# Andrés Araya Falcone

*Gerente de Tecnologia*
*Bolsa de Comercio de Santiago,*
*Chile*

**Rajiv Chodhari**
*Vice President, Financial Markets & Wealth Management IBM, Estados Unidos*

# BLOCKCHAIN

FIAB 2017 – Santa Cruz, Bolivia

Andres Araya Falcone |CIO – Bolsa de Santiago | @andresarayaFA

Rajiv Chodhari | Vice President Financial Markets – IBM | Chodhari@us.ibm.com

## Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

**Abstract.** A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

… the thing that's driving bitcoin at the moment, like other examples of bubbles, is a story … And it's the quality of the story that's attracting all this interest, and it's not necessarily sustainable.
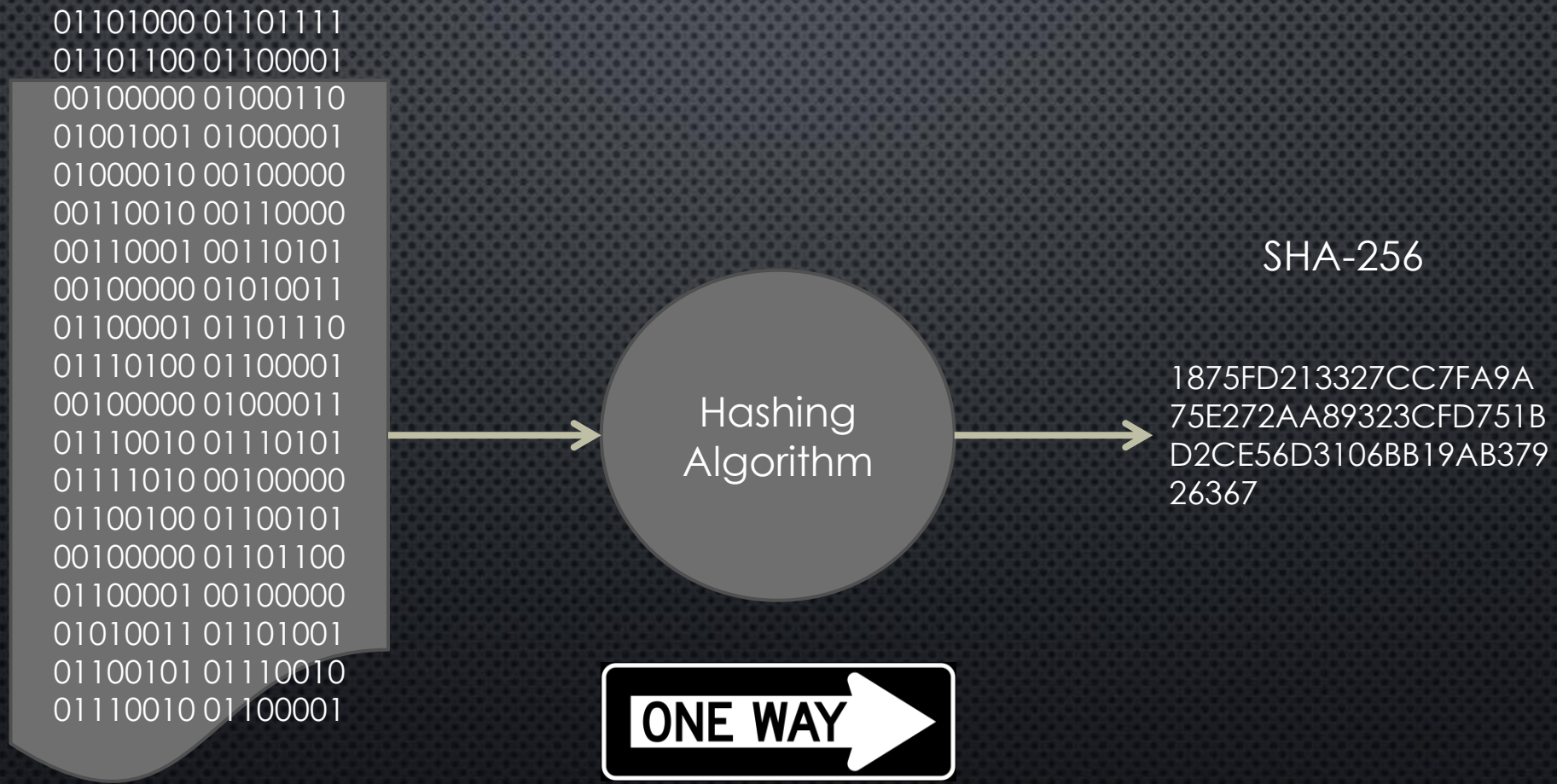
*Robert J. Shiller*
Economy Nobel 2013
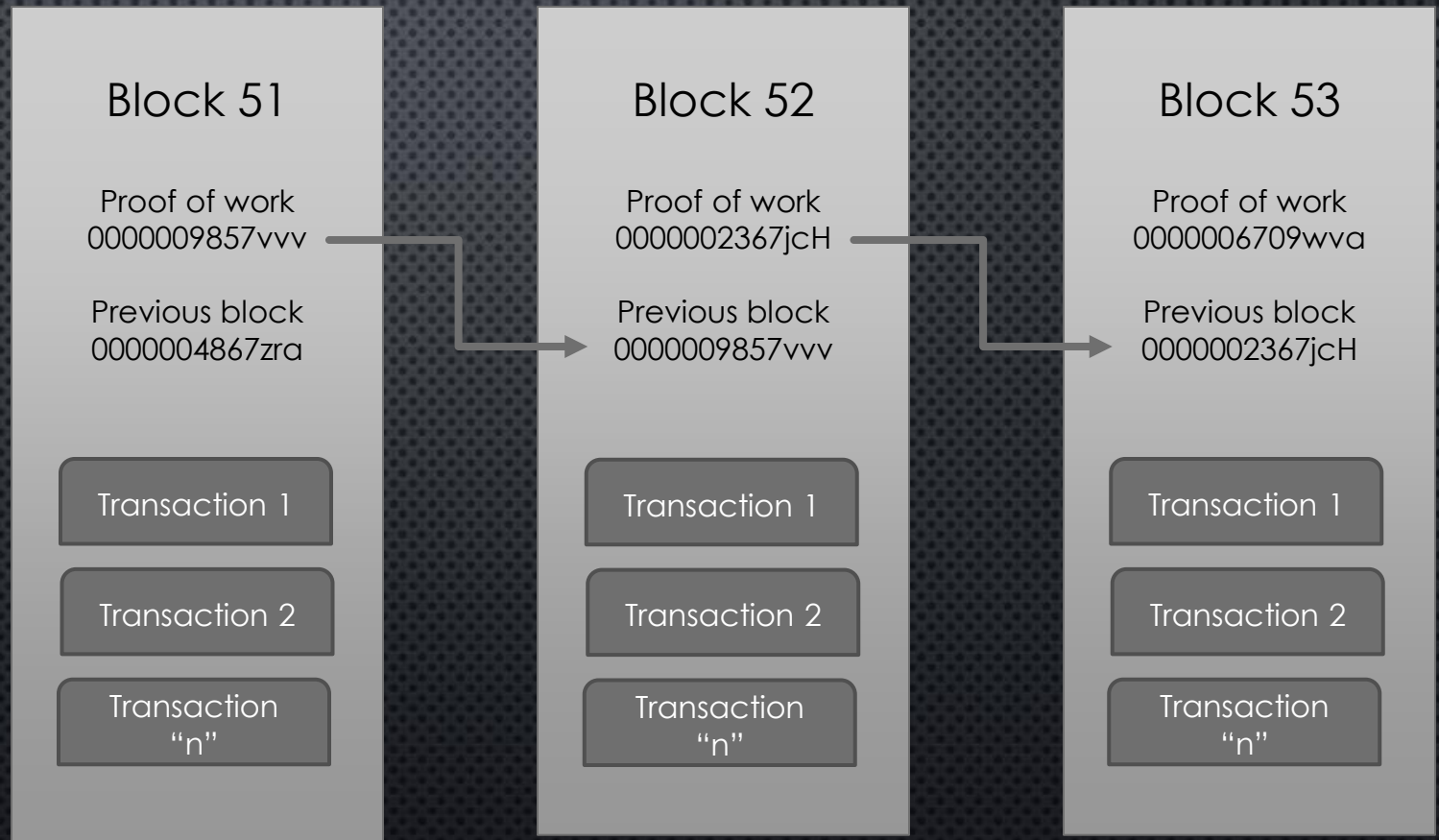
# The Byzantine Generals Problem

