Blockchain and Bitcoin:
Impact on Insurance Industry
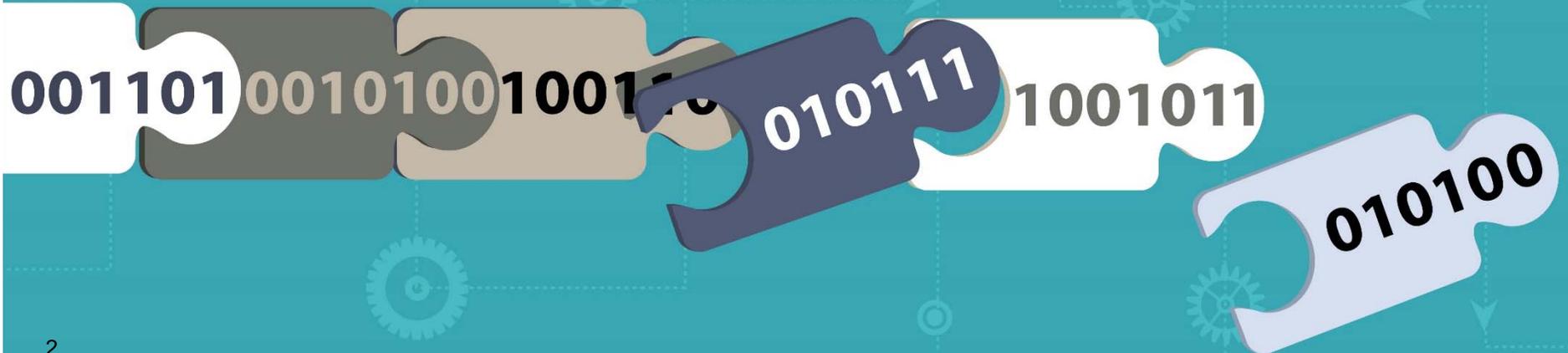
ACLI Financial & Investment Roundtable
Sea Island, Georgia

Edmund J. Zaharewicz
Shareholder
Carlton Fields Jorden Burt, P.A.

March 19, 2018

Introduction

- What is Blockchain?
- What is Bitcoin?
- The Promise of Blockchain
- Industry Focus

- Proofs of Concept
- Challenges
- Legal Issues

What is Blockchain?

Blockchain is:

A. Technology that enables parties to transact electronically without a middleman based on a common digital history

B. The next big thing, of transformational and potentially disruptive value

C. Just another technology, of incremental value

D. "A riddle, wrapped in a mystery inside an enigma"

E. All of the above

How Does Blockchain Work?

- A blockchain is a series of linked data blocks

- A block consists of a "hash" of the previous block and a "payload"

- The hash is used to verify the blockchain and make it hard to tamper with

- If a block is altered, its hash and those of all subsequent blocks must be recalculated or the altered block and all subsequent blocks will be considered invalid

- The payload is anything that can be digitally represented, e.g., money, legal title, medical records, "smart contracts", etc.

A Simple Blockchain
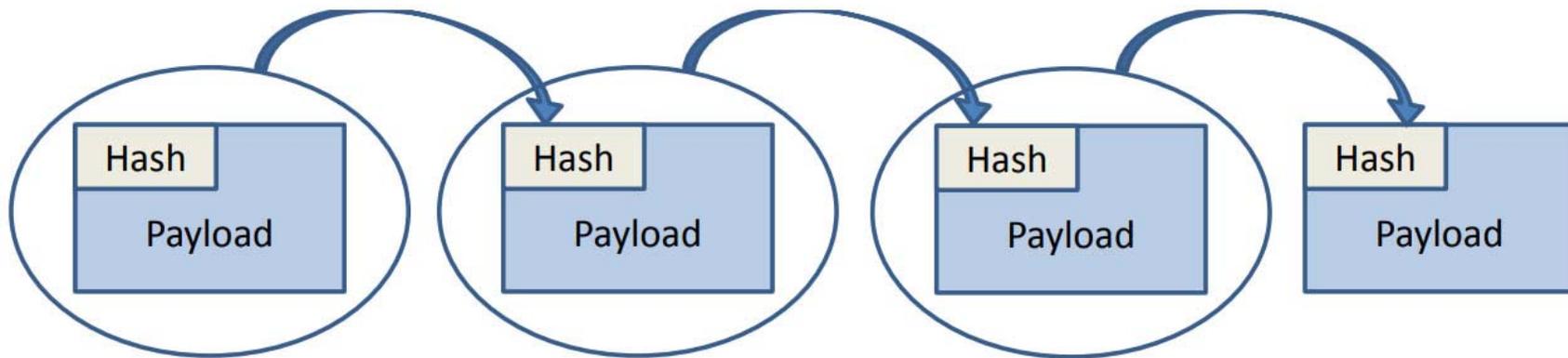
Source: Oleg Mazonka

Data → Hash Algorithm → Hash

"The hash for this string of text is?"

a642b9e7efd8b4655760444db0ce90cbea75e002c57db61a43975bebd8a85f47

"The hash for this string of text is:"

687de15baa0c697b531cbe511a6d3e12be5c814f7f64bbeb15d24d54582088f0

How Does Blockchain Work?

