Smart Contracts, Blockchain and Data Standards

APRIL 4, 2016 | NEW YORK CITY

Sponsoring organizations

Baruch COLLEGE
ZICKLIN SCHOOL OF BUSINESS

CFA Institute

xBRL US

- Campell Pryde, President and CEO, XBRL US
- John Turner, CEO, XBRL International

The Blockchain Bitcoin & Beyond

Christian Lundkvist, ConsenSys

Outline

- What is Bitcoin?

- What is a Blockchain?

- Generalized blockchains

- Smart contracts

What is Bitcoin?

Not that!

(Those are metal coins with the letter "B" on them)

Bitcoin is a specific application of **Blockchain technology**

What is a Blockchain?

A blockchain is a **database** with specific properties:

- **Decentralized:** Redundant copies shared among many P2P-networked participants

- **Strong Authentication:** Updates to the database require cryptographic access control (private keys)

- **Tamper-resistance:** Can get strong assurance that the database has not been tampered with (mining)

The above makes the database resistant to a minority of participants actively trying to forge and/or corrupt data.

The Bitcoin database

In the case of Bitcoin the blockchain database contains

- Accounts (look like this:
  18bdsW2XFibQKk1yFmk718TeZPAbo3aUeN)

- Balances of the accounts (denominated in BTC)

Updating the database means reducing the number of BTC in an account and increasing it in another account ("Sending bitcoins"). Each account has a corresponding private key needed to send.

What is Bitcoin?

- P2P network

- Blockchain of accounts & balances (~30GB)

- Used to store and transmit value tokens ("bitcoins")

- Similar to internal bank database of account balances, but shared and replicated

Use Cases

Narrow protocol, still useful for certain applications

- Currency in low-trust online environments (SR, Overstock)

- Middleware in remittances (Abra, rebit.ph)

Generalized blockchains (Ethereum)

Newer blockchain designs like Ethereum generalizes the Bitcoin blockchain. The Ethereum blockchain includes:

• Accounts & balances (Ether)

• Arbitrary user-created programs (smart contracts) with function interface

• Programs have associated data and funds and programs can call functions of other programs
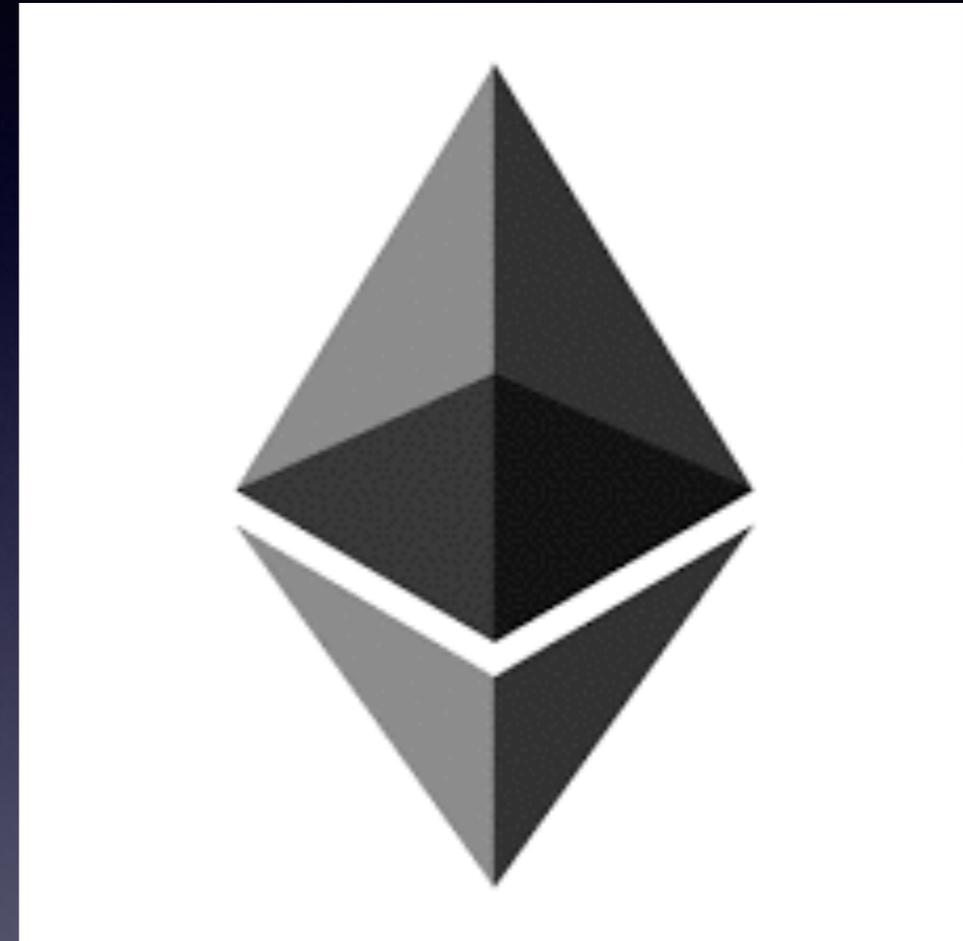
Generalized blockchains (Ethereum)

Updating the Ethereum database can be done in three different ways:

- Sending Ether tokens from one account to another (like bitcoin)