# How Blockchain transaction work

01101000 01101111
01101100 01100001
00100000 01000110
01001001 01000001
01000010 00100000
00110010 00110000
00110001 00110101
00100000 01010011
01100001 01101110
01110100 01100001
00100000 01000011
01110010 01110101
01111010 00100000
01100100 01100101
00100000 01101100
01100001 00100000
01010011 01101001
01100101 01110010
01110010 01100001

Hashing
Algorithm

ONE WAY

SHA-256

1875FD213327CC7FA9A
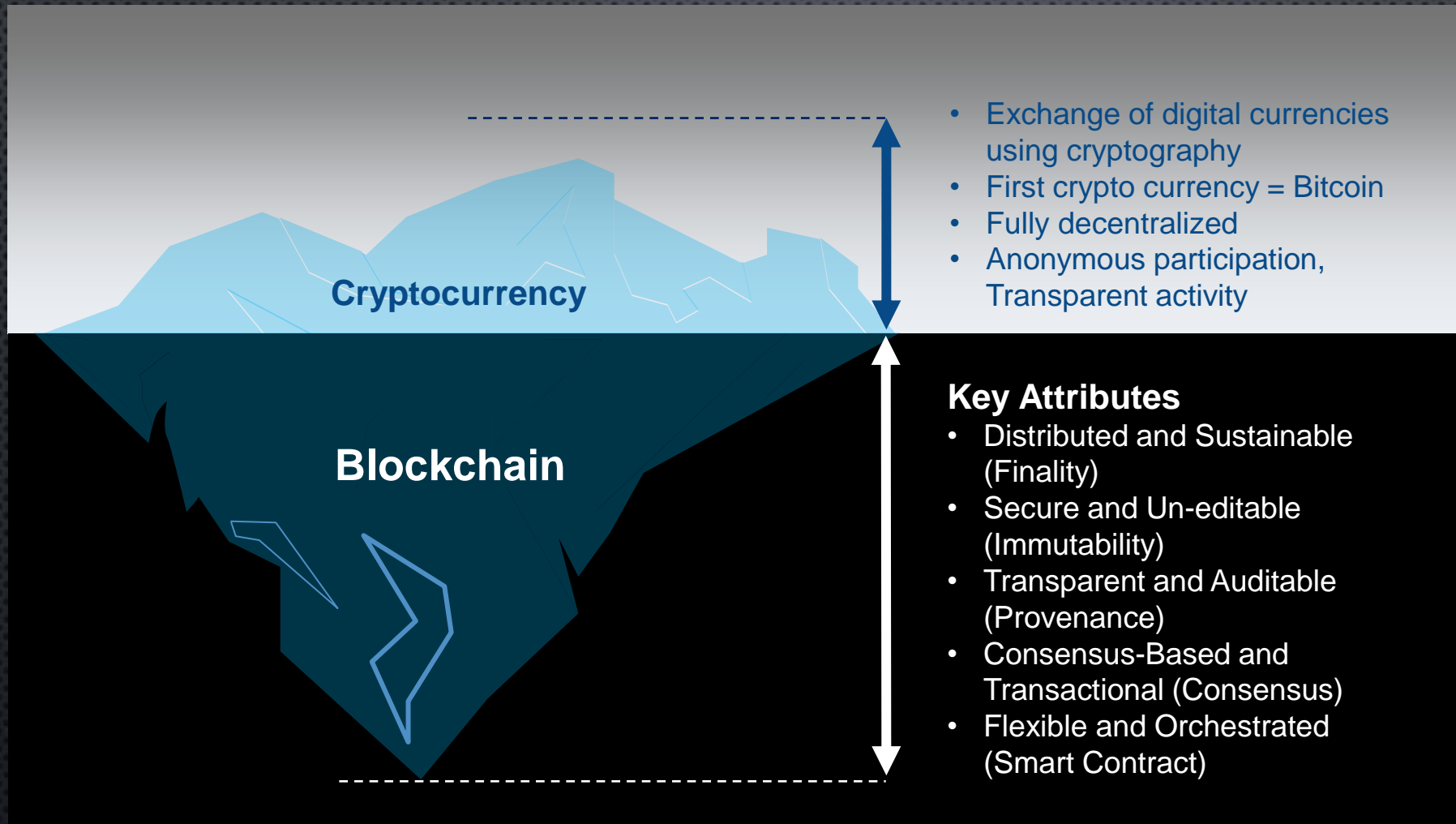75E272AA89323CFD751B
D2CE56D3106BB19AB379
26367

# How Blockchain transaction work

Blockchains solve two major challenges for digital transactions, controlling the information and avoiding duplication, at once.

