Protecting smart contracts of Decentralized Finance systems against Reentrancy attacks

I- Problem

- Decentralized Finance systems are massively popular.
- Big target for attackers.
- Reentrancy attacks pose a threat.
- Thousands of smart contracts are vulnerable to reentrancy attacks.

II- Terminology

- Smart contracts: programs stored on a blockchain that run when predetermined conditions are met.
- Decentralized Finance systems: financial products available on a public decentralized blockchain.
- Reentrancy attacks: Allow the attacker to repeatedly withdraw assets from a smart contract.

III- Research question

How can we protect smart contracts of DeFi systems deployed on the Ethereum blockchain that are known to be vulnerable to reentrancy attacks?

IV- Methodology

- Literature analysis.
- Create a tool to detect reentrancy attacks.
- Proof of concept for the tool.

```
contract Victim {

    function withdraw(unit amount) public {
        if (balance[msg.sender] >= amount){
            msg.sender.call.value(amount)();
            balances[msg.sender] -= amount;
        }
    }
}
```

Fig 1: Solidity code of a vulnerable smart contract

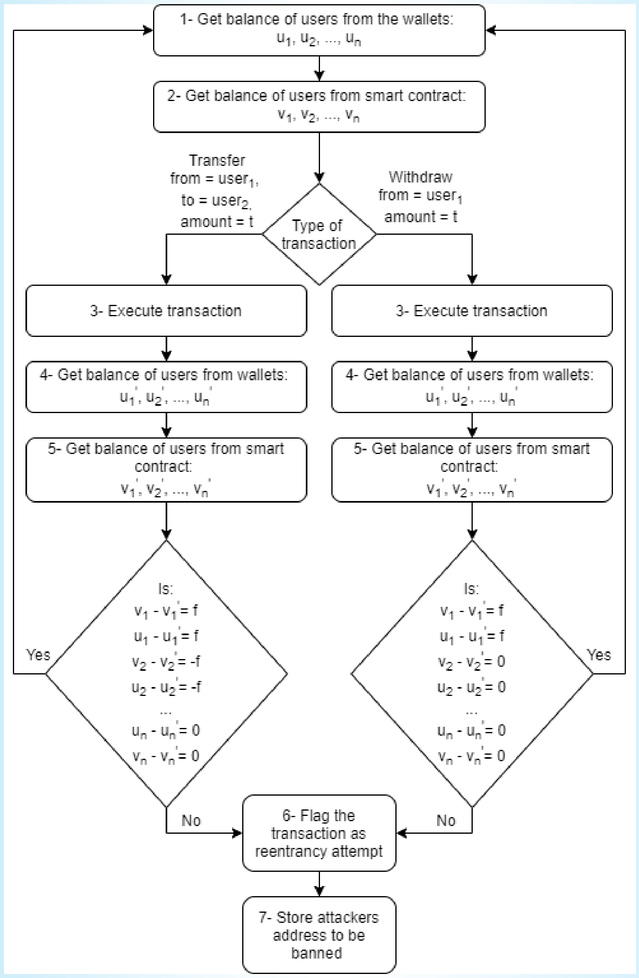

Fig 2: Workflow of SmartTool

V- Solution - SmartTool:

1) Main idea:
- Compare difference between balance on the Protocol layer & the Application layer.
- Stop any transaction that creates a discrepancy between both layers.

2) Proof of concept:
- Attack vulnerable smart contracts by three types of reentracy attacks:

1. Single Function reentrancy attack.
2. Cross Function reentrancy attack.
3. Constantinople reentrancy attack.

VI- Discussion

1) Results of the proof of concept tests:
- SmartTool is able to detect and stop all three attacks.

2) Limitations of SmartTool:
- Causes extra gas costs because of extra checks.
- The current approach needs access to the smart contract's code which is not always possible.

VII- Conclusion

- SmartTool succesfully stops three types of attacks.
- The current implementation was created directly on the vulnerable smart contract, other approaches of implementation can be researched further.

TU Delft

Responsible professor: Zekeriya Erkin | Supervisor: Oğuzhan Ersoy | Research Project - CSE3000 | Nafie El Coudi El Amrani | 4771338 | N.ElCoudiElAmrani-1@student.tudelft.nl