Decentralized System

Solidity (cnt’d)

Payable smart contract

- RibbaShop is an off-line shop that sells candies and stickers in change of Sepolia wei
- It has an initial stock for candies and stickers, and some rules
  - For each transactions it is possible to buy
    - Only one sticker
    - At most five candies
  - Each address can own at most three stickers
  - There is no limit on the number of candies (if they are available in stock)

Payable smart contract

- Only the owner of the smart contract can refill the stocks (both candies and stickers)
- Only the owner of the smart contract can transfer the balance of the smart contract to their own address

Tasks

- **Audit the code** of the smart contract to check for any vulnerabilities or missing functions

- **Add the following functionalities**
  - Stickers can be transferred to other addresses (easy)
    (of course not only on the blockchain but also off-chain)
  - Stickers can be sold to other addresses, possibly with a different price (more difficult)

Audit of smart contracts

- **Manual Code Review**
  - Check for naming conventions and comments; code should be understandable to other developers
  - Review each function to confirm it meets the intended logic
- **Automated Analysis**
  - Use automated tools to scan the contract and catch common vulnerabilities, gas inefficiencies, and areas prone to reentrancy attacks
  - Review automated findings


Start
DEMO