### Block 51

Proof of work
0000009857vvv

Previous block
0000004867zra

Transaction 1

Transaction 2

Transaction "n"

### Block 52

Proof of work
0000002367jcH

Previous block
0000009857vvv

Transaction 1

Transaction 2

Transaction "n"

### Block 53

Proof of work
0000006709wva

Previous block
0000002367jcH

Transaction 1

Transaction 2

Transaction "n"

# Cryptocurrency vs. Blockchain

**Cryptocurrency**

- Exchange of digital currencies using cryptography
- First crypto currency = Bitcoin
- Fully decentralized
- Anonymous participation, Transparent activity

**Blockchain**

**Key Attributes**
- Distributed and Sustainable (Finality)
- Secure and Un-editable (Immutability)
- Transparent and Auditable (Provenance)
- Consensus-Based and Transactional (Consensus)
- Flexible and Orchestrated (Smart Contract)

*However, some key attributes are missing for Blockchain to be business-ready*

# "Business Ready" Blockchain

## Shared Ledger

Append-only distributed system of record shared across business network

## Smart Contracts

Business terms embedded in transaction database & executed with transactions

## Privacy

Ensuring appropriate visibility; transactions are secure, authenticated & verifiable

## Trust

All parties agree to network transactions after verifying data updates from business calculations

# Hyperledger Fabric v1.0 Released



159 engineers from 28 organizations contributed to project to advance open blockchain products and services

Key Features

- Channels for sharing confidential information
- Ordering Service delivers transactions consistently to peers in the network
- Endorsement policies for transactions
- CouchDB world state supports wide range of queries
- Bring-your-own Membership Service Provider (MSP)

# Securities Lending Repository Blockchain

# Network participant

**Stock Exchange**

NETWORK ROLE: FOUNDER OF THE SECURITIES LENDING BLOCKCHAIN

FUNCTIONAL ROLE: FACILITATES TRADES, ENSURES REGULATIONS ARE FOLLOWED, REQUESTS COLLATERAL

**Regulator**

Network role: Participant on the network to review trades

Functional role: Audits market participants to make sure regulations are abided by

