E.T.S. DE INGENIERÍA DE TELECOMUNICACIÓN
UNIVERSIDAD DE MÁLAGA


UNIVERSIDAD DE MÁLAGA | uma.es

# A STUDY ON ETHEREUM SECURITY: BRIDGING EDUCATIONAL GAPS THROUGH THE DEVELOPMENT OF FAILLAPOP

Marco López González
Tutor: Isaac Agudo Ruiz

Grado en Ingeniería Telemática

Málaga, 18 de 07 de 2024

## Contents

E.T.S. DE INGENIERÍA DE TELECOMUNICACIÓN
UNIVERSIDAD DE MÁLAGA

# Motivation

## Security Problems

E.T.S. DE INGENIERÍA DE TELECOMUNICACIÓN
UNIVERSIDAD DE MÁLAGA

Chainalysis

### $197 Million Stolen: Euler Finance Flash Loan Attack Explained [UPDATED 4/6/23]

Chainalysis new

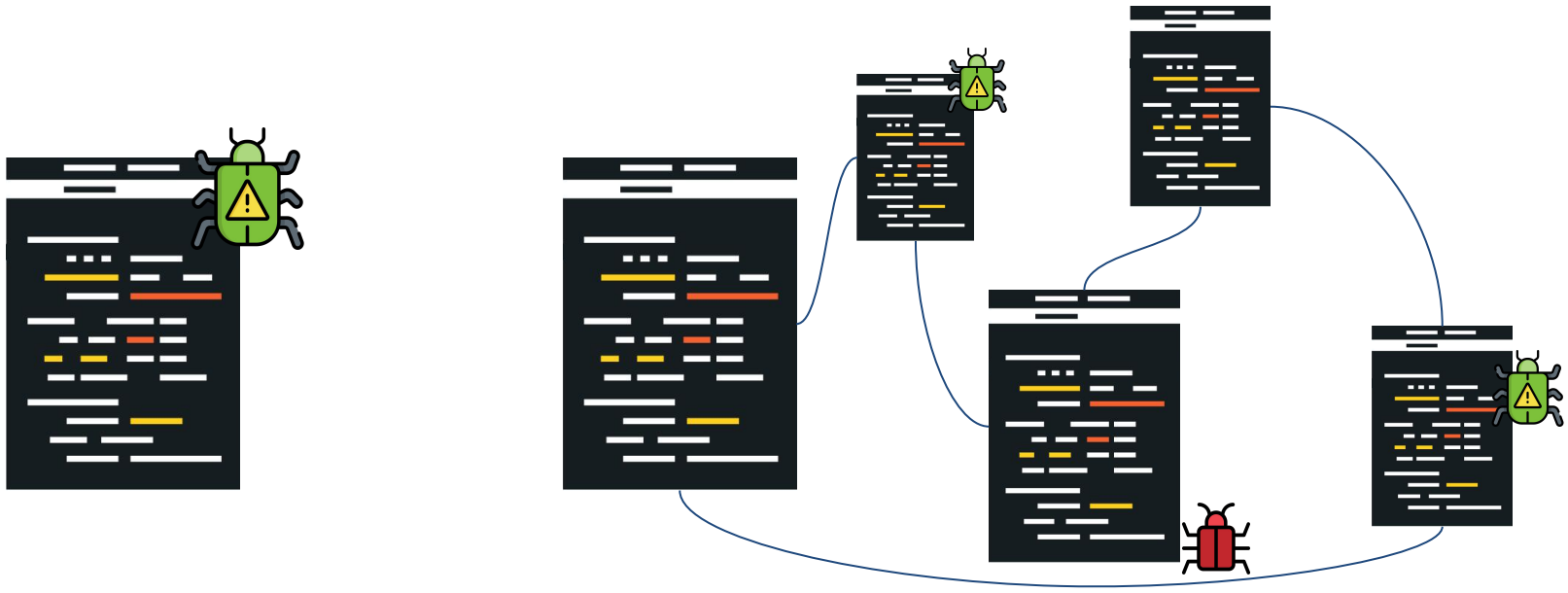
| Categories | Attacks | | Bug Bounties | |
|---|---|---|---|---|
| | # Bugs | Fund loss | # Bugs | Bounties |
| Lending | 1 | $ 5,000K | 2 | $ 1,630K |
| Dexes | 7 | $ 13,950K | 3 | $ 65K |
| Yield | 6 | $ 20,300K | 1 | $ 10K |
| Services | 3 | $ 5,600K | 2 | $ 610K |
| Derivatives | - | - | 2 | $ 200K |
| Yield Aggregator | 1 | $ 2,100K | 2 | $ 300K |
| Real World Assets | 2 | $ 1,127K | 1 | $ 50K |
| Stablecoins | 5 | $211,360K | - | - |
| Indexes | - | - | 1 | $ 90K |
| NFT Marketplace | 1 | $ 20K | - | - |
| NFT Lending | 2 | $ 5,800K | - | - |
| Cross Chain | - | - | 1 | $10,000K |
| Others | - | - | 1 | $ 1,050K |
| Total | 28 | $265,257K | 16 | $14,005K |