- Blockchain technology is a particular organization of "blockchains"
  1. A global blockchain
     - Records when a transaction occurred, and
  2. One or more internal blockchains
     - Records the details of transactions
- Each block on the global blockchain contains a collection (the block's payload) of transactions at a point in time

A Simple Global Blockchain

Source: Oleg Mazonka
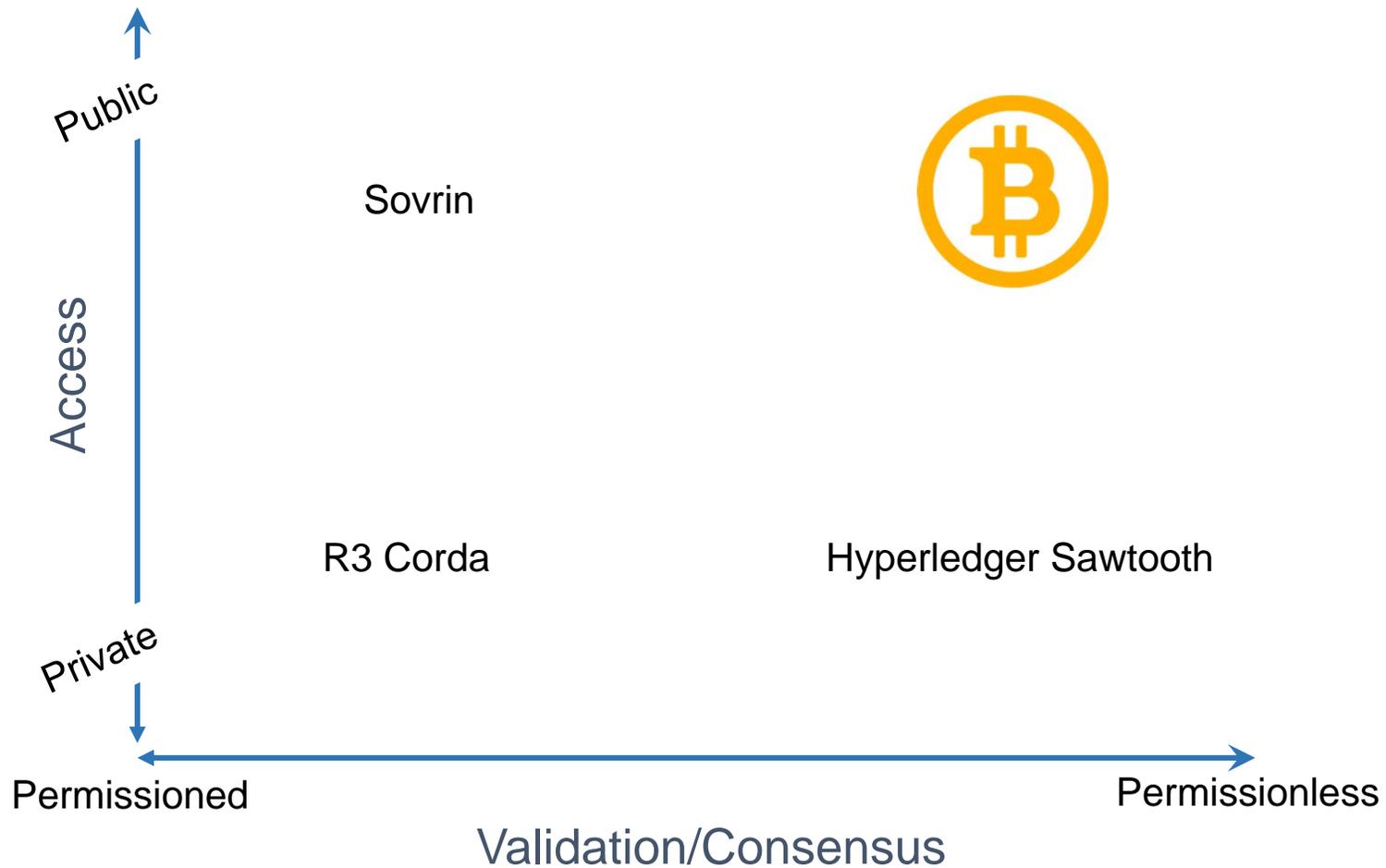
8
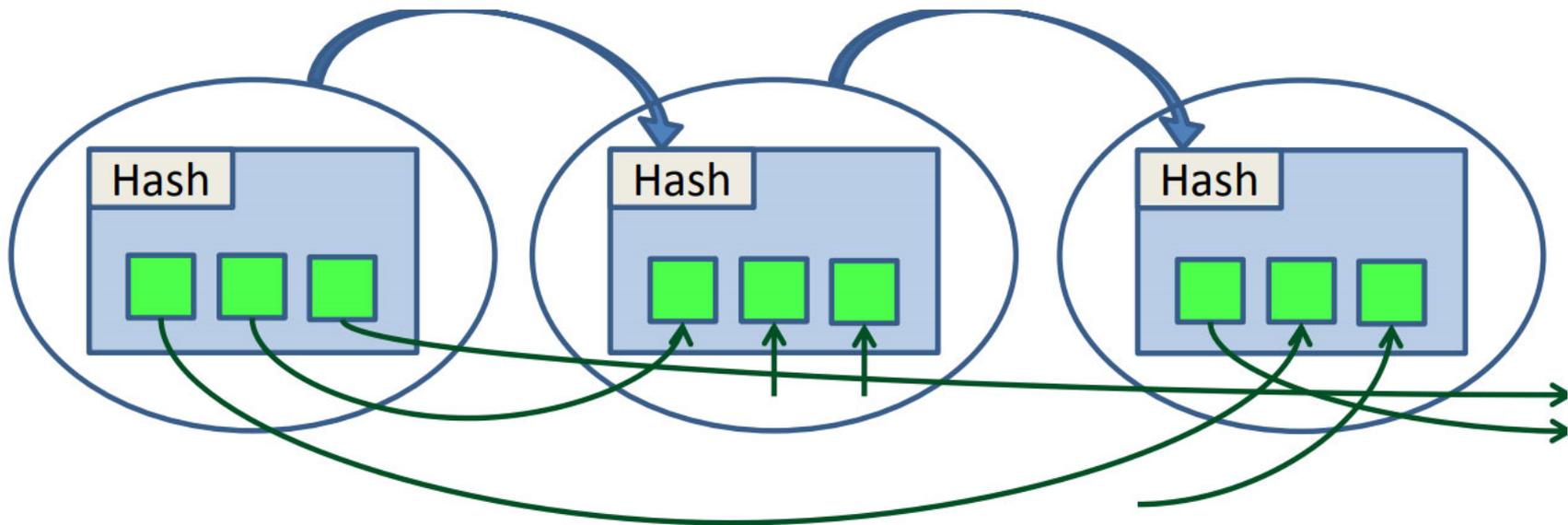
How Does Blockchain Work?

