Blockchain and Applications in Information Security

A.J. Bahou, Esq., LLM, MsECE
615-850-8542
AJ.Bahou@wallerlaw.com

InfoSec Nashville
September 2018
Agenda

• Introduction
  – What is Blockchain?
  – Why does it matter?

• Components
  – Cryptography
  – Terms - Blocks, Tokens, Hashes, Immutable

• Blockchain Applications in Information Security
  – Use Cases and Examples for Discussion
  – Prior Hacks
• This is merely an introduction & terminology is used in various ways...(focus on concepts as we begin).

• My apologies in advance, but if I say I can’t answer ....
  – It might be because we have
    o Clients with Patent Applications
    o Clients with Business Models
  – that are not ready for disclosure yet.
What is Blockchain?

- Cryptographic Distributed Ledger
  - A Blockchain is a distributed public database that keeps a permanent record of digital transactions.
  - Promise to consider...
Why does Blockchain matter?

• This technology could change everything...like
  – Electricity
  – Transistor
  – Internet

• No central authority (in theory)
  – Is consensus good enough?
  – Will the consensus always make the ‘right’ decision?
Cryptography & Security Basics

Alice → Charlie → Bob

Eve
Cryptography

- Process of converting ordinary information (plaintext) into encrypted unintelligible text (ciphertext).

- Encryption
  \[ e^k = d^k, \text{ where } 'k' \text{ is the key} \]
PKI

- Public Key Infrastructure

https://en.wikipedia.org/wiki/Public-key_cryptography
PKI

https://en.wikipedia.org/wiki/Public-key_cryptography
PKI

• Public Key Infrastructure

https://en.wikipedia.org/wiki/Public-key_cryptography
PKI

- Advanced Variation – Diffie-Hellman Key Exchange

In the Diffie–Hellman key exchange scheme, each party generates a public/private key pair and distributes the public key. After obtaining an authentic copy of each other's public keys, Alice and Bob can compute a shared secret offline. The shared secret can be used, for instance, as the key for a symmetric cipher.

https://en.wikipedia.org/wiki/Public-key_cryptography
Hashing

- Hashing is a mathematical **algorithm** that maps data of **arbitrary size** to a bit string of a **fixed size** (a hash function) which is designed to also be a one-way function, that is, a function which is **infeasible** to invert.

https://en.wikipedia.org/wiki/Cryptographic_hash_function
Hashing

Tokens

Peer A

Block: # 4
Nonce: 115068
Tx: $ 62.1 from: Rick to: lisa
$ 867.5 from: Captz to: Stras
$ 276.3 from: Victor to: lisa
$ 97.1 from: Rick to: Sam
$ 119.6 from: Captz to: Jan Br
Prev: 0000a9dd50de891b2de8601c6d933c586152c8903
Hash: 0000a9dd50de891b2de8601c6d933c586152

Block: # 5
Nonce: 147675
Tx: $ 14.12 from: Denis to: Edmu
$ 2.76 from: Lord I to: John I
$ 413.7 from: Kathe to: Miss
Prev: 0000a5cceedd53f9078325617d14f0c28903
Hash: 0000285555f5dce83cecd78c5c16d712aa5b1

https://www.youtube.com/watch?v=_160oMzblY8
Creating the Chain

Tokens

Peer A

<table>
<thead>
<tr>
<th>Block</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nonce</td>
<td>116068</td>
</tr>
<tr>
<td>Tx:</td>
<td>$62.1</td>
</tr>
<tr>
<td></td>
<td>$867.1</td>
</tr>
<tr>
<td></td>
<td>$276.1</td>
</tr>
<tr>
<td></td>
<td>$97.1</td>
</tr>
<tr>
<td></td>
<td>$119.1</td>
</tr>
<tr>
<td>Prev:</td>
<td>0000a9dd50de891b2de8601c6d933c586152</td>
</tr>
<tr>
<td>Hash:</td>
<td>0000a5ccee53f9078325617d14f0c28903</td>
</tr>
</tbody>
</table>

Block: # 5

Nonce: 147675

Tx: $14.12 From: Denis → Edmu
$2,760 From: Lordi → Johnl
$413.7 From: Kathen → Misslan

Prev: 0000a5ccee53f9078325617d14f0c28903
Hash: 00002855f5cde83ccccd78c516d712a5b1

https://www.youtube.com/watch?v=_160oMzblY8
Blockchain

- Satoshi Nakamoto Whitepaper, Oct. 31, 2008
Example

Simplified Bitcoin Block Chain

Terms

• Blocks – files that contain permanently recorded transaction data
• Hashes – algorithm that maps data to a fixed size
• Tokens – can represent any fungible tradable good
• Nonce – an arbitrary number that may only be used once
Terms

• Immutable – unchanging over time or unable to change
• Distributed – copied on various nodes throughout the network
• Ledger – collection of transactions
• Nodes – computer connected to the network that performs the task of validating and relaying transactions
Applications of Blockchain in Information Security
Growth of Blockchain in Cyber Security

• Cyber security is one of the most important use-cases for blockchain.