Demystifying Exploitable Bugs in Smart Contracts

# Motivation

## Capture the Flag Deficits

E.T.S. DE INGENIERÍA DE TELECOMUNICACIÓN
UNIVERSIDAD DE MÁLAGA



# Methodology

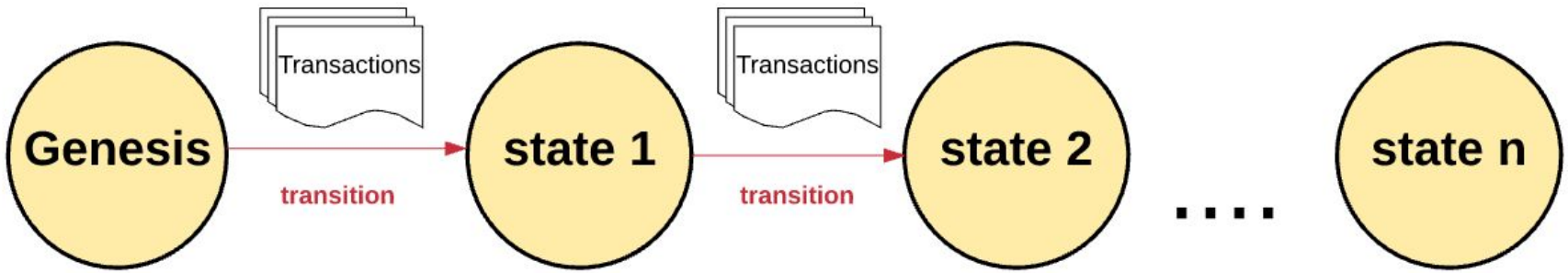
E.T.S. DE INGENIERÍA DE TELECOMUNICACIÓN
UNIVERSIDAD DE MÁLAGA

1. Literature Review and State-of-the-Art Analysis
2. Initial Project Audit and CTF Participation
3. Research on Common Vulnerabilities in Real Applications
4. Design and Implementation of New Features
5. Faillapop's Adherence to Best Practices

# Ethereum

E.T.S. DE INGENIERÍA DE TELECOMUNICACIÓN
UNIVERSIDAD DE MÁLAGA

- What is Ethereum?
  - Distributed deterministic state machine
  - Single state - globally accessible
  - Virtual Machine




Imagen

# Ethereum

## Smart Contracts

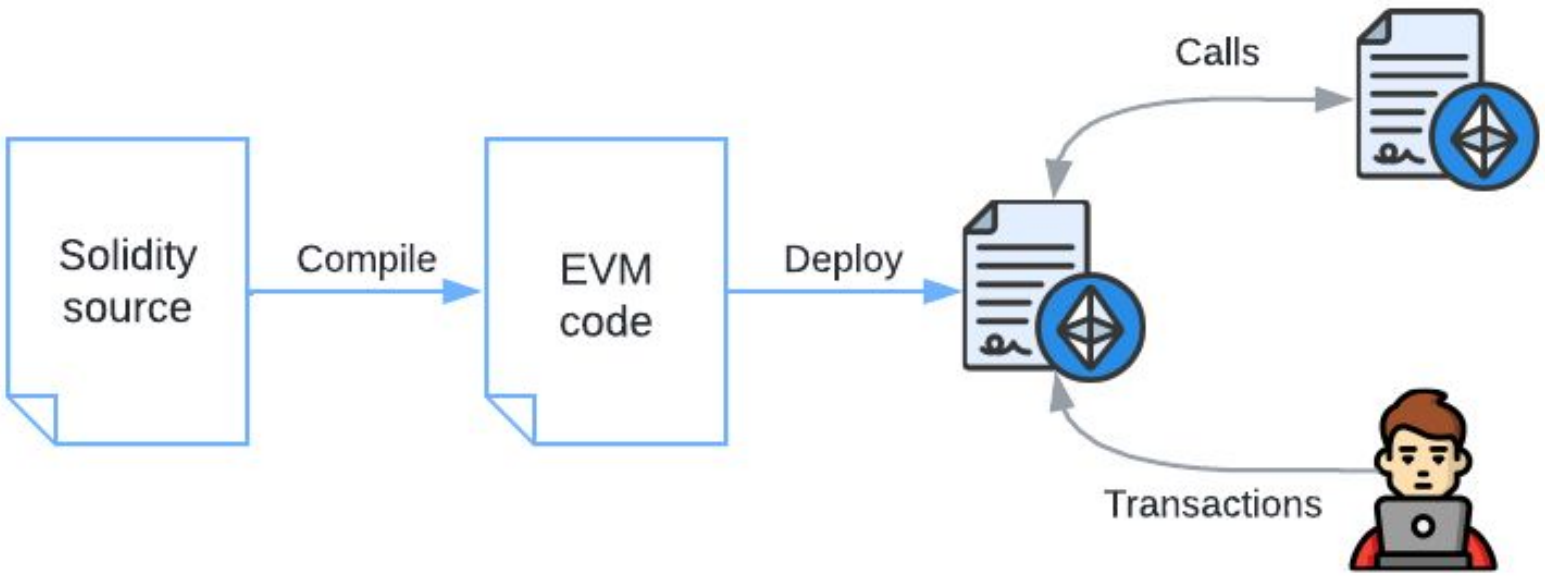
E.T.S. DE INGENIERÍA DE TELECOMUNICACIÓN
UNIVERSIDAD DE MÁLAGA

```
pragma solidity ^0.8.0;

contract ContratoSimple {

    uint256 public numeroParticipantes;

    function add() public {
        numeroParticipantes++;
    }

    function set(uint256 _incremento) public{
          numeroParticipantes += _incremento;
    }

    function get() public view returns (uint256) {
        return numeroParticipantes;
    }
}
```