- Uploading a program to the blockchain

- Calling a function of a program on the blockchain
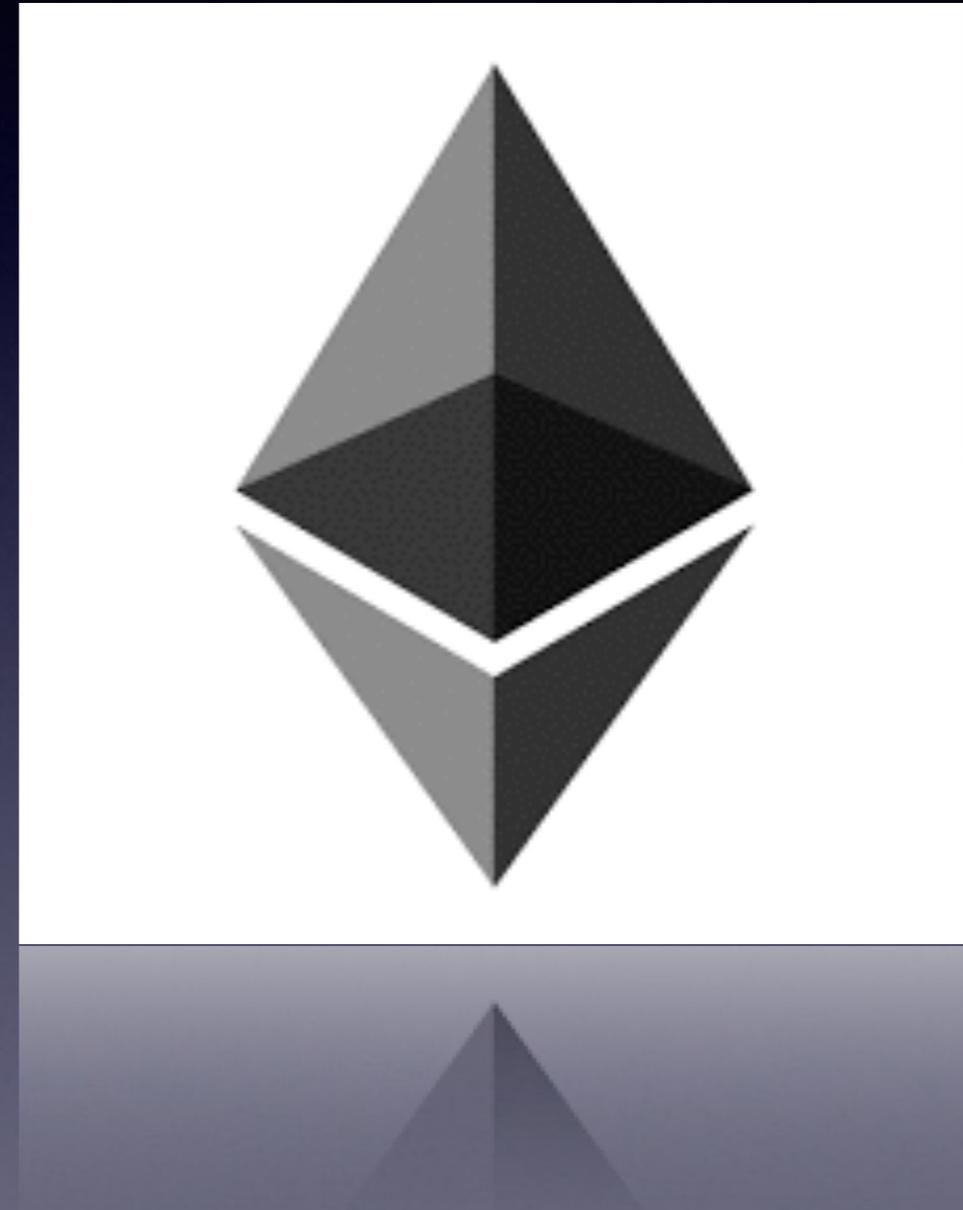
Example: Simple Bet

- Alice and Bob wants to bet on who wins a baseball game

- The bet can be facilitated through a smart contract

- A third party like ESPN can maintain a smart contract containing sports scores that can be queried by other smart contracts

Example: Simple Bet

A: Y 📊 💰

🧑‍🦰
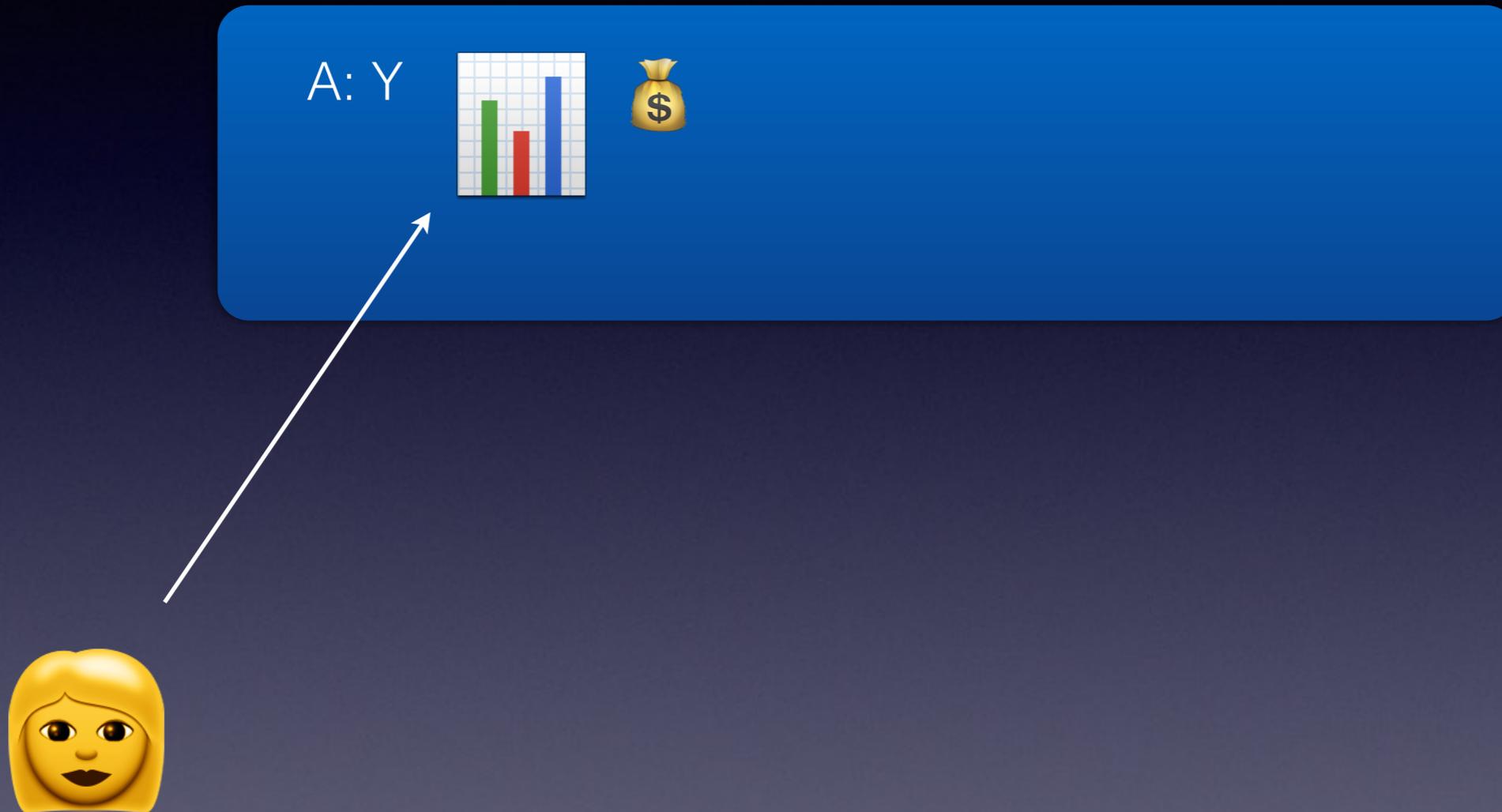
Alice uploads a smart contract to the blockchain along with her bet (Yankees)
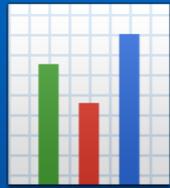
Example: Simple Bet