At the transactional level:

- PKC is used (though not always) to establish and convey ownership

- A block is identified by a public key and owned by the holder of the associated private key

- Only a block's owner can transfer its "value" to a new (the next) block by placing the new owner's public key in the new block and digitally signing it

Other features:

- Every node on the network keeps a copy of the global blockchain

- All blocks and transactions are broadcast over the network

- Only blocks and transactions that abide by "the rules" (i.e., a "consensus" protocol) are added to the global blockchain

- Blocks or transactions that attempt to "rewrite" history are ignored

Blockchain/Distributed Ledger Types

Public

Access

Sovrin

R3 Corda   Hyperledger Sawtooth

Private

Permissioned   Permissionless

Validation/Consensus

What is Bitcoin?

- Bitcoin is a virtual currency or cryptocurrency
- It is "the first decentralized, censor-proof, portable, secure, durable, and scarce digital asset"
- It is regarded for using blockchain technology to solve the "double speeding" problem
- Bitcoin's "success" has popularized blockchain and its potential for a wide variety of applications

Bitcoin: A Brief History

2008 Bitcoin has it origins in a 2008 whitepaper by "Satoshi Nakamoto"

2009 Jan. – Bitcoin code released; network born

May – Two pizzas bought for 10k BTC ($.01/BTC)

2010 Satoshi no longer involved; others take lead

2011+ More merchants accept bitcoin

Bitcoin weathers many ups and downs

2017 Bitcoin soars from ~$1k to $20k

2018 Feb. – Bitcoin down by over 60% from 2017 high

How Does Bitcoin Work?