# Ethereum

## Smart Contracts

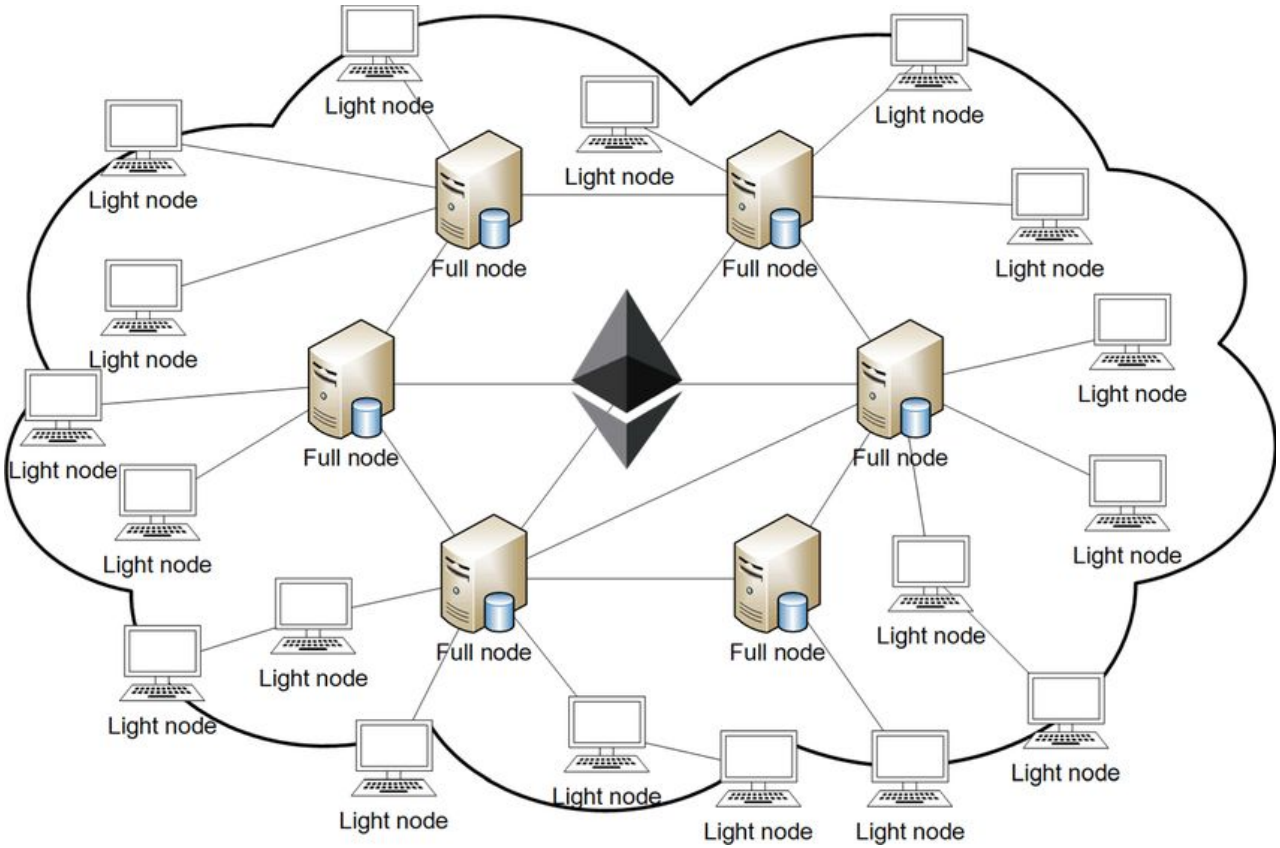




# Ethereum

## Consensus Rules






Imagen

# Ethereum Security

## Properties

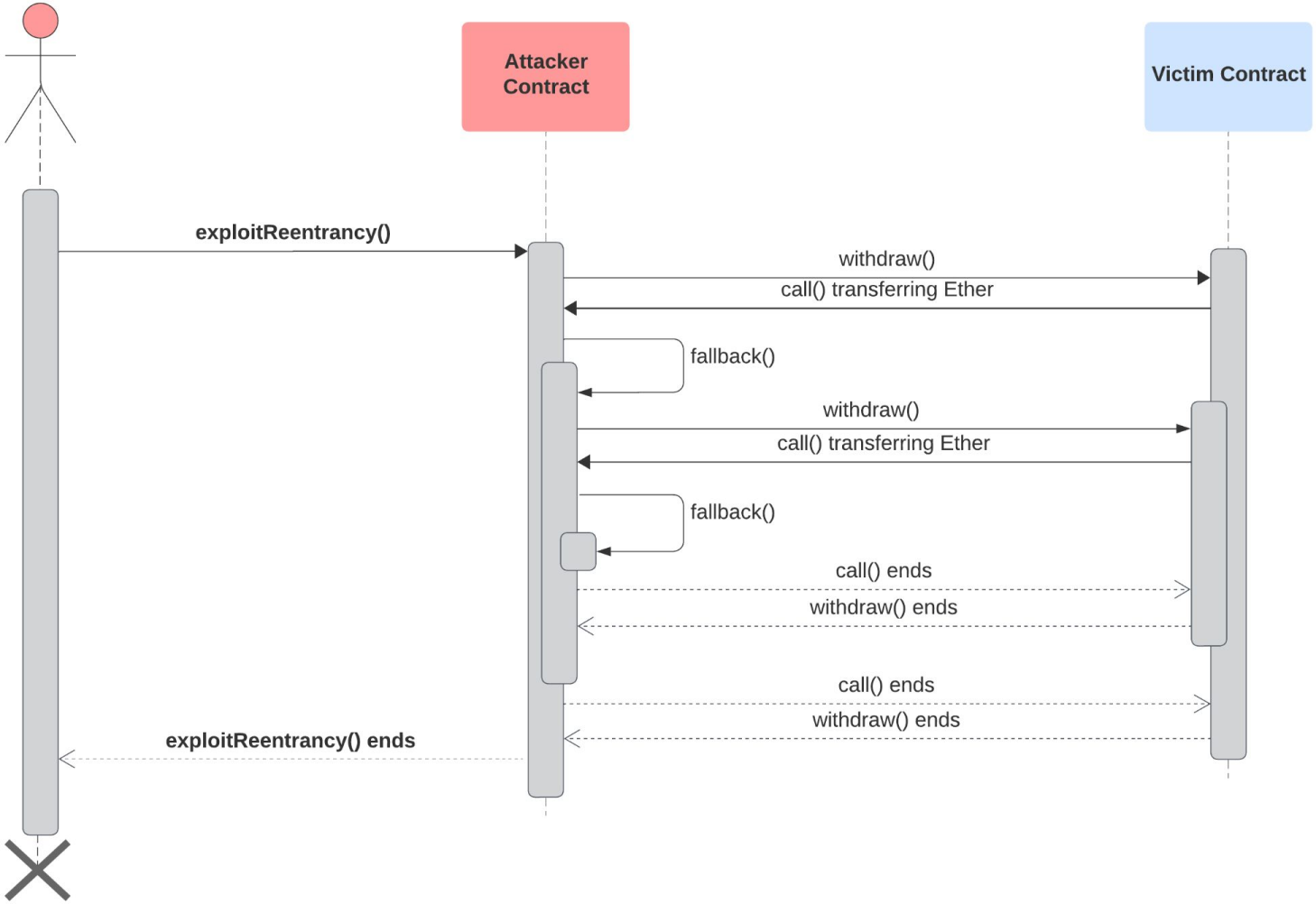


- Immutability
- Determinism
- Transparency
- Flash Loans
- MEV