Bob makes his bet (Red Sox) to the contract

Example: Simple Bet

A: Y   📊 💰
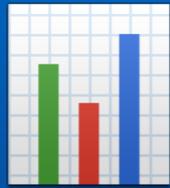
B: RS 📊 💰

The contract lays dormant with custody of the funds

Example: Simple Bet

A: Y 📊 💰
B: RS 💰

📈
Win: RS

👩 👱

On game day the Red Sox wins.The winning team is published on the blockchain by ESPN

Example: Simple Bet
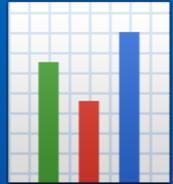
Bob calls the contract to claim his winnings

Example: Simple Bet

The contract calls the getWinner() function
of the ESPN contract which returns Red Sox

Example: Simple Bet

A: Y 📊
B: RS

💰💰
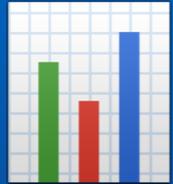
📈
Win: RS

👱‍♀️   👱‍♂️

The contract verifies that Bob is the winner
and sends the winnings

Applications of smart contracts

- Auto-settling financial derivatives

- Triple-entry accounting systems

- Efficient inter-bank settlement

- Self-enforcing legal contracts

- Secure transfer of property titles

- With logic on blockchain - less need for server backend

In general: Smart contracts with front ends allows for **Decentralized Applications (dApps)**

About ConsenSys

- Blockchain Production Studio

- Building dApps and basic infrastructure/platforms

- Identifying areas and industries where blockchain tech can improve/disrupt

- Developing on Ethereum right now since most developer-friendly

Thank you! 😃

QUESTIONS?

Epilogue: Mining

- Updates to the database come in **blocks**

- Each block is hashed to a small number

- Can check hashes to verify integrity

Smart Contracts for Compliance

Mike Goldin
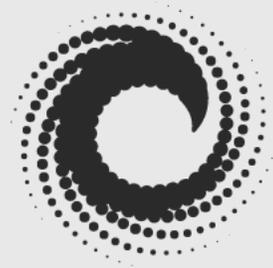
XBRL: The Blockchain Before The Blockchain!

- XBRL aims to resolve many problems that blockchains aim to resolve.
- Open, uniform standards.
- Some automation of standards conformance checking.
- Some automation of compliance checking.
- Blockchains can go further by automating penalties for bad compliance on the basis of structured data.

Accountability + enforcement, by example

- Lets look at a very simple smart contract.
- This is Solidity, a programming language for the Ethereum blockchain.

```
contract QuarterlyReport {

    bool frozen;
    uint penaltyEscrow;

    address accountableSignatory;
    address accepter;
    address penaltyCollector;

    uint40 reportHash;
    bool accepted;

    function QuarterlyReport(address _accountableSignatory, address _accepter,
                             address _penaltyCollector, uint _penaltyEscrow) {

        accountableSignatory = _accountableSignatory;
        accepter = _accepter;
        penaltyCollector = _penaltyCollector;
        penaltyEscrow = _penaltyEscrow;

        frozen = false;
        accepted = false;
    }

    function submitPenaltyEscrow() {
        if(this.balance == penaltyEscrow || msg.value != penaltyEscrow) {
            msg.sender.send(msg.value);
            return;
        }
    }

    function submitReportHash(uint40 _reportHash) {
        if(this.balance != penaltyEscrow || msg.sender != accountableSignatory
           || frozen == true) {
            return;
        }

        reportHash = _reportHash;
    }

    function freezeSubmissions() {
        if(msg.sender != accepter) {
            return;
        }

        frozen = true;
    }

    function acceptReport() {
        if(msg.sender != accepter || frozen != true) {
            return;
        }

        accountableSignatory.send(penaltyEscrow);
        accepted = true;
    }

    function rejectReport() {
        if(msg.sender != accepter || frozen != true) {
            return;
        }

        penaltyCollector.send(penaltyEscrow);
    }

}
```

```
contract QuarterlyReport {

    bool frozen;
    uint penaltyEscrow;

    address accountableSignatory;
    address accepter;
    address penaltyCollector;

    uint40 reportHash;
    bool accepted;
```

```
function QuarterlyReport(address _accountableSignatory, address _accepter,
                        address _penaltyCollector, uint _penaltyEscrow) {

    accountableSignatory = _accountableSignatory;
    accepter = _accepter;
    penaltyCollector = _penaltyCollector;
    penaltyEscrow = _penaltyEscrow;

    frozen = false;
    accepted = false;
}
```

```
function submitPenaltyEscrow() {
  if(this.balance == penaltyEscrow || msg.value != penaltyEscrow) {
    msg.sender.send(msg.value);
    return;
  }
}


function submitReportHash(uint40 _reportHash) {
  if(this.balance != penaltyEscrow || msg.sender != accountableSignatory
     || frozen == true) {
    return;
  }

  reportHash = _reportHash;
}
```

```
function submitPenaltyEscrow() {
  if(this.balance == penaltyEscrow || msg.value != penaltyEscrow) {
    msg.sender.send(msg.value);
    return;
  }
}

function submitReportHash(uint40 _reportHash) {
  if(this.balance != penaltyEscrow || msg.sender != accountableSignatory
     || frozen == true) {
    return;
  }

  reportHash = _reportHash;
}
```

```
function submitPenaltyEscrow() {
  if(this.balance == penaltyEscrow || msg.value != penaltyEscrow) {
    msg.sender.send(msg.value);
    return;
  }
}


function submitReportHash(uint40 _reportHash) {
  if(this.balance != penaltyEscrow || msg.sender != accountableSignatory
      || frozen == true) {
    return;
  }

  reportHash = _reportHash;
}
```

```
function freezeSubmissions() {
  if(msg.sender != accepter) {
    return;
  }

  frozen = true;
}

function acceptReport() {
  if(msg.sender != accepter || frozen != true) {
    return;
  }

  accountableSignatory.send(penaltyEscrow);
  accepted = true;
}

function rejectReport() {
  if(msg.sender != accepter || frozen != true) {
    return;
  }

  penaltyCollector.send(penaltyEscrow);
}
```

```
function freezeSubmissions() {
  if(msg.sender != accepter) {
    return;
  }

  frozen = true;
}


function acceptReport() {
  if(msg.sender != accepter || frozen != true) {
    return;
  }

  accountableSignatory.send(penaltyEscrow);
  accepted = true;
}

function rejectReport() {
  if(msg.sender != accepter || frozen != true) {
    return;
  }

  penaltyCollector.send(penaltyEscrow);
}
```

```
function freezeSubmissions() {
  if(msg.sender != accepter) {
    return;
  }


  frozen = true;
}
```

```
function acceptReport() {
  if(msg.sender != accepter || frozen != true) {
    return;
  }


  accountableSignatory.send(penaltyEscrow);
  accepted = true;
}
```

```
function rejectReport() {
  if(msg.sender != accepter || frozen != true) {
    return;
  }


  penaltyCollector.send(penaltyEscrow);
}
```

```
function freezeSubmissions() {
  if(msg.sender != accepter) {
    return;
  }

  frozen = true;
}

function acceptReport() {
  if(msg.sender != accepter || frozen != true) {
    return;
  }

  accountableSignatory.send(penaltyEscrow);
  accepted = true;
}

function rejectReport() {
  if(msg.sender != accepter || frozen != true) {
    return;
  }

  penaltyCollector.send(penaltyEscrow);
}
```

