CAPLOCK SECURITY

Auditing Smart Contracts

May 14, 2019

Tuan Phan, CISSP, PMP, CBSP, Security+, SSBB
Partner, Caplock Security LLC
tphan@caplocksecurity.com @ChainOpSec LinkedIn.com/in/tuanphan/
202-780-5455

1

About Us

CAPLOCK SECURITY

Caplock Security provides actionable and impactful information security services to businesses and Federal government agencies.

Caplock Security understands information security from every angle, enabling us to get to the root of the problem faster and with more lasting results. Our focus on information security offers invaluable insight for our clients when delivering innovative security solutions to meet these obstacles.

From emerging to mature technologies, Caplock Security is the trusted advisor to key decision makers to help shape and manage information security strategies, policies, and risk management.

2

Learn More about Blockchain Security?

CAPLOCK SECURITY

- Sign up for my Blockchain Security Seminar
- Details: http://www.caplocksecurity.com/blockchain-security-training
- URL: eventbrite - https://www.eventbrite.com/e/blockchain-security-seminar-tickets-61197477302
- Date and Time: Tue, June 25, 2018 from 9 AM – 5 PM
- Location: 1701 Duke Street, Suite 500, Alexandria, VA 22314

3

Disclaimer

CAPLOCK SECURITY

Everything you are about to observe and learn from this presentation are the opinions of the presenter(s) and Caplock Security LLC. Statements presented do not represent the views or policies of anyone other than the presenter. The information in this presentation is provided for educational purposes only, and are not recommendations. Under no circumstances does this information represent a recommendation for a particular product, service, design or implementation.

INFORMATION IS PROVIDED TO THE ATTENDEES "AS IS." NEITHER CAPLOCK SECURITY LLC, NOR ITS PRINCIPLES, NOR ITS AFFILIATES, NOR ANY THIRD PARTY PROVIDER MAKE ANY EXPRESS OR IMPLIED WARRANTIES OF ANY KIND REGARDING THE INFORMATION, INCLUDING, WITHOUT LIMITATION, ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE.

4

Agenda

CAPLOCK SECURITY

- What is Smart Contract?
- Use Cases
- Regulatory Drivers
- Legality
- Characteristics and Programming
- Auditing Considerations
- Security Considerations
- Best practices
- Final Words

5

What is a Smart Contract

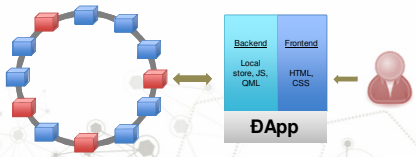
CAPLOCK SECURITY

- Is a computer program consisting of lines of code that prescribes its conditions and outcomes.
  - Solidity
  - Go/Javascript
  - Java
- Is stored and processed on a distributed ledger.
- Stays dormant until called by a transaction.
- Transactions performed are written onto the distributed ledger.

6

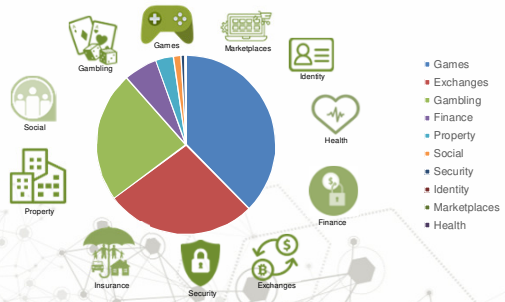
Đapps and Smart Contracts

- ĐApps are blockchain-enabled applications/websites/platforms
- Rely on smart contracts for logic processing.



7

Use Cases for Smart Contracts



8

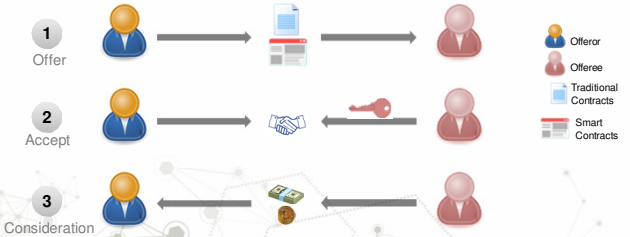
Key Regulatory Drivers

United States
- Electronic Signatures in Global and National Commerce (ESIGN) Act
- Uniform Electronic Transactions Act (UETA)
- FDA's 21 CFR Part 11

European Union
- Electronic Identification and Trust Services Regulation (910/2014/EC)
- Electronic Signature Directive (1999/93EC) [obsoleted]

9

Are Smart Contracts Legally Binding?