# Ethereum Security

## Reentrancy

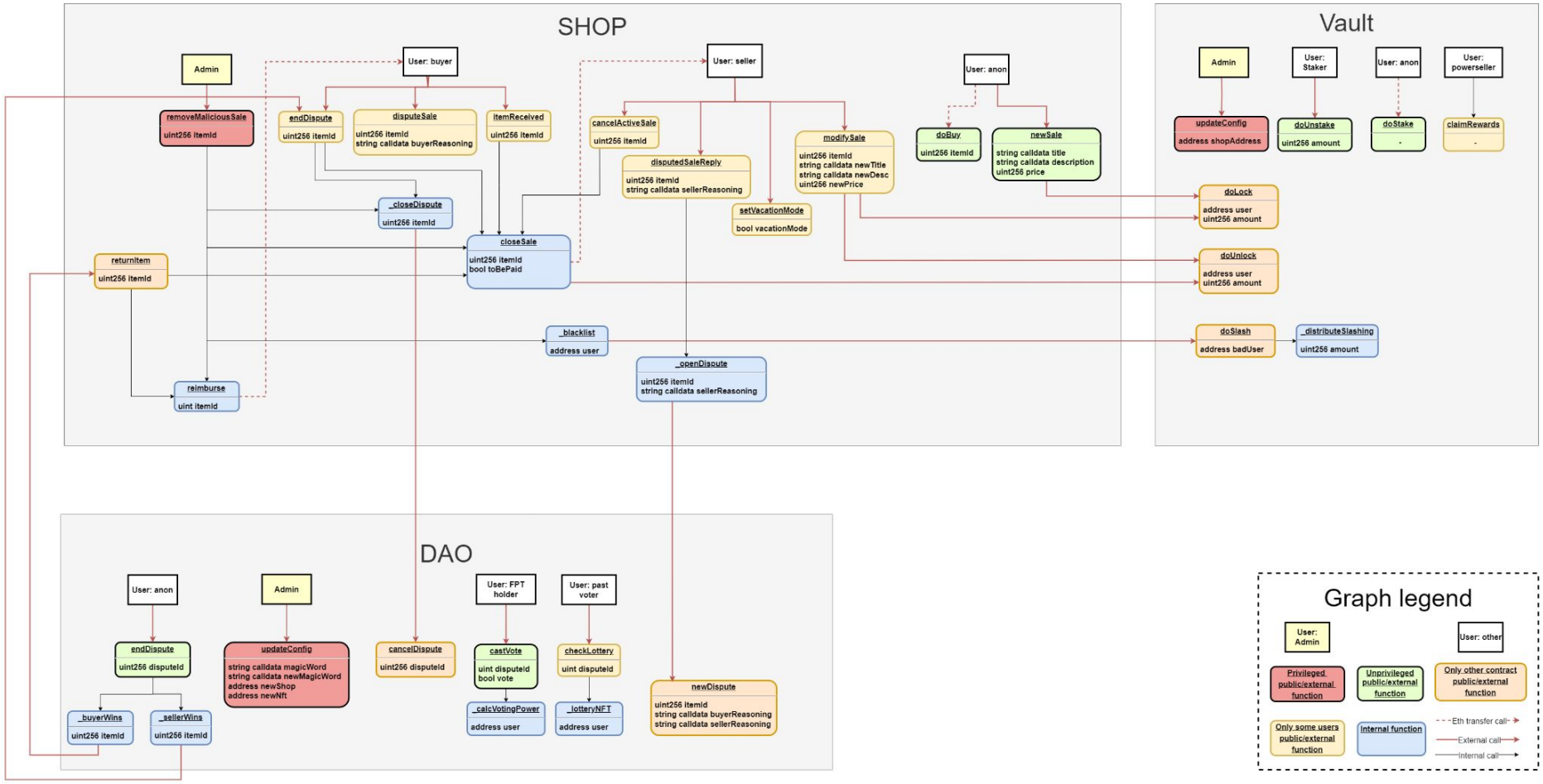
E.T.S. DE INGENIERÍA DE TELECOMUNICACIÓN
UNIVERSIDAD DE MÁLAGA



# Faillapop

## Initial Stage

E.T.S. DE INGENIERÍA DE TELECOMUNICACIÓN
UNIVERSIDAD DE MÁLAGA

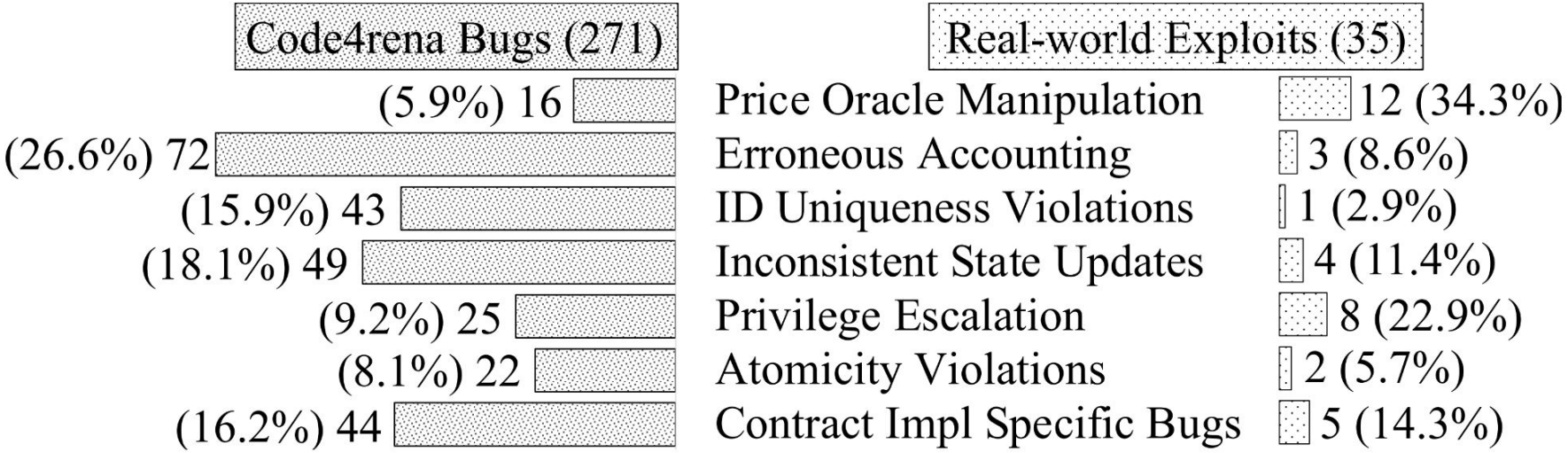