XBRL + blockchains

- The XBRL you know and love

- Plus the ability for regulators to collect penalties programmatically on the basis of XBRL data

- Markets on SEC penalty tokens? ☺

Sponsoring organizations

BaruchCOLLEGE
ZICKLIN SCHOOL OF BUSINESS

CFA Institute

xBRL US

The Landscape for Blockchain Technology

- Campbell Pryde, President and CEO, XBRL US
- Philip Moyer, Senior VP and Managing Director, Technology, Safeguard Scientifics
- Joseph Lubin, Founder, Consensys

BLOCKCHAIN TECHNOLOGY LANDSCAPE > APRIL 2016

XBRL|US

OTHER
R3 CEV *Bank Consortium*

APPLICATIONS
(Products & Services)

BITCOIN NETWORK BASED

PAYMENT PROCESSOR
- BITPAY
- CIRCLE

EXCHANGE
- COINJAR
- BITSTAMP
- KRAKEN
- COINBASE
- MORE

TRADING PLATFORM

HEDGY
Product: *Bitcoin Trading Platform*

LedgerX
Product: *Bitcoin Options Trading Platform*

TeraExchange
Product: *Bitcoin Swap Trading Platform*

ISSUANCE PLATFORM

LINQ (NASDAQ)
Product: *Private Issuance Platform*

tØ
Product: *Debt & Equity Trading Platform*

NON-BITCOIN NETWORK BASED

BLOCKCHAIN TOOL PROVIDERS

CHAIN
Tools: *Bitcoin API's & Tools*

SYMBIONT
Tools: *Smart Contract API's & Tools*

BLOCKSTREAM
Tools: *Sidestream*

MONETAGO
Tools: *Bitcoin API's & Tools*

CONSENSYS
Tools: *API's and Tools for Ethereum, bitcoin and private permissioned ledgers*

BLOCKAPPS
Tools: *API's and Tools that are compatible with Ethereum*

ERIS INDUSTRIES
Tools: *Smart Contract apps on Eris software network using Tendermint and Ethereum compatible*

DAH (Digital Asset Holdings)
Tools: *API's & Tools for Financial Services*

ITBIT
Tools: *API's & Tools for Financial Services using Bankchain*

INFRASTRUCTURE ADD-ON

COUNTER PARTY
Infrastructure: *Smart Contracts*

ROOTSTOCK
Infrastructure: *Smart Contracts*

INFRASTRUCTURE
(Blockchain Networks)

NON PERMISSIONED PUBLIC LEDGER

BITCOIN BLOCKCHAIN
Currency: *Bitcoin*
Settlement Process: *Proof of Work*
Ledger Owner: *All Users*

ETHEREUM
Currency: *Ether*
Settlement Process: *Proof of Work*
Ledger Owner: *All Users*

TENDERMINT
Settlement Process: *Consensus (Proof of Stake)*

PERMISSIONED PUBLIC LEDGER

HYPER LEDGER
Settlement Process: *Proof of Work*
Ledger Owner: *All Users*

RIPPLE
Currency: *XFR*
Settlement Process: *Consensus*
Ledger Owner: *Trusted Parties*

PERMISSIONED PRIVATE LEDGER

BANKCHAIN
Settlement Process: *Consensus*
Ledger Owner: *ItBit*

Blockchain Funding Climate

Philip Moyer,

Managing Director Safeguard Scientifics

Financial Technology Markets

Global

- London Financings have been growing at twice the rate of Silicon Valley
- KPMG 100 Top FinTech Companies:
  - 40 US companies,
  - 20 from EMEA,
  - 18 from the UK
  - 22 from ASPAC.

Corporate Venture Larger & Smarter

$16bn Funding in last year	+198.53% YoY Funding Growth	1,257 Deals in last year	+111.62% YoY Deal Growth
231 Avg Deals per Quarter	$2.66bn Avg Funding per Quarter	Q1'15 Biggest Quarter ($ Funding)	Q3'14 Biggest Quarter (# of deals)
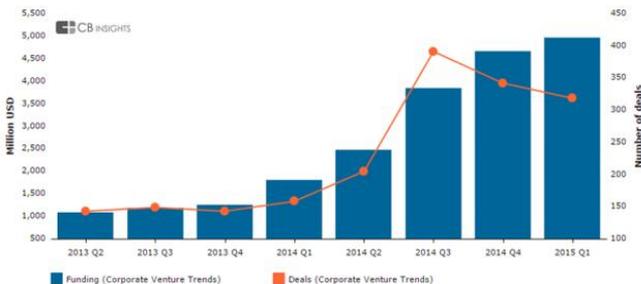
Sector	Semi-Unicorns	Unicorns	Total
Lending	11	11	22
Payments	11	6	17
Investing	1	5	6
Real estate	2	3	5
Insurance	3	1	4
Accounting	2	0	2
Credit Reports	2	0	2
Security	1	1	2
Bitcoin	1	2	3
Other	2	5	7

Data Sourced: FT Capital

February - 50 Fin Tech Deals (Source FT Capital)

- 18 - Payments
- 12- Securities & Cap Mkts
- 9 – Banking
- 6 – Finance Mgmt
- 3 – Insurance
- 2 – Finance BPO

Valuations

Infrastructure: 10x,   Tools 7-10x   Applications: 3-7x

Public FinTech Sector Universe
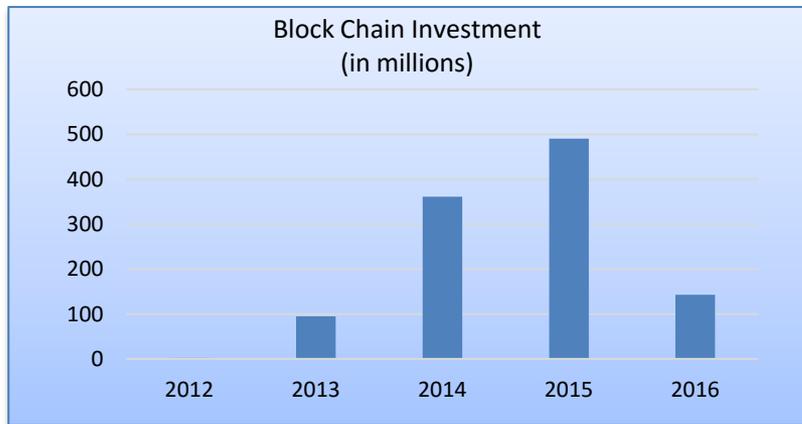
Median Price / Earnings Multiples by FT Sector

