Softbinator TECHNOLOGIES

Secure by design

Definition

Secure by design, in software engineering, means that software products and capabilities have been designed to be foundationally secure.

web2 vs web3

- Your server has public access
- Hard to impossible to upgrade your code
- Limited computational power

Languages

- Solidity
- Vyper
- Huff
- Yul
- Rust
- FE
- MOVE

Rules

- Business logic must account for decentralization
- Know your underlying VM
- KISS
- Test, test, test

Business Logic

- What third parties i’m integrating with. Are they safe?
- Does this business logic work for a blockchain project?

VM

- EVM
- SVM
- Move VM

KISS - **K**eep **I**t **S**imple, **S**tupid

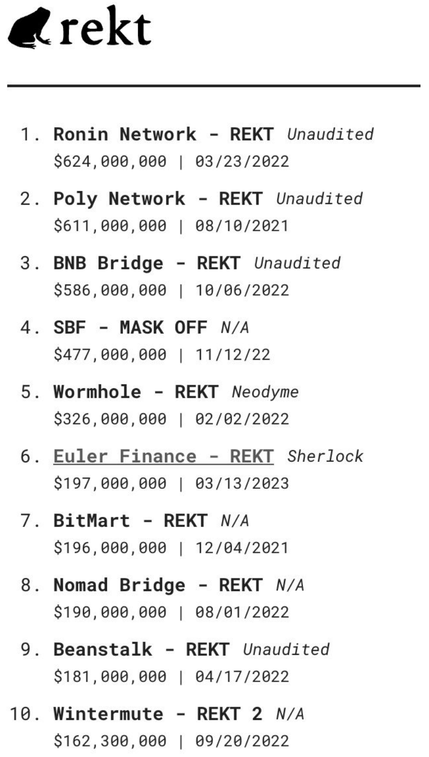
- How many contracts do i need?
- Do I need an oracle
- Do I need them to be upgradable (Upgradability can be a bug not a feature)
- Does it needs any centralization?
- What ACL strategy do i need?

Test, Test, Test

- Unit Testing (hardhat, foundry)
- Integration Testing (hardhat, foundry, web2 testing)
- Fuzzing (foundry, echidna)
- Invariant testing (foundry, certora, echidna)
- Formal Verification (Certora, SMTChecker, Halmos, K)

Learn from past mistakes

Audits are gold but not a diamond.



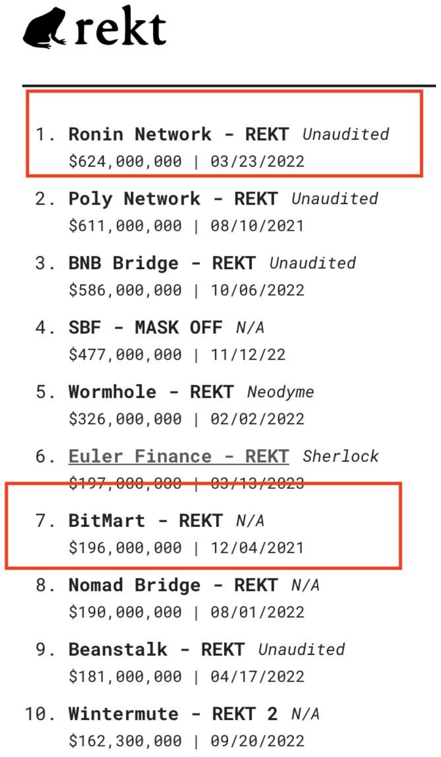
rekt

1. **Ronin Network - REKT** *Unaudited*
   $624,000,000 | 03/23/2022
2. **Poly Network - REKT** *Unaudited*
   $611,000,000 | 08/10/2021
3. **BNB Bridge - REKT** *Unaudited*
   $586,000,000 | 10/06/2022
4. **SBF - MASK OFF** *N/A*
   $477,000,000 | 11/12/22
5. **Wormhole - REKT** *Neodyme*
   $326,000,000 | 02/02/2022
6. Euler Finance - REKT *Sherlock*
   $197,000,000 | 03/13/2023
7. **BitMart - REKT** *N/A*
   $196,000,000 | 12/04/2021
8. **Nomad Bridge - REKT** *N/A*
   $190,000,000 | 08/01/2022
9. **Beanstalk - REKT** *Unaudited*
   $181,000,000 | 04/17/2022
10. **Wintermute - REKT 2** *N/A*
    $162,300,000 | 09/20/2022

rekt.news

web2 vs web3

Web2 security is important!



