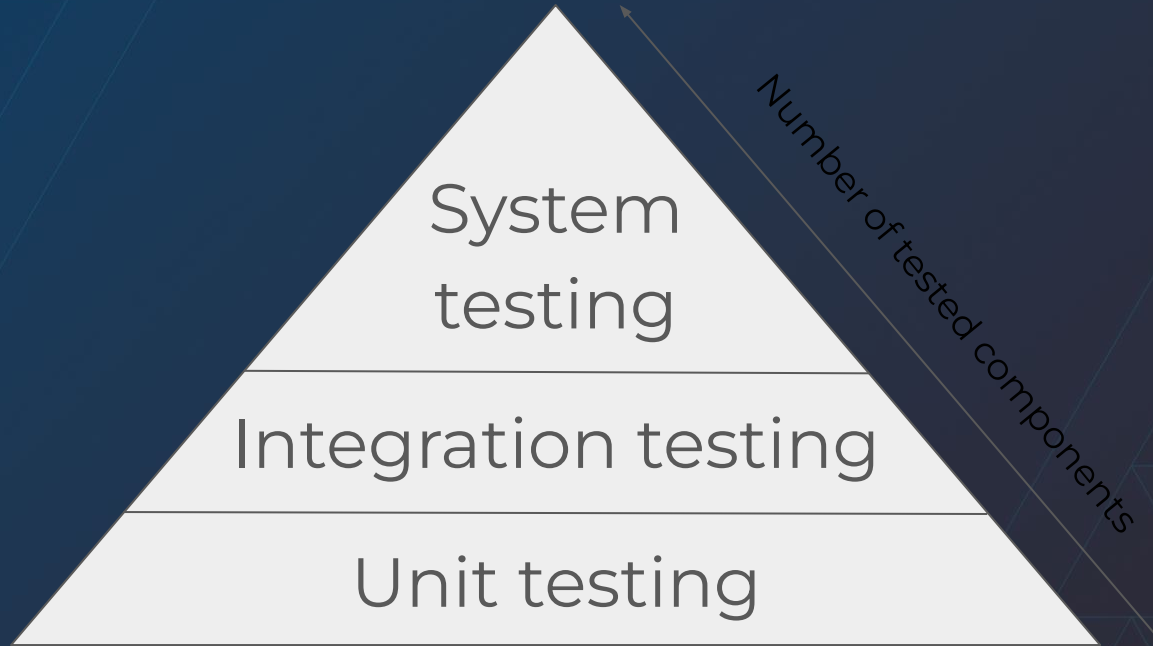


Properties

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

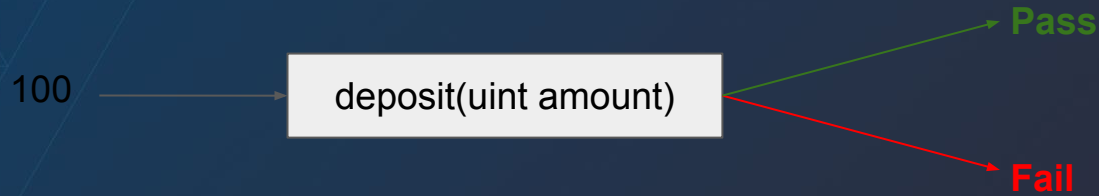


Different kinds of tests

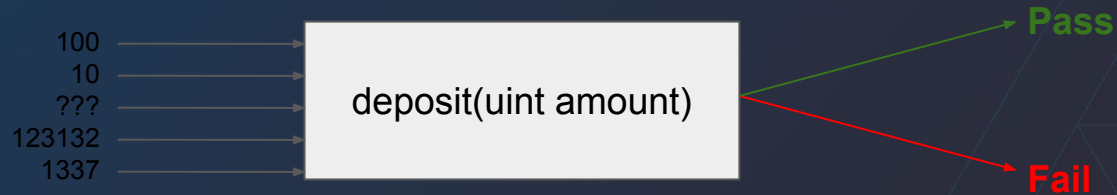


Property Based Testing (Randomized input test)

Unit test

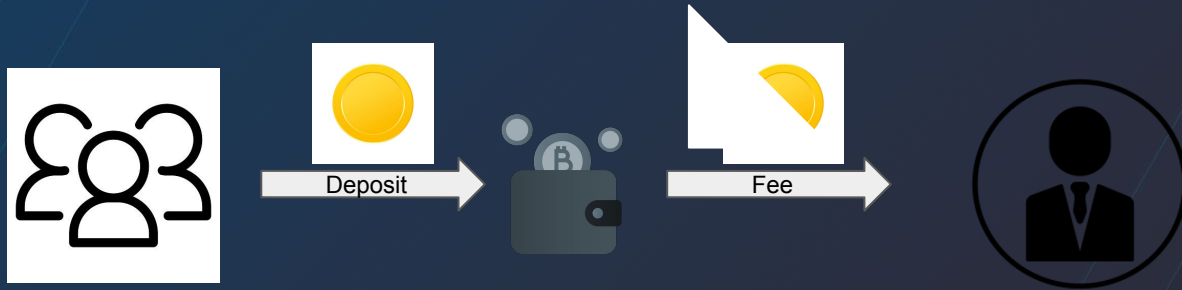


Property based testing



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



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**

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.

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 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.

Enter your main point /
statement here.



Thank you!

Your Name

Your title, your organization

email@emailaddress.com



@twitterhandle