2016E Price / Earnings Multiples

Lending / Mortgage / Real Estate Solutions	26.5x
Payroll / HR / Benefits Solutions	24.4x
Insurance / Healthcare Solutions	20.7x
Investment Solutions	20.2x
Alternative Trading Systems and Market Makers	19.3x
Global Securities Exchanges	19.1x
Banking Solutions	19.1x
Financial Media / Data Solutions	18.6x
Payment Software / Hardware	17.4x
Payment Processing / Outsourcing	16.6x
Outsourced Processing Solutions	16.3x
eBrokerage / eFinance	16.3x
Trust and Services Focused FIs	11.5x
Specialty Finance / Consumer Lending	11.2x
Payments POS Devices / Solutions	10.6x
Selected Diversified FIs	10.2x
BDC / Public Investment Vehicles	8.1x

slide 2

SMART CONTRACTS, BLOCKCHAIN AND DATA STANDARDS
April 4, 2016 | New York City

Sponsoring Organizations
Baruch COLLEGE
ZICKLIN SCHOOL OF BUSINESS
CFA Institute
xBRL US

42 of 136

Blockchain Funding Market

Over $1B in Blockchain Deals

Block Chain Investment (in millions)

Year	Investment
2012	0
2013	~90
2014	~360
2015	~490
2016	~140

Global # of Deals

Location	Deals	Location	Deals
Bay Area, CA	22	Cambridge, MA	2
New York, NY	12	Ireland	2
London, UK	7	Hong Kong	2
Southern CA	7	France	2
Canadian	5	Phillipines	2
Austin, TX	4	Australia	2
Singapore	4	Israel	1
Spain	3	Japan	1
Sweden	3	South Korea	1

Data Sourced From : VentureSource, Crunchbase

Institutional Investors

- 177 Unique Investors

- Top 10 Most Active Blockchain Investors

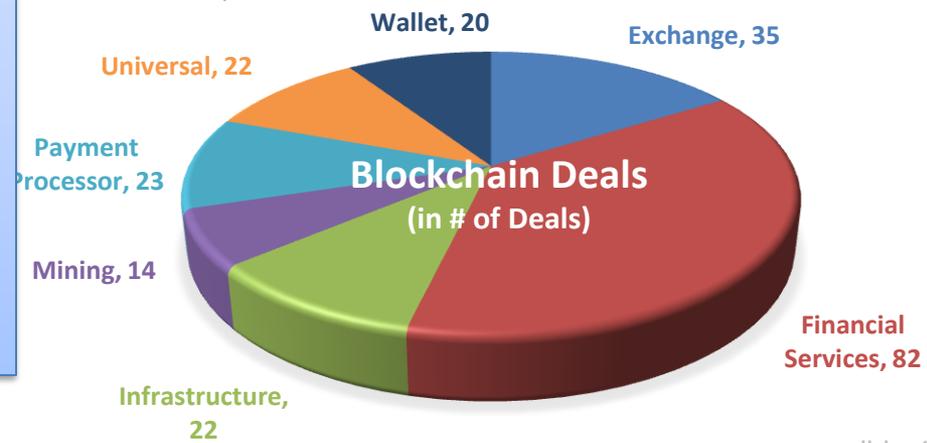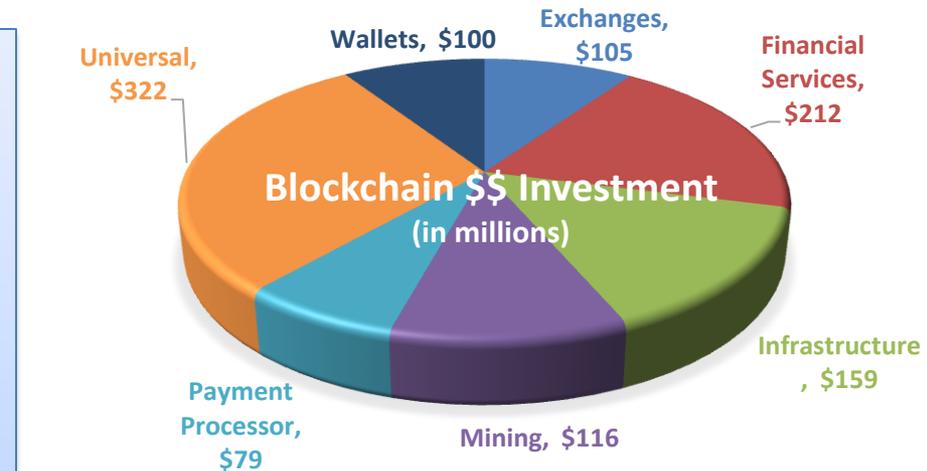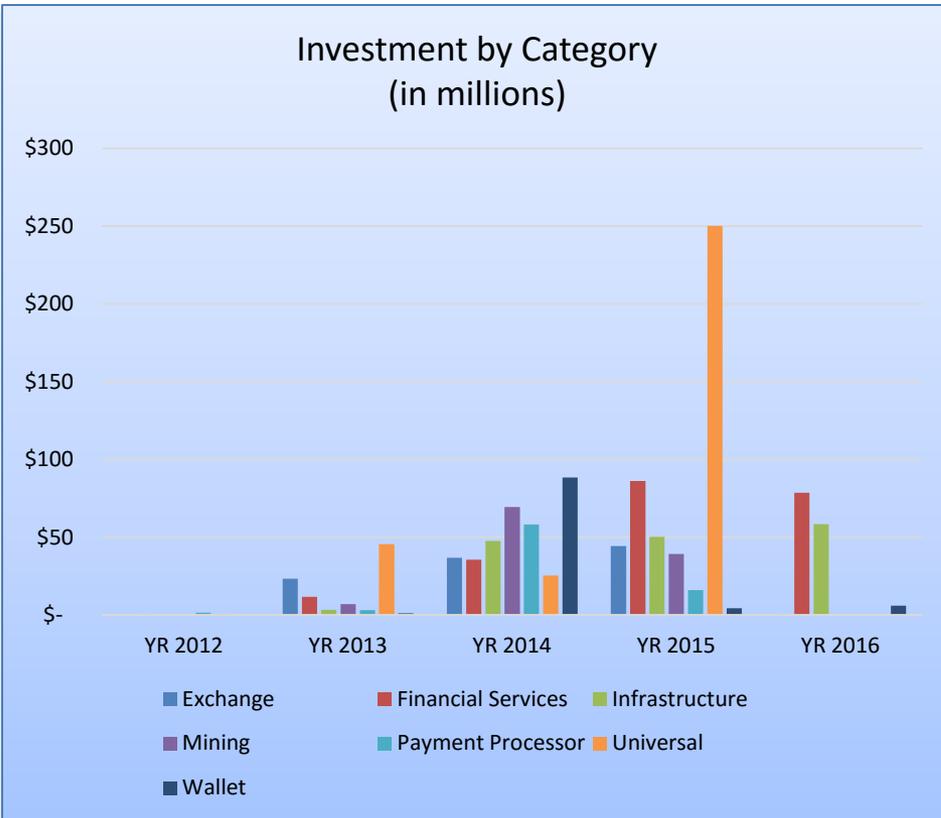| Investor	Deals	Investor	Deals
Digital Currency Group	14	AME Cloud Ventures	4
Blockchain Capital	8	Khosla Ventures	4
Plug and Play Ventures	7	RRE Ventures	3
Pantera Capital	5	Coinsilium	3
500 Startups	4	SV Angel	3