• A 2017 IBM Study of 3,000 global C-suite executives found that 33 percent of organizations are considering or already using blockchain for
  - security against fraud and
  - protecting against cybercrime being the main reason organizations are interested.

https://medium.com/polyswarm/5-important-use-cases-for-blockchain-92ae2a35484d
Blockchain Use Cases in Information Security

- Identity and Access Management
- Data Management - Improved Confidentiality and Data Integrity
- Securing Edge Devices with Authentication
- Secure Private Messaging
- Next Generation PKI
- Safer DNS
- Reduce DDos Attacks
Identity Management Using Blockchain

(12) United States Patent
Muftic

(10) Patent No.: US 9,635,000 B1
(45) Date of Patent: Apr. 25, 2017

(54) BLOCKCHAIN IDENTITY MANAGEMENT SYSTEM BASED ON PUBLIC IDENTITIES LEDGER

(71) Applicant: Sead Muftic, Rockville, MD (US)
(72) Inventor: Sead Muftic, Rockville, MD (US)
( * ) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: 15/163,922
(22) Filed: May 25, 2016

Primary Examiner — Chau Le
(74) Attorney, Agent, or Firm — Morris, Manning & Martin LLP; Daniel E. Sineway, Esq.

(57) ABSTRACT
The invention describes an identity management system (IDMS) based on the concept of peer-to-peer protocols and the public identities ledger. The system manages digital identities, which are digital objects that contain attributes used for the identification of persons and other entities in an IT system and for making identity claims. The identity objects are encoded and cryptographically encapsulated. Identity management protocols include the creation of iden-
Identity Management

Sovrin™: A Protocol and Token for Self-Sovereign Identity and Decentralized Trust
Data Management

• Government Agencies (Public information with integrity)
  – birth and death dates
  – marital status
  – business licensing
  – property transfers, or
  – criminal activity.

Data Management

• Example nation of Estonia
  – Keyless Signature Infrastructure (KSI) to safeguard all public-sector data
  – KSI creates hash values
  – Hash values can be used to identify records
  – But hash values cannot be used to reconstruct the information in the file itself
  – KSI allows government officials to monitor changes within various databases
  – Electronic health records of all Estonian citizens are managed using KSI technology

• Delaware – Smart Incorporation on the Blockchain
Data Management

Individual blockchain ledgers could let public agencies deliver networked services and citizens control their own data.

**Public agencies**
Public agencies could easily get the information they need to deliver services to citizens—insofar as they have the required permissions to access the data.

**Companies**
The private sector could be included in selected parts of the services blockchain.

**Citizens**
Citizens could give public agencies read or write access to their data, case by case.

**Individual blockchain ledgers**
- Secured by public/private-key cryptography
- Civil-registry data
- Tax/social-security data
- Agency-interaction records

**Rule**
Citizens could set up contracts with agencies, for their own convenience.

**Smart contracts**
Defines those situations where information can be shared.

**Regulation**
Once predefined situations kick in, agencies could automatically gain permission to access citizens’ data.

McKinsey&Company
Securing Edge Devices with Blockchain

- IoT devices host the ledger and is capable of participating in blockchain transactions, including mining.

- Each device is provisioned with a private key (Cloud Security Alliance, Using Blockchain to Secure the IoT, 2018)

*Each IoT node acts as a blockchain transaction node.*
Securing Edge Devices with Blockchain

• Cloud-Enabled IoT Blockchain Network (BC, M2M, API)
  – Whitelist devices
  – Two-way authentication
Securing Edge Devices with Blockchain

- Smart Cities, Trusted Communications
Secure Private Messaging

- Status Ethereum-based messenger app (https://status.im)
  - Uses Ethereum node on smartphone, such as a cryptocurrency wallet as an interface for decentralized applications
  - Whisper Protocol – multicast, peer-to-peer, end-to-end encrypted gossip protocol
Next Generation PKI - Estonian Government Example

• Since 2013, Estonian Government have used Keyless Signature Infrastructure (KSI) pairs of cryptographic ‘hash functions’ with a distributed ledger to
  − Guarantee a record of the state of any component within the network
  − Guarantee data stores

• Citizens use ID cards to:
  − Order prescriptions
  − Vote
  − Bank online
  − Review kid’s school records
  − Apply for state benefits
  − File tax returns
  − Upload their will
  − Serve in armed forces, etc.
Securing Cryptocurrency

Hacker-Powered Security For Blockchain + Cryptocurrency

More than 40 of the largest blockchain and cryptocurrency organizations trust HackerOne to secure their platforms and protect their customers.