- Bitcoin was a reaction to the ability of governments to devalue their currencies
- Like gold, bitcoins are scarce and require effort to "mine"
  - Total bitcoins is fixed at 21m
  - ~16.8m bitcoins mined so far
  - Rate of mined bitcoins decreases over time

- Bitcoin's consensus protocol operates by
  - Making it computationally difficult to add new blocks to the global blockchain (proof-of-work)
  - Rewarding "miners" for adding new blocks with bitcoins and fees
  - Taking the longest branch when "branching" occurs
- Bitcoin database is "computationally impractical for an attacker to change if honest nodes control a majority of CPU power"
- In short: Easy to verify, hard to change

Blockchain Attributes

Blockchain has a number of useful attributes

- Transactions are decentralized (peer to peer), fault tolerant, secure, transparent, pseudonymous (quasi-anonymous), tamperproof and verifiable

- No central trusted authority is needed

- Participants agree on a single history of events

- Supports "smart contracts" (Ethereum)

The Promise of Blockchain

Some see blockchain potentially as transformational as the Internet by enabling an environment for decentralized applications (DApps)

Decentralized Applications

Smart Contracts

Blockchain

Internet

The Promise of Blockchain

- Views vary on blockchain's potential impact on the insurance industry
    - From disruptive / transformational
    - To "merely" enabling / incremental
- Some see the possibility of new and innovative products
    - Peer to peer insurance
    - Parametric insurance
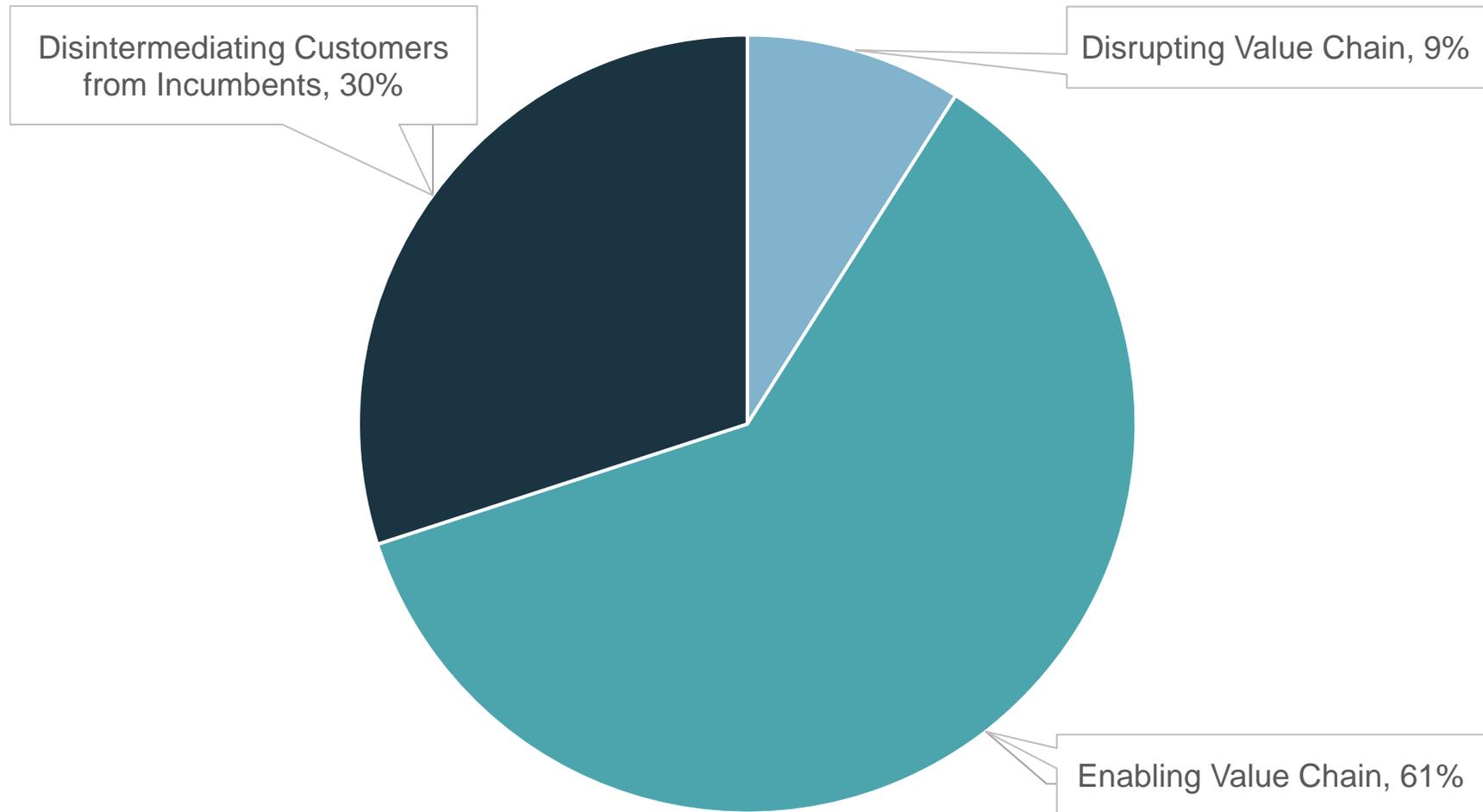   - Micro-insurance