**Brokerage House**

Network role: Active participant that plugs into the network

Functional role: Represents an client in short sale (buyer or seller), facilitates trades, collects fees
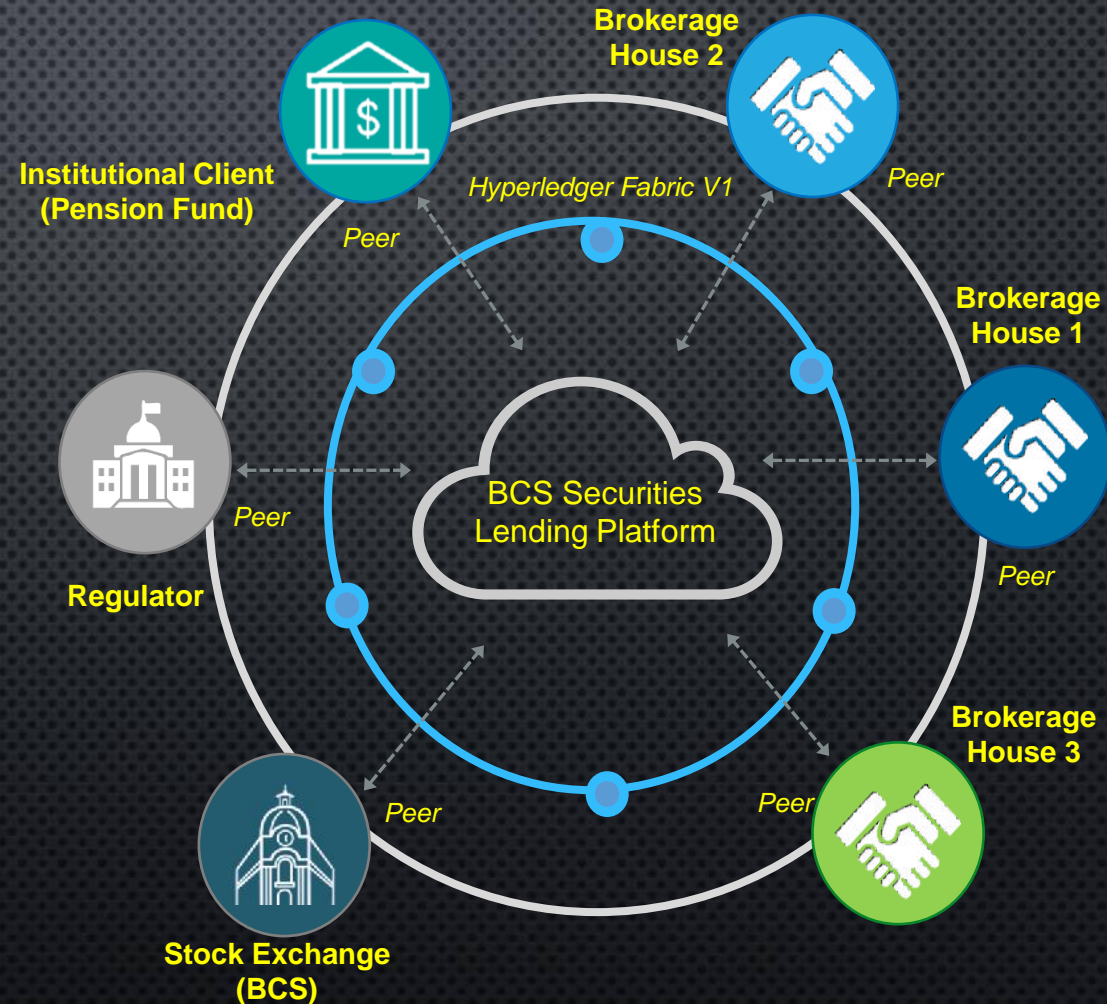
**Institutional Client**

Network role: Participant on the network to view their trades across Brokerage House

Functional role: Participates in short sales (borrower or lender)

# What will the BCS Blockchain network look like?

High-level network overview:

1. BCS is the founder of the network and also acts as a Peer.
2. Each major participant is a separate node (or "Peer") on the network.
3. Participants include Stock Exchange, Brokerage House, and Regulator.
4. Shared distributed ledger of securities lending and short sale information.
5. Peers validate information distributed on the shared ledger.
6. All the participants in the network communicate via channels.
7. Channels ensure data privacy among relevant participants for a given transaction.

Brokerage House 2

Institutional Client (Pension Fund)

*Hyperledger Fabric V1*

*Peer*

*Peer*

Brokerage House 1

Regulator

*Peer*

BCS Securities Lending Platform

*Peer*

*Peer*

*Peer*

Brokerage House 3

Stock Exchange (BCS)

# Blockchain benefits

**Saves time**

Transaction time from days to near instantaneous

**Removes cost**

Overheads and cost intermediaries

**Reduces risk**

Tampering, fraud & cyber crime

**Increases trust**

Through shared processes and recordkeeping

# Roadmap

**① Launch Securities Lending Blockchain**

**② Brokerage Houses adopt nodes**

**③ Expand Usage**

- Start with equities, then fixed income
- All peers are on the common infrastructure
- While the network is shared, the data is segregated by participant
- Data is accessible from the web interface
- Regulators can participate in the network

- Can create their own node and join
- Create own applications and automate their internal processes
- Optionally, Regulators can own a node

- Institutional Clients participate in network (also can own a node)
  - See their own data across participating Brokerage Houses
  - Create their own applications / analytics
- Consortium led by BCS to expand the network beyond Securities Lending
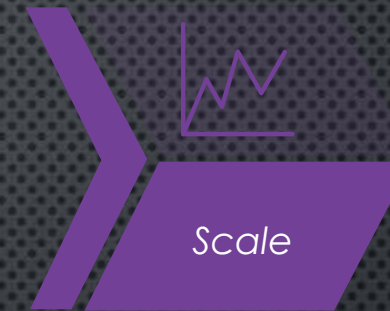
# Engagement model for successful network