# Faillapop

## Initial Security Evaluation

E.T.S. DE INGENIERÍA DE TELECOMUNICACIÓN
UNIVERSIDAD DE MÁLAGA

1. Initial Project Audit 
2. Engagement in CTF Exercises 
3. Examination of Common Vulnerabilities in Real Applications




Demystifying Exploitable Bugs in Smart Contracts

# Faillapop

## Initial Project Audit

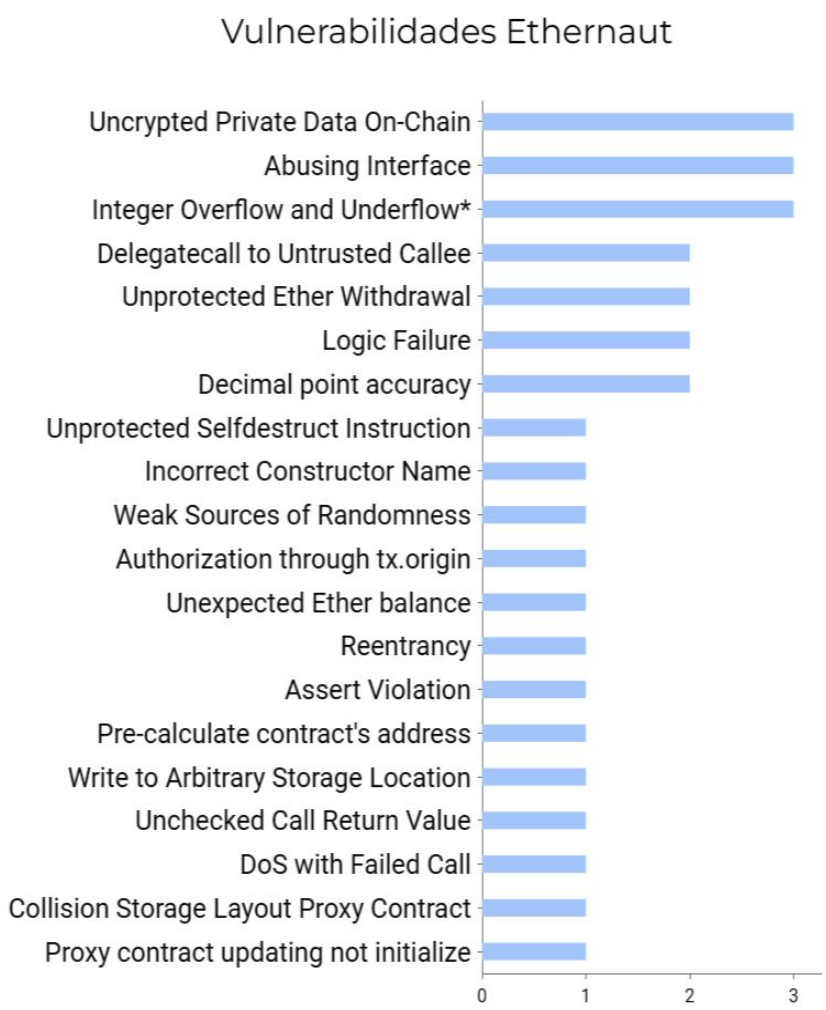
