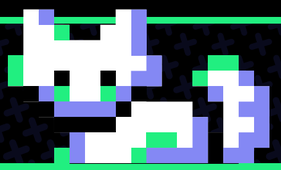
PLAYER 1 HIGHSCORE 2500 PLAYER 2

START MENU SIGN IN

INTRODUCTION TO WEB3 SECURITY

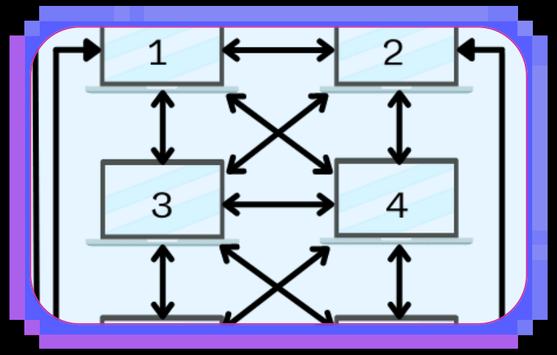
RE:HACK

BY RE:HACK



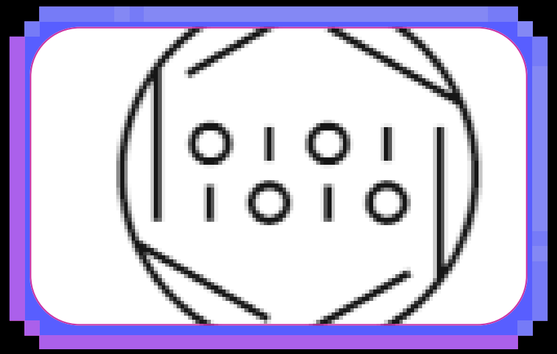
MENU

WHAT IS BLOCKCHAIN ?



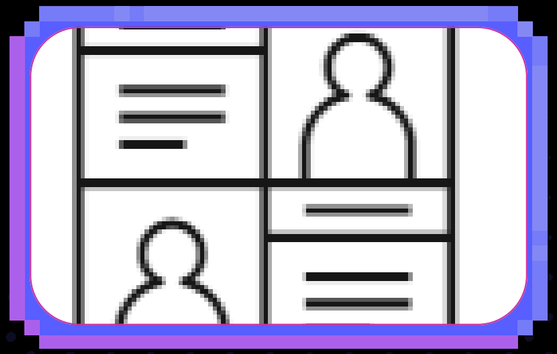
A DECENTRALIZED LEDGER

Every transaction is recorded on chain and is anonymous.



IMUTABLE RECORDS

Data cannot be tampered with.



NOT OWNED BY A SINGLE ENTITY

Uses a peer-to-peer network and a distributed network technology.

BLOCKCHAIN

MENU 01 07 12

WHAT ARE SMART CONTRACTS?

- SET OF RULES TO SPEED UP TRANSACTIONS
- RUN AUTOMATICALLY ON THE BLOCKCHAIN
- USED TO STORE FUNDS(EX: SMART CONTRACT WALLET)
- NEEDS PROPER SECURITY REVIEW AS THEY STORE BILLIONS OF DOLLARS IN CRYPTO.

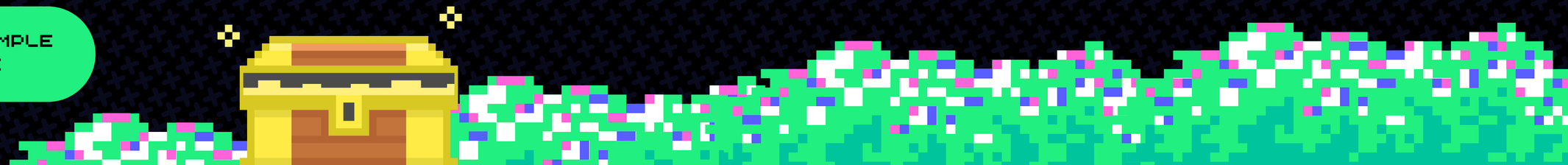
CAN YOU FINDTHE VULNERABILITY HERE?

```
// withdraw function allows users to transfer their eth to an address
    function withdraw(uint256 amount, address from, address to) public {
        require(balances[from] >= amount, "Insufficient balance");

       //updates the internal balance mapping
        balances[from] -= amount;
        balances[to] += amount;

        // Transfer the amount to the 'to' address
        payable(to).transfer(amount);
    }
```

LETS PLAY A SIMPLE CHALLENGE



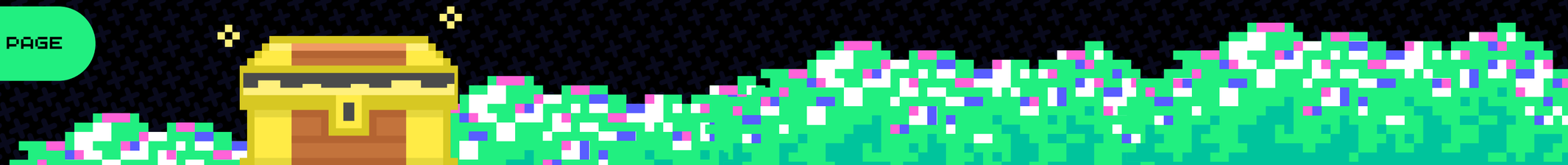
CHALLENGE 2#

```
function claimReward() public {
    require(balances[msg.sender] > 0, "No balance to claim reward");

    balances[msg.sender] += 1 ether;
    hasClaimedReward[msg.sender] = true;

    // Transfer reward to the user
    payable(msg.sender).transfer(1 ether);
}
```

BACK TO AGENDA PAGE



CHALLENGE 3# RE-ENTRANCY

```
function withdraw() public {
    uint256 bal = balances[msg.sender];
    require(bal > 0);

    (bool sent,) = msg.sender.call{value: bal}("");
    require(sent, "Failed to send Ether");

    balances[msg.sender] = 0;
}
```

BACK TO AGENDA PAGE