## Let's Talk

1. Discuss Blockchain technology
2. Explore customer business model
3. Show Blockchain Application demo

## Blockchain Hands-on

1. Understand Blockchain concepts & elements (e.g. IBM Garage)
2. Hands on with Blockchain
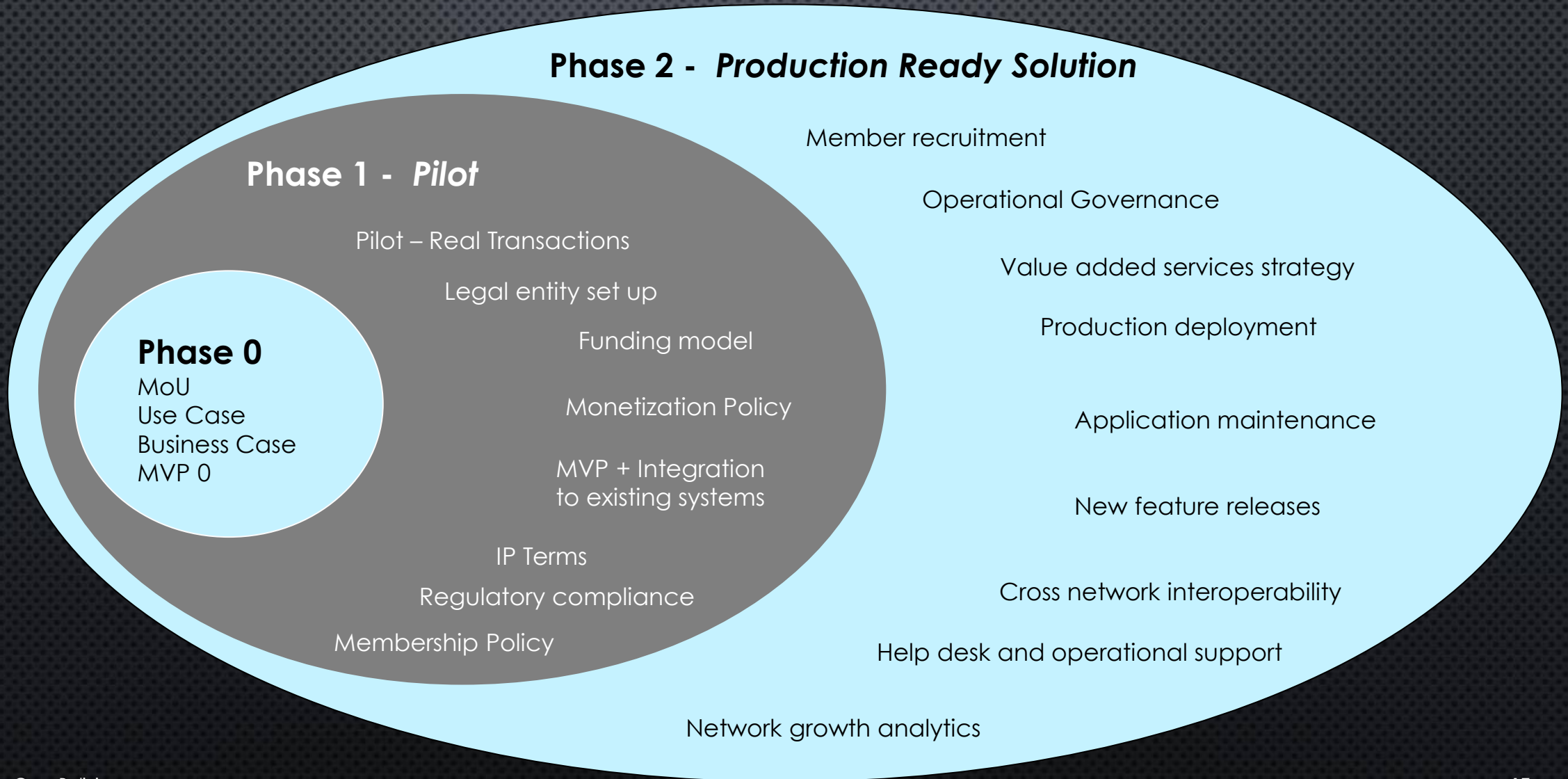3. Standard demo customization