E.T.S. DE INGENIERÍA DE TELECOMUNICACIÓN
UNIVERSIDAD DE MÁLAGA

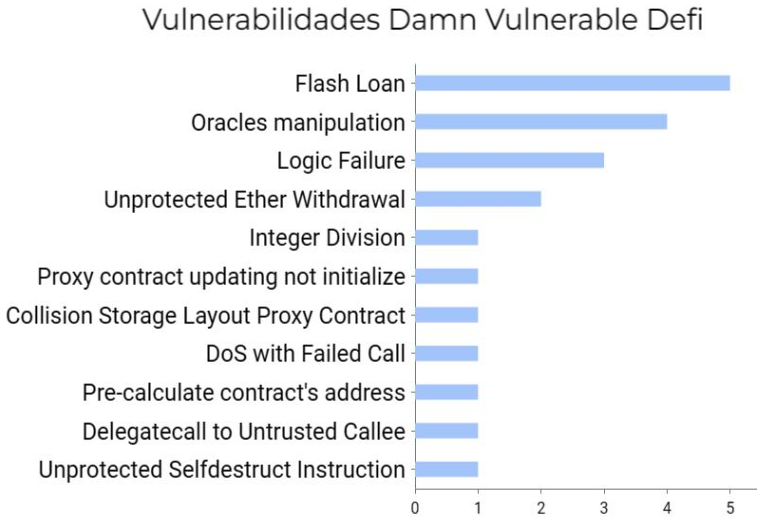
1. Code Structure Analysis
2. Threat Modeling
3. Initial Code Reading
4. Detailed Vulnerability Identification
5. Execution Flow Analysis
6. Proof of Concept