rekt

1. **Ronin Network - REKT** *Unaudited*
   $624,000,000 | 03/23/2022
2. **Poly Network - REKT** *Unaudited*
   $611,000,000 | 08/10/2021
3. **BNB Bridge - REKT** *Unaudited*
   $586,000,000 | 10/06/2022
4. **SBF - MASK OFF** *N/A*
   $477,000,000 | 11/12/22
5. **Wormhole - REKT** *Neodyme*
   $326,000,000 | 02/02/2022
6. **Euler Finance - REKT** *Sherlock*
   $197,000,000 | 03/13/2023
7. **BitMart - REKT** *N/A*
   $196,000,000 | 12/04/2021
8. **Nomad Bridge - REKT** *N/A*
   $190,000,000 | 08/01/2022
9. **Beanstalk - REKT** *Unaudited*
   $181,000,000 | 04/17/2022
10. **Wintermute - REKT 2** *N/A*
    $162,300,000 | 09/20/2022

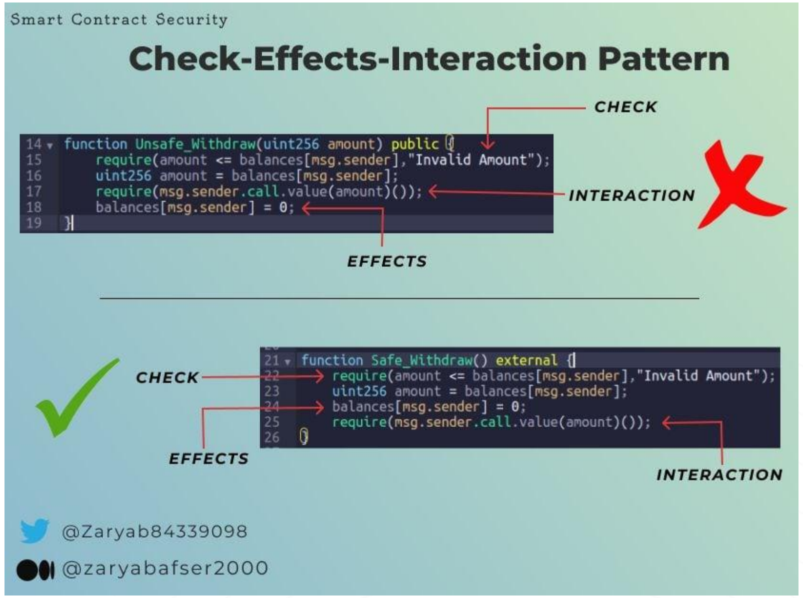
rekt.news

Common mistakes

Writing secure code is like constructing a fortress - every wall, every gate, and every defense mechanism must be meticulously crafted and fortified to prevent even the most determined intruders from penetrating its defenses.

CEI and Reentrancy

CEI = Checks-Effects-Interactions



```
function Unsafe_Withdraw(uint256 amount) public {
    require(amount <= balances[msg.sender],"Invalid Amount");
    uint256 amount = balances[msg.sender];
    require(msg.sender.call.value(amount)());
    balances[msg.sender] = 0;
}
```

```
function Safe_Withdraw() external {
    require(amount <= balances[msg.sender],"Invalid Amount");
    uint256 amount = balances[msg.sender];
    balances[msg.sender] = 0;
    require(msg.sender.call.value(amount)());
}
```

CEI and Reentrancy

Think bigger

Function Level Reentrancy
Cross-Function Reentrancy
Cross-Contracts Reentrancy
Read-Only Reentrancy

Least Privilege Principle

ACL are important, you need to analyze every privileged function and think twice who should have access to it.

Some mistakes:

- public functions that have access to sensitive data
- 3rd party managing to access functions via a suite of function calls
- Unrevoked roles

Edge-case testing

99% of the flows work, the 1% are the ones who produce bugs

Some mistakes:

- Unbounded arrays most of the time can produce DoS
- Not counting for the block gas limit
- Not considering flash loans