## First Project

1. IBM Design Thinking workshop to define business challenge
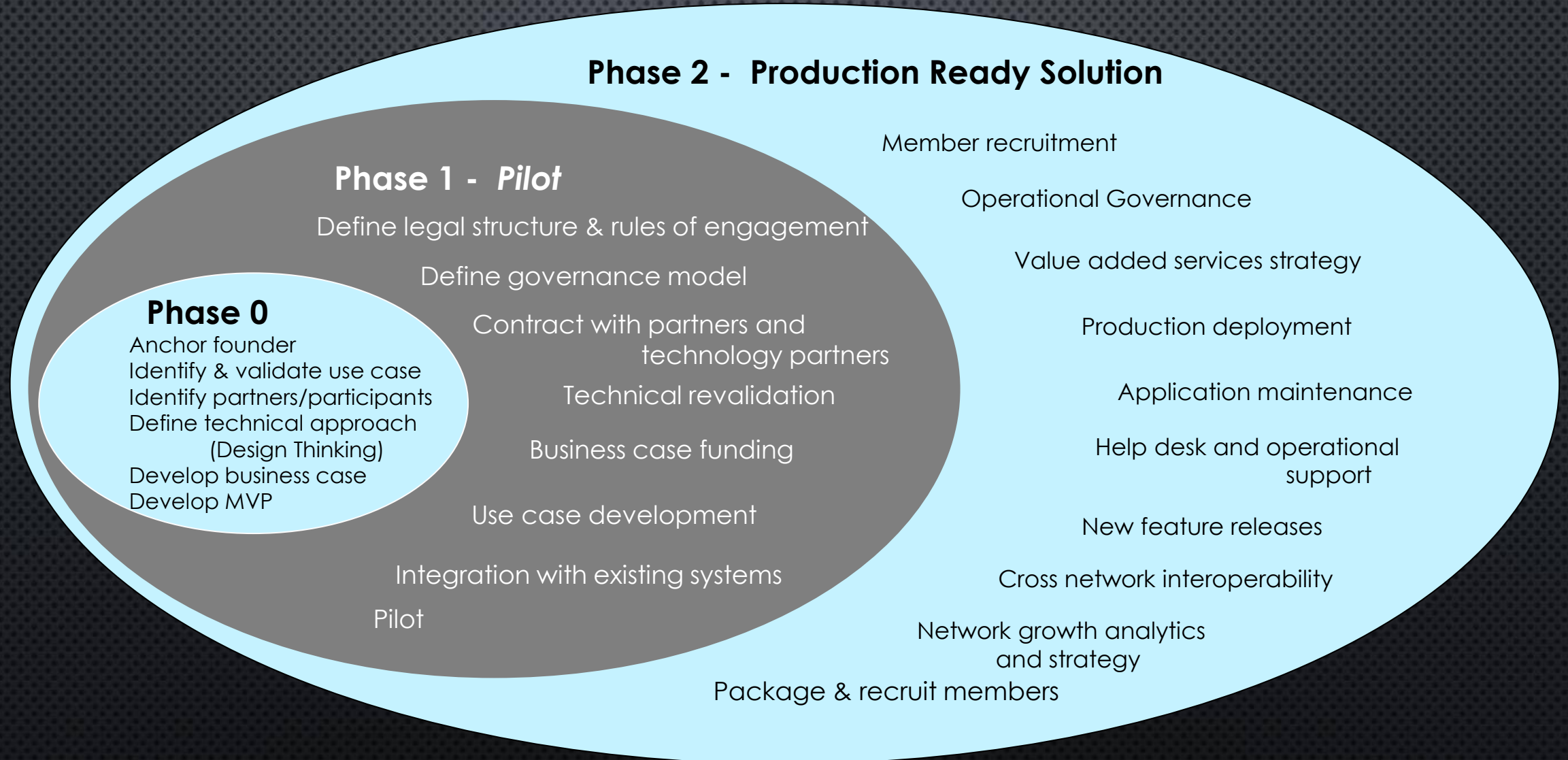2. Agile iterations incrementally build project functionality
3. Enterprise integration

## Scale

1. Scale up pilot by adding network members
2. Expand with value added services
3. Business Process Re-engineering
4. Systems Integration