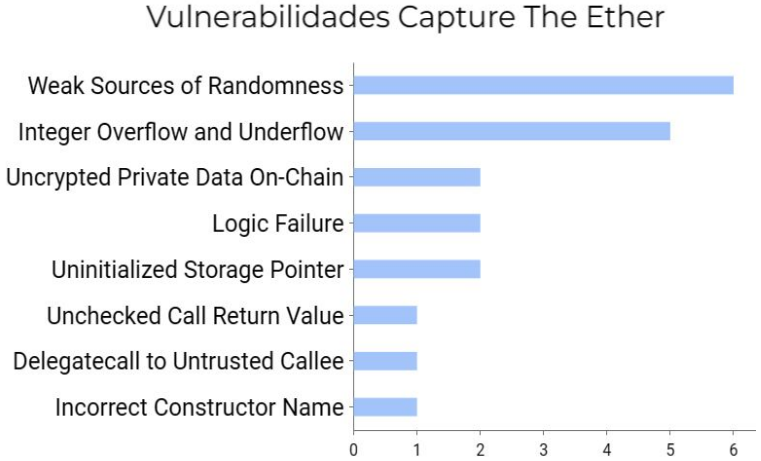
# Faillapop

## Engagement in CTF Exercises

E.T.S. DE INGENIERÍA DE TELECOMUNICACIÓN
UNIVERSIDAD DE MÁLAGA



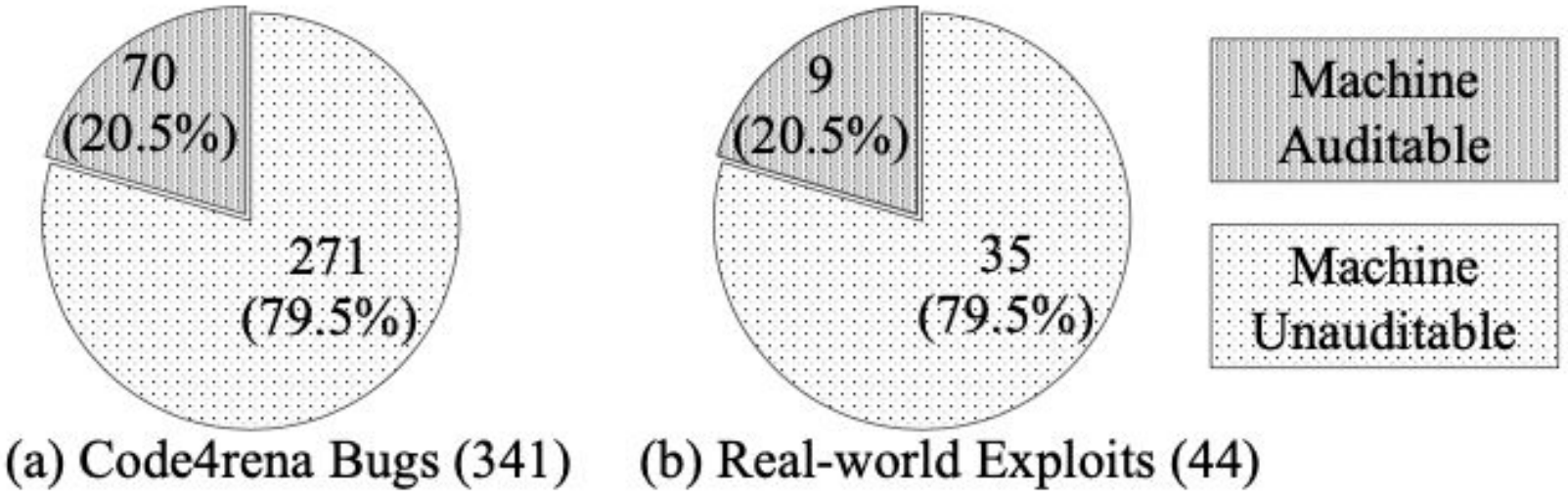



# Faillapop

## Examination of Common Vulnerabilities in Real Applications

E.T.S. DE INGENIERÍA DE TELECOMUNICACIÓN
UNIVERSIDAD DE MÁLAGA

- 385 vulnerabilities
- 167 Smart Contracts



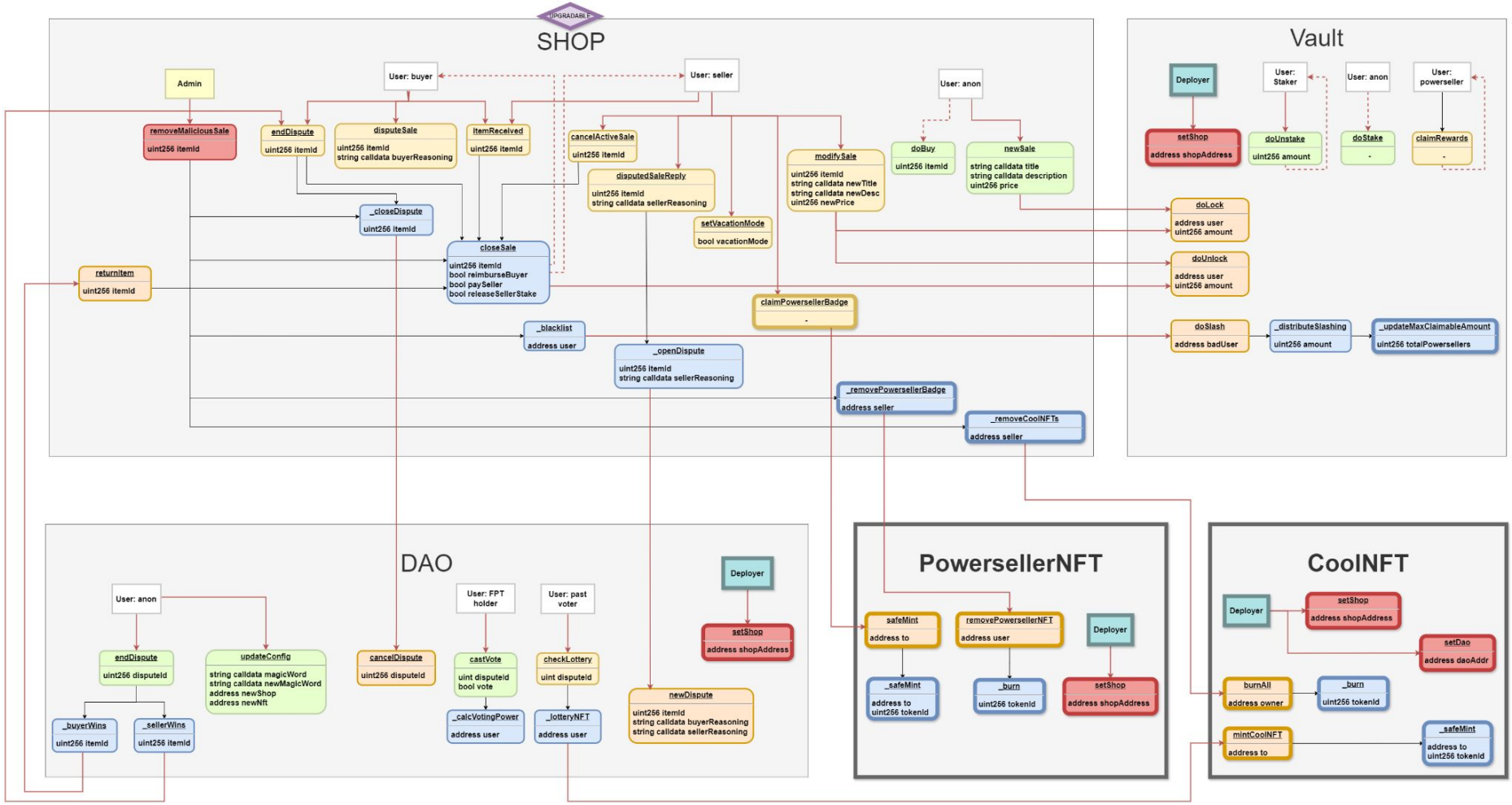

(a) Code4rena Bugs (341) (b) Real-world Exploits (44)