Corporate Investors

Citi, Visa, Mastercard, American Express, NY Life, StateStreet, JP Morgan, Wells Fargo, Goldman Sachs,BBVA, Barclays, Comm Bank of Australia, Credit Suisse, Royal Bank of Scotland, UBS, Banco Santander, Danske Bank, Sumitomo Mitsui Banking Corporation, Westpac, JP Morgan,

London Stock Exchange, Nasdaq, NYSE,

Deloitte, Microsoft, IBM, Intel, Cisco….

-

Blockchain Funding

We are in the infrastructure build-out phase…

Investment by Category (in millions)

Blockchain $$ Investment (in millions)
- Wallets, $100
- Exchanges, $105
- Financial Services, $212
- Universal, $322
- Payment Processor, $79
- Mining, $116
- Infrastructure, $159

Blockchain Deals (in # of Deals)
- Wallet, 20
- Exchange, 35
- Universal, 22
- Payment Processor, 23
- Mining, 14
- Financial Services, 82
- Infrastructure, 22

Data Sourced From : VentureSource, Crunchbase

Examples of Large Blockchain Deals

NAME	CATEGORY	DESCRIPTION	TOTAL RAISE	ROUND
21 Inc (21e6)	Infrastructure/Ledgers	Bit Coin Computer	$121	First
Coinbaase	Exchange	Wallet, Peer to Peer Payment	$106	Third
Blockstream	Tools	SideStream	$76	Series A
Circle	Payment Processor	Peer to Peer Payment	$76	Third
BitFury	Tools	Mining	$60	Third
Digital Asset Holdings	Tools	APIs & Tools for Financial Services	$60	N/A
Chain	Tools	Bitcoing API's & Tools - PAAS	$44	Second
Ripple Labs	Infrastructure/Ledgers	Financial services	$41	First
Xapo	Wallet	Bitcoin Wallet	$40	First
BitPay	Payment Processor	Merchant - Bitcoin Payment Processor	$33	First
Blockchain	Infrastructure/Ledgers	Wallet	$31	First
KnCMiner	Tools	Mining	$29	Second
itBit	Trading Platform	Exchange	$28	First
Vogogo	Payment Processor	Payment Processor	$21	Second
Etherium	Infrastructure/Ledgers	Open Source PAAs	$18	Seed
BitStamp	Exchange	Currency Exchange	$10	First

Data Sourced From : VentureSource, Crunchbase

Sponsoring Organizations
Baruch COLLEGE
ZICKLIN SCHOOL OF BUSINESS
CFA Institute
xBRL US

Sponsoring organizations

BaruchCOLLEGE
ZICKLIN SCHOOL OF BUSINESS

CFA Institute

xBRL
US

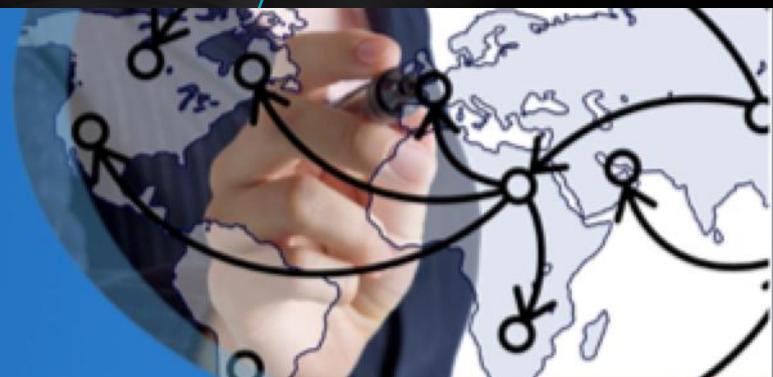# James Allen, CFA, Head of Capital Markets Policy for CFA Institute

Blockchain Presentations

– Nasdaq Linq for Private Securities Issuance

– ItBit Bankchain for Gold & Corporate Actions

– Ethereum Total Return Swap (eTRS)