The Promise of Blockchain

Others see the possibility of improved operations and efficiencies across entire insurance value chain

- Products and distribution
- Underwriting / risk management
- Policyholder acquisition / servicing / administration

- Claims management
- Investments, payments and accounting
- Regulatory and Compliance

Industry Focus

- InsurTech funding overall increased 36% year over year to $2.3b in 2017

- Most InsurTech funding to date has not focused on blockchain, however

- One estimate puts blockchain funding overall in the last 14 months at
  - $1.3b   Traditional venture capital
  - $4.5b   Initial coin offerings (ICOs)

InsurTechs by Focus in Value Chain

Disintermediating Customers from Incumbents, 30%

Disrupting Value Chain, 9%

Enabling Value Chain, 61%

Source: CB Insight; McKinsey & Company research

Industry Focus

- Insurance blockchain initiatives
  - Blockchain Insurance Industry Initiative (B3i)
  - The Institute's RiskBlock Alliance
  - LIMRA's Blockchain Advisory Council
- Some activity at carrier and sponsored accelerators / venture arms
- Interest at the NAIC
  - Innovation and Technology (EX) Task Force
  - Center of Insurance Policy and Research (CIPR)

Proofs of Concept

- B3i
  - Catastrophe insurance contracts
- RiskBlock Alliance / Nationwide
  - Proof of insurance for insurers, insureds, and law enforcement
- Allianz
  - Catastrophe bond trading
  - Cross borders captive insurance policies
- AXA
  - Fizzy, flight delay insurance
- AIG, IBM, Standard Chartered
  - Converted multinational insurance policies into a smart contract

Proofs of Concept

- Ⓑ **Microsoft, EY, Willis Towers, Maersk**
  - Ⓑ Supply chain solutions enabling marine insurance
- Ⓑ **Startup StarHub, Prudential**
  - Ⓑ Small to medium-sized business trade platform enabling commercial insurance options
- Ⓑ **Start up Stratumn, Deloitte, and 14 Euro Insurers**
  - Ⓑ Industry solution for French regulatory notice requirements

Challenges

- Scalability
- Computing power / Energy consumption
- Governance
- Key Management
- Ability to Adapt
- Interoperability
- Privacy
- Regulatory uncertainty

Legal Issues

- Jurisdictional issues
- Liability
- Legality of blockchain records
- Enforceability of smart contracts
- Regulated products
- Cybersecurity and privacy
- Intellectual property

State Activities

- Various state virtual currency provisions
  - Uniform Regulation of Virtual Currency Businesses Act
- Some blockchain specific provisions
  - Delaware Blockchain Initiative; legality of records, stock ledgers and smart securities; T+0 trade settlement
  - Illinois Blockchain Initiative
  - NV: legality of records; prohibition on local taxes and other meddling
  - AZ: legality of records and smart contracts
  - VT: legality of records

Regulatory Approaches

- Building Capabilities – Focus on in-house expertise, education, coordination, and issue spotting
  - SEC DLT Working Group
- Facilitation – Focus on external education and outreach
  - SEC Transfer Agent Concept Release
  - LabCFTC
  - Regulatory sandboxes
  - AIA's proposed NAIC Model Insurance Innovation Regulatory Variance or Waiver Act
- Enforcement
  - SEC Enforcement Division Cyber Unit
  - SEC crackdown on ICOs and retail cyber funds

References

- Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System, 2008
- Oleg Mazonka, "Blockchain: Simple Explanation," 2016
- Sarah Meiklejohn, "Top Ten Ostacles along Distributed Ledgers' Path to Adoption," 2017
- Illinois Blockchain and Distributed Ledger Task Force, "Final Report to the General Assembly," 2018
- Willis Tower Watson, "Quarterly InsurTech Briefing Q4," 2017
- CB Insight, "What is Blockchain Technology"