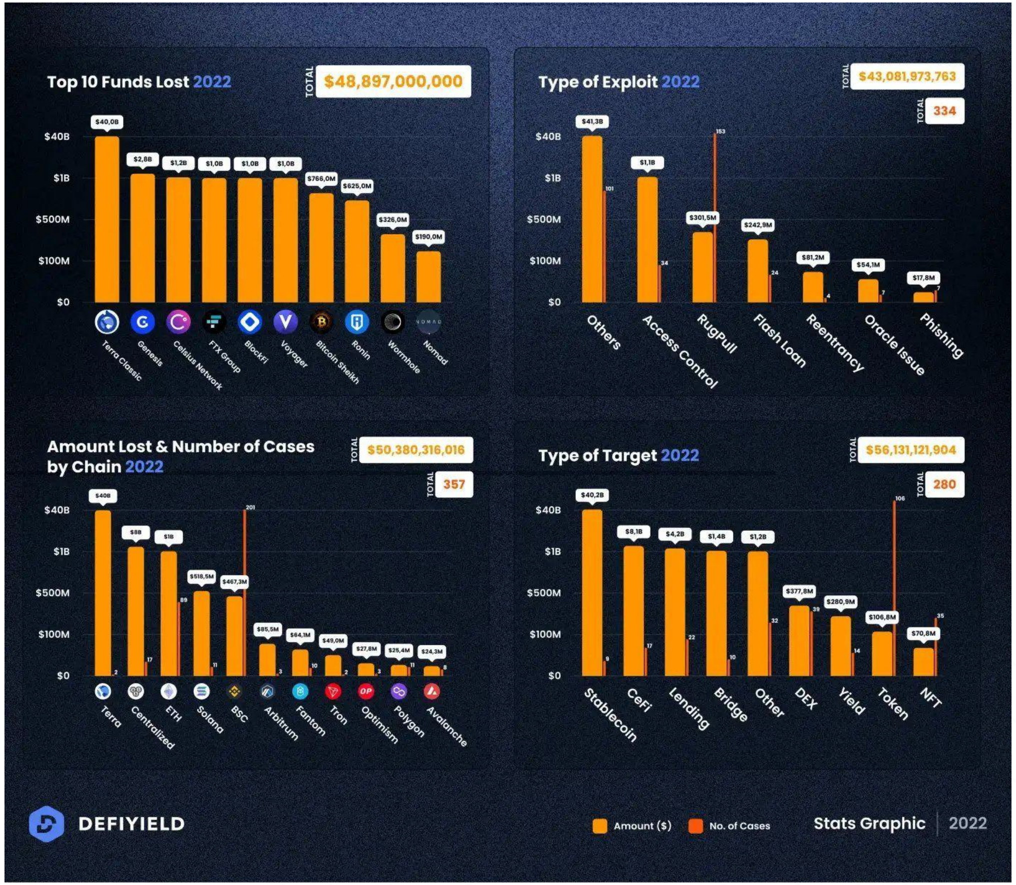
Oracles

Don’t trust your oracle

Some mistakes:

- Stale data
- Incorrect data

Stats


Top 10 Funds Lost 2022
TOTAL $48,897,000,000
$40B
$1B
$500M
$100M
$0
$40,0B
$2,8B
$1,2B
$1,0B
$1,0B
$1,0B
$766,0M
$625,0M
$326,0M
$190,0M
Terra Classic
Genesis
Celsius Network
FTX Group
BlockFi
Voyager
Bitcoin Sheikh
Ronin
Wormhole
Nomad
Type of Exploit 2022
TOTAL $43,081,973,763
TOTAL 334
$41,3B
101
$1,1B
34
$301,5M
153
$242,9M
24
$81,2M
4
$54,1M
7
$17,8M
7
Others
Access Control
RugPull
Flash Loan
Reentrancy
Oracle Issue
Phishing
Amount Lost & Number of Cases by Chain 2022
TOTAL $50,380,316,016
TOTAL 357
$40B
2
$8B
17
$1B
89
$518,5M
11
$467,3M
201
$85,5M
3
$64,1M
10
$49,0M
2
$27,8M
3
$25,4M
11
$24,3M
8
Terra
Centralized
ETH
Solana
BSC
Arbitrum
Fantom
Tron
Optimism
Polygon
Avalanche
Type of Target 2022
TOTAL $56,131,121,904
TOTAL 280
$40,2B
9
$8,1B
17
$4,2B
22
$1,4B
10
$1,2B
32
$377,8M
39
$280,9M
14
$106,8M
106
$70,8M
35
Stablecoin
CeFi
Lending
Bridge
Other
DEX
Yield
Token
NFT
DEFIYIELD
🟧 Amount ($)
🟥 No. of Cases
Stats Graphic | 2022

❮ Q & A

**Thank you,
frens!**