NASDAQ LINQ

Smart Contracts, Blockchain and Data Standards
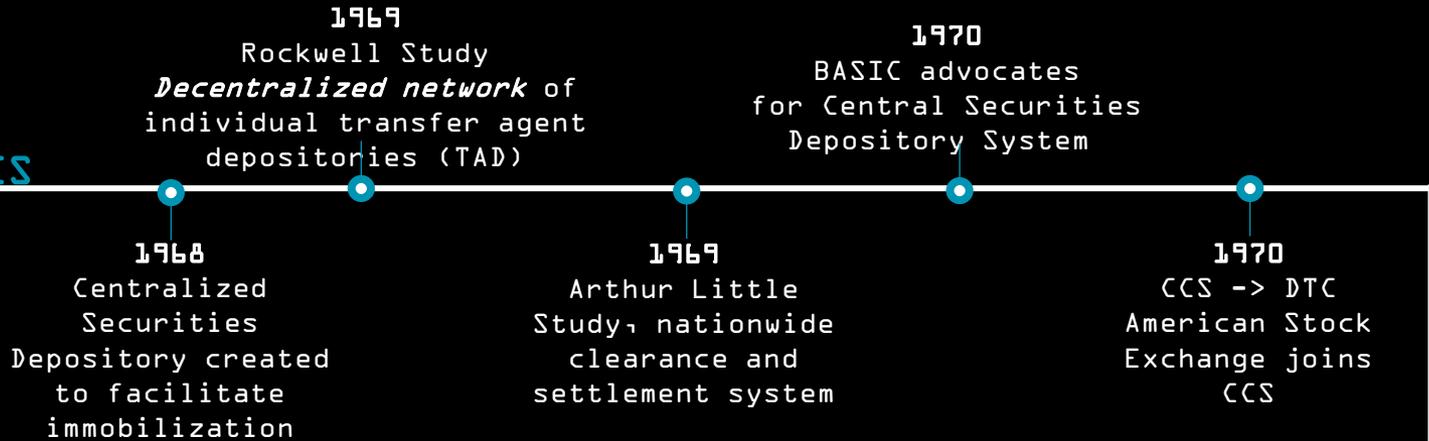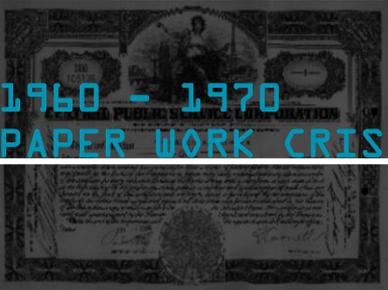
APRIL 4, 2016 | NEW YORK CITY
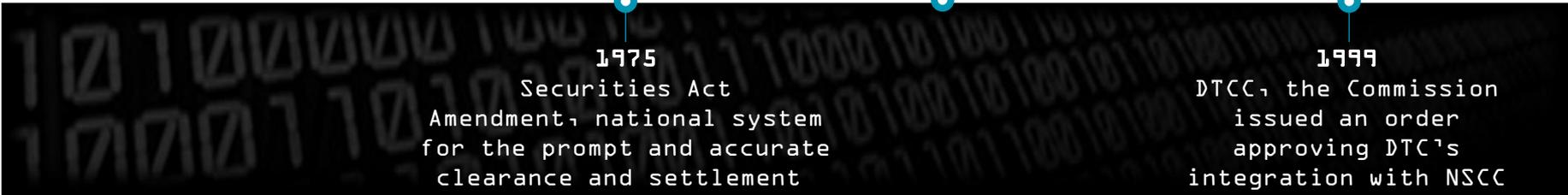
THE INFLUENCE OF TECHNOLOGY AND RISK
ON CAPITAL MARKETS STRUCTURES

- Brief History

- Current State

- Blockchain in the mix

- Linq

Nasdaq

EVOLUTION OF CAPITAL MARKETS

1969
Rockwell Study
Decentralized network of
individual transfer agent
depositories (TAD)

1970
BASIC advocates
for Central Securities
Depository System

1960 - 1970
PAPER WORK CRISIS

1968
Centralized
Securities
Depository created
to facilitate
immobilization

1969
Arthur Little
Study, nationwide
clearance and
settlement system

1970
CCS -> DTC
American Stock
Exchange joins
CCS

1980-1990
DTC mergers and
acquisitions

1970 - 2000
EFFICIENCIES THROUGH CENTRALIZATION

1975
Securities Act
Amendment, national system
for the prompt and accurate
clearance and settlement

1999
DTCC, the Commission
issued an order
approving DTC's
integration with NSCC

FUTURE
Markets Everywhere

2008 - FUTURE
ENTER THE BLOCKCHAIN

2008
Satoshi Nakamoto
published the
seminal bitcoin paper

2015
First Transaction on Nasdaq
Linq
Announcement of Proxy Voting
Increased Traction in

THE WORLD TODAY

CENTRALIZED CORE

MULTIPLE INTERMEDIARIES

SILOES OF INFORMATION

PAIN-POINT - RECONCILIATION
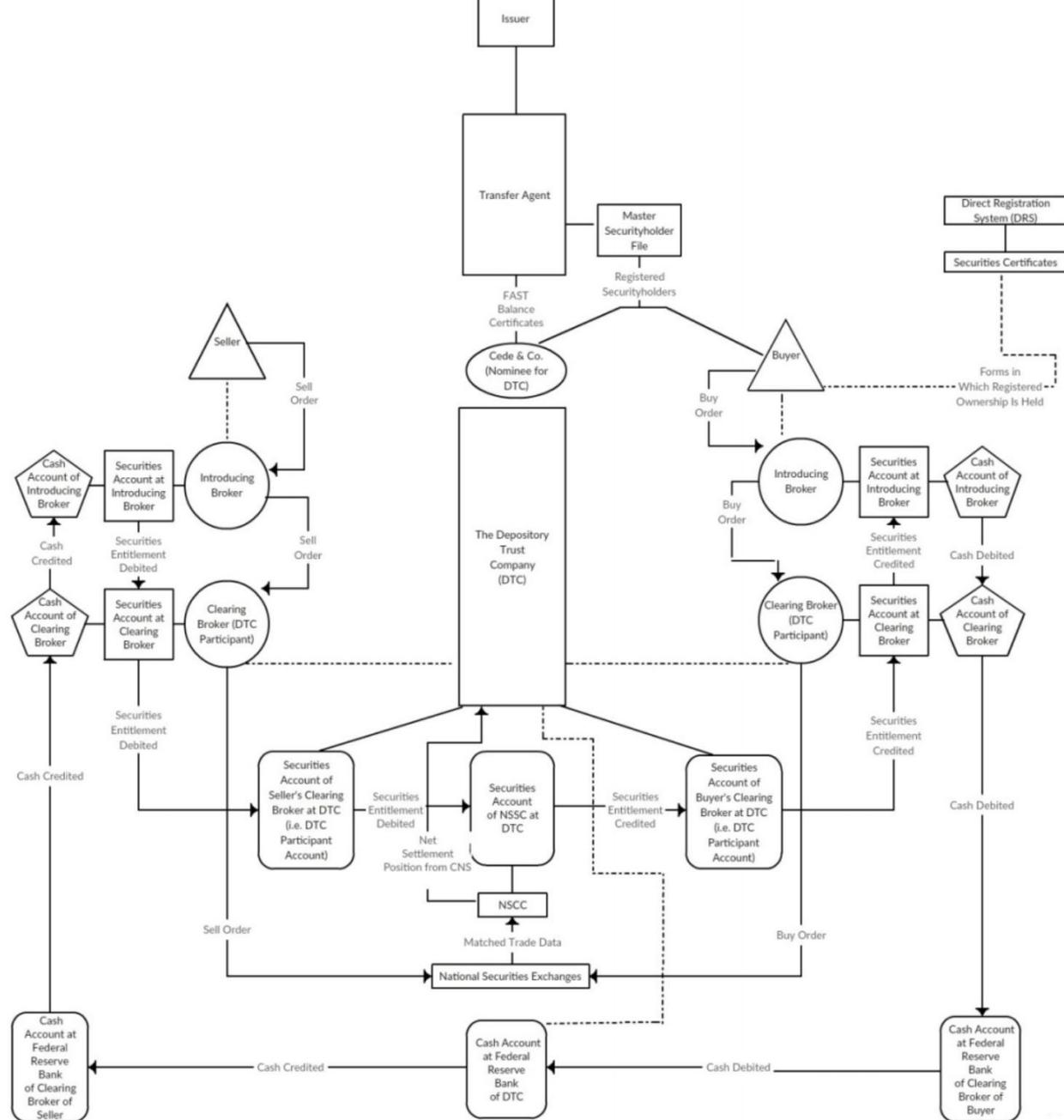
WHY IS BLOCKCHAIN RELEVANT FOR CAPITAL MARKETS?