Demystifying Exploitable Bugs in Smart Contracts

# Faillapop

## Current Stage

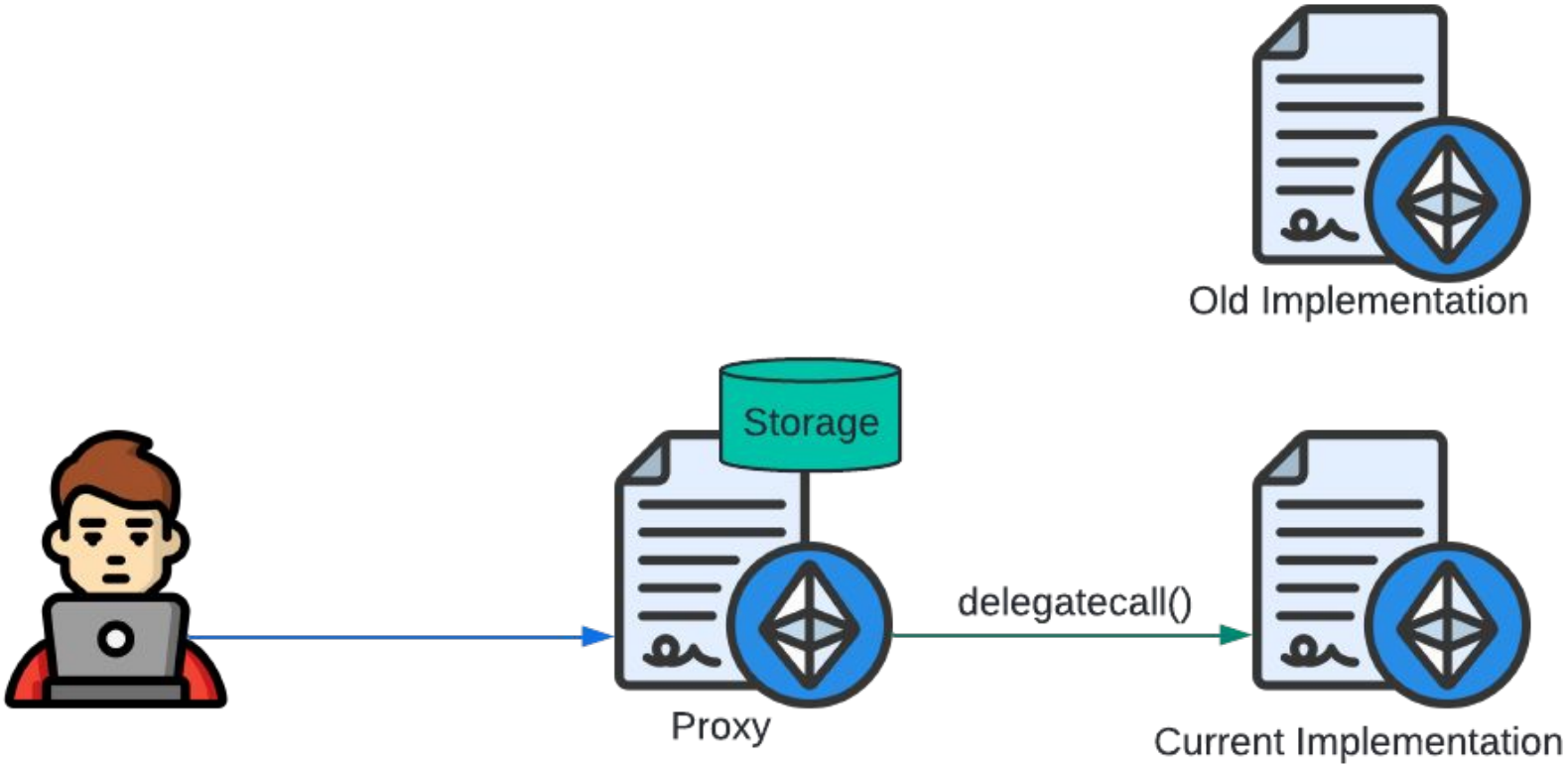
E.T.S. DE INGENIERÍA DE TELECOMUNICACIÓN
UNIVERSIDAD DE MÁLAGA



# Faillapop

## Proxy for Upgradeable Shop Contract





# Faillapop

## Features

E.T.S. DE INGENIERÍA DE TELECOMUNICACIÓN
UNIVERSIDAD DE MÁLAGA

- Commit-Reveal Scheme for Dispute Voting
- Comprehensive Documentation
- Deployment Script Implementation
- Optimization Using Inline Assembly
- Comprehensive Unit and Integration Testing

# Faillapop

## Conclusions and Future Work

E.T.S. DE INGENIERÍA DE TELECOMUNICACIÓN
UNIVERSIDAD DE MÁLAGA

- Conclusions
  - Comprehensive and realistic educational resources
  - Faillapop
    - ➢ Simulates complex applications
    - ➢ Develop practical skills
    - ➢ Benefits institutions and companies
- Future Work
  - Continuous updating
  - Promotion and workshops


UNIVERSIDAD
DE MÁLAGA | uma.es