## Start small, grow quickly

# 3 phases of "Go to Market" for a consortium

**Phase 2 -** *Production Ready Solution*

**Phase 1 -** *Pilot*

Member recruitment

Operational Governance

Pilot – Real Transactions

Value added services strategy

Legal entity set up

Production deployment

Funding model

**Phase 0**
MoU
Use Case
Business Case
MVP 0

Monetization Policy

Application maintenance

MVP + Integration
to existing systems

New feature releases

IP Terms

Regulatory compliance

Cross network interoperability

Membership Policy

Help desk and operational support

Network growth analytics

# 3 phases of "Go to Market" for a founder journey

**Phase 2 - Production Ready Solution**

**Phase 1 - *Pilot***

**Phase 0**
Anchor founder
Identify & validate use case
Identify partners/participants
Define technical approach
    (Design Thinking)
Develop business case
Develop MVP

Define legal structure & rules of engagement

Define governance model

Contract with partners and
        technology partners

Technical revalidation

Business case funding

Use case development

Integration with existing systems

Pilot

Member recruitment

Operational Governance

Value added services strategy

Production deployment

Application maintenance

Help desk and operational
support

New feature releases

Cross network interoperability

Network growth analytics
and strategy

Package & recruit members

# A financing model without VCs?

# Cryptocurrency ICO stats 2017 VS. Global IPO activity

Total raised $2.1 bn
Total number of ICOs: 139

Source: https://www.coinschedule.com/stats.php?year=2017

Total raised $63.5 bn
Median deal size $212 mm
Total number of IPOs: 170

Source: Renaissance Capital IPO Intelligence

In a more abstract context, as the first open protocol for exchange 0x represents the beginning of the end for the exchange industry's rent seeking oligopoly: zero exchange.

The first registration of a fund manager to operate a bitcoin investment fund in Canada has been approved by the British Columbia Securities Commission. First Block Capital Inc is also registered as an investment fund manager and exempt market dealer in Ontario.

Also read: Bank of Russia Considers It Premature to Permit Digital Currencies, Warns of ICO Risks

### Bitcoin Fund Manager's Registration Approved

The British Columbia Securities Commission (BCSC) announced on Wednesday "the first registration of an investment fund manager in Canada solely dedicated to cryptocurrency investments." The announcement read:

> " The BCSC has granted First Block Capital Inc. registration as an investment fund manager and an exempt market dealer in order to operate a bitcoin investment fund. "

In one of the strongest regulatory crackdowns on a fast-moving trend, the People's Bank of China (PBoC), the state's central bank and main financial regulator, has released a statement ruling initial coin offerings (ICOs) illegal and ordering groups that have raised money this way return funds.

Source: https://news.bitcoin.com/canadian-securities-commission-grants-bitcoin-fund-manager-registration/

Source: https://www.forbes.com/sites/leonhardweese/2017/09/04/chinas-central-bank-rules-initial-coin-offerings-are-illegal-orders-return-of-funds/#4b289538f216

PAYMENTS AND MONEY TRANSFERS

Learn how to secure YOUR supply chain  with KSI  **blockchain technology** ›

Contact us ›

Jobs at Guardtime ›

# KSI
## Technology

Guardtime's KSI® system is a blockchain
technology that provides massive scale data
authentication without reliance on

# CYBERSECURITY

VOTING

We're hiring! Join our growing, multi-talented team. View current openings.

# Every product has a story

We enable great businesses to build trust in their goods and supply chain.
Provenance powered data helps shoppers choose your product.

| Enter your email... | START FOR FREE |

*Find out more*

# SUPPLY CHAIN MANAGEMENT

# THE FIRST BLOCKCHAIN-SECURED PLATFORM FOR REAL ESTATE RECORDKEEPING

Private Alpha (v1.1) Now Available

# REAL ESTATE

"So even if digital currencies are here to stay, who knows which one will turn out to be the winner?

Hundreds of e-commerce start-ups appreciated rapidly in the tech bubble based on the premise that 'the Internet will change the world.' It did, but most of the companies ended up worthless."

*Howard Marks*
His firm Oaktree Capital had $99 billion of assets under management as of June 2017.

# BLOCKCHAIN

FIAB 2017 – Santa Cruz, Bolivia

Andres Araya Falcone | CIO – Bolsa de Santiago | @andresarayaFA

Rajiv Chodhari | Vice President Financial Markets – IBM | Chodhari@us.ibm.com