10

Models of Smart Contracts

- Smart contracts vs. traditional natural language contracts
  - Consumer-centric
  - Completeness
  - Governance, amendments and disputes
- Two models:

11

Key Characteristics of Smart Contract

- Turing completeness
- Immutable
- Visibility (untrusted vs. trusted)
- Deterministic
- Atomic
- Interaction with other interfaces
- Self-destruct (deleted contracts)

12

Programming Smart Contracts

CAPLOCK SECURITY

Ethereum
- Solidity
- An IDE (Remix IDE, EthFiddle)
- Wallet with some test currencies
- Local development environment or web-based at https://remix.ethereum.org/
- Connection to the actual blockchain network, local or testnet

Hyperledger Fabric
- Go/Javascript (popular for permissioned blockchains)
- An IDE (HLFV Composer, VSCode or similar editors)
- Local development environment or IBM Bluemix Console
- Connection to the actual blockchain network, local or testnet

13

What IT Auditing is not?

CAPLOCK SECURITY

- Is not accounting controls or financial auditing.
- Is not compliance checking or testing.
- Is not an evaluation of whether IT considerations to be carried out in scope of an audit.

14

Core of IT Auditing

CAPLOCK SECURITY

- Understand the "technology thing" to identify and mitigate risk.
- Achieve and monitor compliance effectively
- Assess effectiveness of the control systems and rules.

IT Auditing = Identifying risk and the appropriate controls to mitigate risk to an acceptable level

15

Audit Considerations for Offeror and Offeree

CAPLOCK SECURITY

- Financially stable/viable, experienced, and knowledgeable
- Collusions, misconduct and manipulations
- Number of parties
- Conflicts of interest
- Able to deliver on the promises

16

Audit Considerations for the Contract

CAPLOCK SECURITY

- Accurately represents the promises of the smart contract
- Clear agreement addressing non-operational issues
- Escrow or not
- Security audit
- Speed of transactions
- Cost of transactions

17

Audit Considerations from External

CAPLOCK SECURITY

- Regulators
- Herstatt (settlement) risk
- Platform dependencies
- Scalability
- Privacy

18

Vulnerabilities in Smart Contracts

- 34,200 out of 1 million (3%) smart contracts have some forms of trace vulnerabilities.
  - Suicidal contracts: can be killed by arbitrary addresses [Parity bug ~ $300M]
  - Greedy contracts: can reach a state in which they cannot release ether
  - Prodigal contracts: can be made to release ether to arbitrary addresses [DAO attack ~ $150M]
- Review of Ethereum smart contract indicated bugs per line of code exceeds 100 per 1000 lines, or 2X to 6X the industry average.
- Majority of vulnerabilities are the result of coding errors.

19

Quick Solidity Walkthrough

```
pragma solidity ^0.4.24;

contract Messenger {
    address owner;
    string[] messages;
    uint256 balance;

    constructor() public {
        owner = msg.sender;
    }

    function add(string newMessage) public {
        require(msg.sender == owner);
        messages.push(newMessage);
    }

    function count() view public returns(uint){
        return messages.length;
    }

    function getMessages(uint index) view public returns(string){
        return messages[index];
    }

    function GetBalance() public constant returns(uint256){
        return this.balance;
    }

    function deposit() payable {}
}
```

Messenger

30

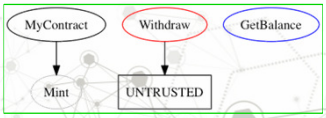
Security Considerations

- Access Control
- Reentrancy
- Integer Over/Underflow Manipulation
- Unchecked Return
- Timestamp Manipulation
- Randomness
- Racing Conditions
- Front Running
- Default Visibility
- Denial of Services

31

Visualization Tools

- Visualize function control flow of a contract and highlights potential security vulnerabilities:
  - Surya
  - Solgraph
  - EVM Lab
  - Ethereum graph debugger



50

Static and Dynamic Analysis Tools

- Use symbolic analysis, taint analysis and control flow checking to detect a variety of security vulnerabilities.
  - Mythril
  - Slither
  - Echidna
  - Oyente
  - Securify
  - SmartCheck
  - Octopus
  - Chaincode Scanner*

* Denotes Hyperledger Fabric

51

Test Coverage & Linters

- Ensure that test evaluate all of the code under test.
- Improve code quality by enforcing rules for style and composition, making code easier to read and review.
  - Solidity Coverage (test coverage)
  - Solcheck
  - Solint
  - Solium
  - Solhint

52

Best Practices for Smart Contracts

- Prepare for failure
- Rollout carefully
- Keep contracts simple
- Stay up to date
- Be aware of blockchain properties
- Choose Simplicity over Complexity

53

Final Words

- Ethereum, Hyperledger Fabric and other complex blockchain programs are new and highly experimental.
- Security is paramount for blockchain technology.
- Smart contracts are only as smart as the developers.
- Transparency, expert reviews, user testing and use of automated security tools are mechanisms to minimize vulnerabilities.
- The effectiveness of the audit will be dependent on the auditor's understanding of the underlying mechanisms of the smart contract and the blockchain platform.

54

CAPLOCK SECURITY

Thank you for your time!

Tuan Phan, CISSP, PMP, CBSP, Security+, SSBB
Partner, Caplock Security LLC
tphan@caplocksecurity.com @ChainOpSec LinkedIn.com/in/tuanphan/
202-780-5455

55