LET'S TALK
Securing Cryptocurrency - HackerOne

**Powerful Platform**
- Quickly create your program and begin receiving vulnerability reports
- Easily manage reports and communicate with hackers
- Monitor your success and pay bounties for valid reports

**Flexible + Scalable**
- Adjust your scope at any time and scale your program with ease
- Run your program yourself or we can fully manage it for you
- Test in small increments, or continuously with an ongoing program

**Security Expertise**
- Invite top security researchers to test your assets
- Identify and filter based on skills and experience
- Test mobile wallets, digital exchanges, smart contracts, and more
Securing Cryptocurrency – HackerOne Bug Bounty

Policy

Introduction

Coinbase recognizes the importance and value of security researchers’ efforts in helping keep our community safe. We encourage responsible disclosure of security vulnerabilities via our bug bounty program (“Bug Bounty Program”) described on this page.

Note: This program is for the disclosure of software security vulnerabilities only. If you believe your Coinbase account has been compromised, change your password and immediately contact support via our support form.

The Bug Bounty Program directly serves Coinbase’s mission by helping us be the most trusted way to use digital currency. In that spirit, the scope and philosophy of the program aim to safeguard two highest priority assets (“Sensitive Data”):

- Digital and fiat currency balances
- Customer information

The Bug Bounty Program scope covers all software vulnerabilities in services provided by Coinbase.

A valid report is any in-scope report that clearly demonstrates a software vulnerability that harms Coinbase or Coinbase customers. A report must be a valid, in scope report in order to qualify for a bounty. Coinbase will determine in its sole discretion whether a report is eligible for a reward and the amount of the award.
Securing Cryptocurrency – HackerOne Bug Bounty

In order to provide general guidelines to researchers regarding the payouts that can be expected for a given report, Coinbase uses the severity of a report to place the report into one of the following tiers.

<table>
<thead>
<tr>
<th>Vulnerability Tier</th>
<th>Reward</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td>$50,000</td>
</tr>
<tr>
<td>High</td>
<td>$15,000</td>
</tr>
<tr>
<td>Medium</td>
<td>$2,000</td>
</tr>
<tr>
<td>Low</td>
<td>$200</td>
</tr>
</tbody>
</table>

The payouts listed next to each tier are minimum bounties for the tier. Bonuses in excess of the tier minimum can be awarded based on the severity of the vulnerability or creativity of the exploitation. Researchers are also more likely to earn a larger reward for exceptionally clear and high-quality reports.

Previous bounty amounts are not considered precedent for future bounty amounts. Software is constantly changing and therefore the given security impact of the exact same vulnerability at different times in the development timeline can have drastically different security impacts.
How do we—as InfoSec professionals—need to protect information on the Blockchain?
Prior Hacks Related to Blockchain

• Mt. Gox
  − June 2011 - $8 million stolen (admin pw)
  − Feb. 2014 - $460 million stolen (attack on the hot wallet)

• Issues
  − No version control
    o Bug fixes delayed
    o Untested code deployed

https://www.rsaconference.com/writable/presentations/file_upload/fon4-t11_hacking_blockchain.pdf
Hacks Related to Blockchain

• The DAO (Distributed Autonomous Organization)
  – $50 million hack
  – DAO smart contract flaw known since May 2016
  – Hacker used flaw that allowed splits inside splits, moving Ether repeatedly without checking the ‘balance’
  – Hard fork resulted

https://www.rsaconference.com/writable/presentations/file_upload/fon4-t11_hacking_blockchain.pdf
https://www.deepdotweb.com/2016/10/06/cryptocurrency-hacks-biggest-heists-blockchain-history/
Compare to Traditional Banking

• Deposit made, balance updated, but can’t always use funds.

What is comparison with exchanging cryptocurrency?
  - No FDIC
## Industries to Consider

<table>
<thead>
<tr>
<th>Industry</th>
<th>Industry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Banking &amp; Finance</td>
<td>Cybersecurity</td>
</tr>
<tr>
<td>Supply Chain Management</td>
<td>Government</td>
</tr>
<tr>
<td>Networking and IoT</td>
<td>Insurance</td>
</tr>
<tr>
<td>Voting</td>
<td>Charity</td>
</tr>
<tr>
<td>Health Care</td>
<td>Energy Management</td>
</tr>
<tr>
<td>Online Music</td>
<td>Real Estate</td>
</tr>
<tr>
<td>Crowd Funding</td>
<td>Forecasting</td>
</tr>
</tbody>
</table>
Resources

• Webpages
  – CoinDesk.com
  – Bitcoin.com
  – Blockchain.info
  – Insight.Bitpay.com
  – Ethereum.org/
https://blockchain.info/tree/155502176
Conclusions

• Blockchain will disrupt many industries, including cybersecurity.

• Potential Applications in Information Security may allow the use of Blockchains to manage digital identities, protect large amounts of data, and secure edge devices.

• Cybersecurity jobs are safe – just be ready to protect the Blockchain.
Questions?

A.J. Bahou, Esq.
615-850-8542
AJ.Bahou@wallerlaw.com