A DIGITAL ASSET = A DIGITAL BEARER TOKEN

Physical Bearer Tokens

Digital Bearer Tokens

Bitcoin	Exists

Currencies	
Securities	Emerging
Commercial IOUs	
Brand/Loyalty Points	
Etc..	

Source: chain.com
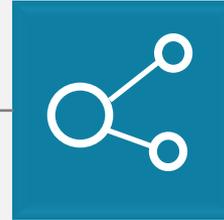
Nasdaq

WHERE DIGITAL ASSETS GET THEIR VALUE
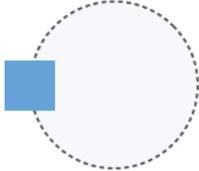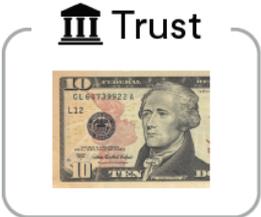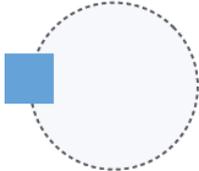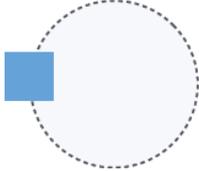
Source: chain.com

HOW IS BLOCKCHAIN DIFFERENT?

Assets are **issued onto a network** that spans organizations

Entities control asset movement by **directly interacting** with the network's shared ledger

LEDGER

00110110
00110110
00110110

All transactions are enabled and secured by **cryptography**

7

Programmable "smart contracts" enable complex transactions
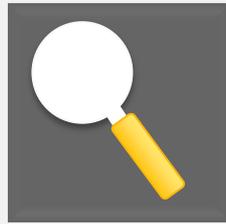
Instant, **direct** value transfer; 24/7

Flexible, digital rails enable user-friendly apps and **interoperability**

Transaction finality: eliminates clearing, reconciliation, errors; a single source of truth provides perfect auditability

Source: chain.com

Nasdaq

LINQ ARCHITECTURE
TECHNICAL INNOVATION IN PRIVATE SECURITIES

User Features leverage the underlying infrastructure and provide value-added services including **ledger visibility**, **contract management**, **investor communication** and **order management**.

Linq API enables management of unregistered securities including **issuance**, **allocations**, **corporate actions**, **auctions**, **transactions** and **settlement** through integration with paying agent.

Blockchain Enabled Ledger provides **data provenance**, **immutability**, **protection from double-spend** and **distribution** of record keeping.

Issuers

Investors
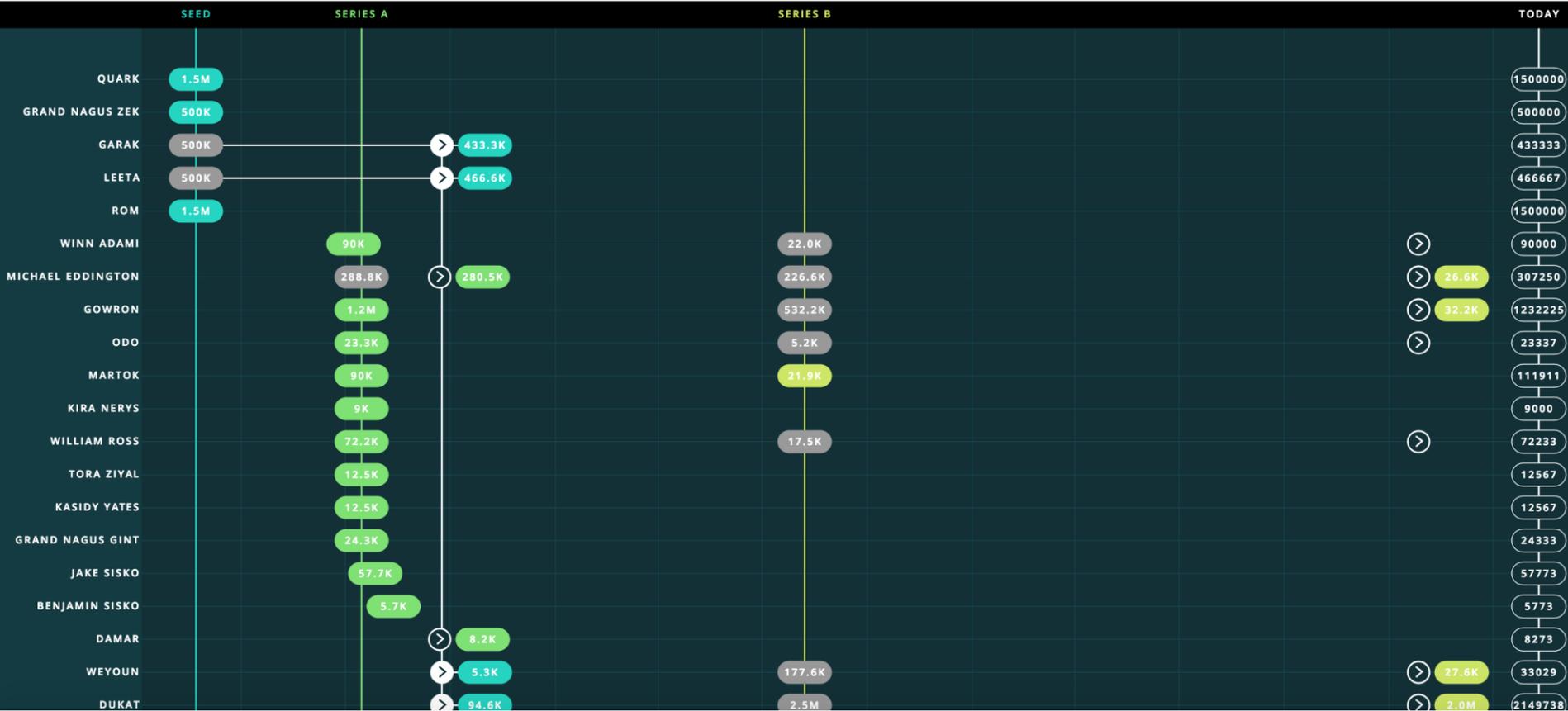
Issuer Node

Manager Node

Block Generator

Auditor Node

9

Nasdaq
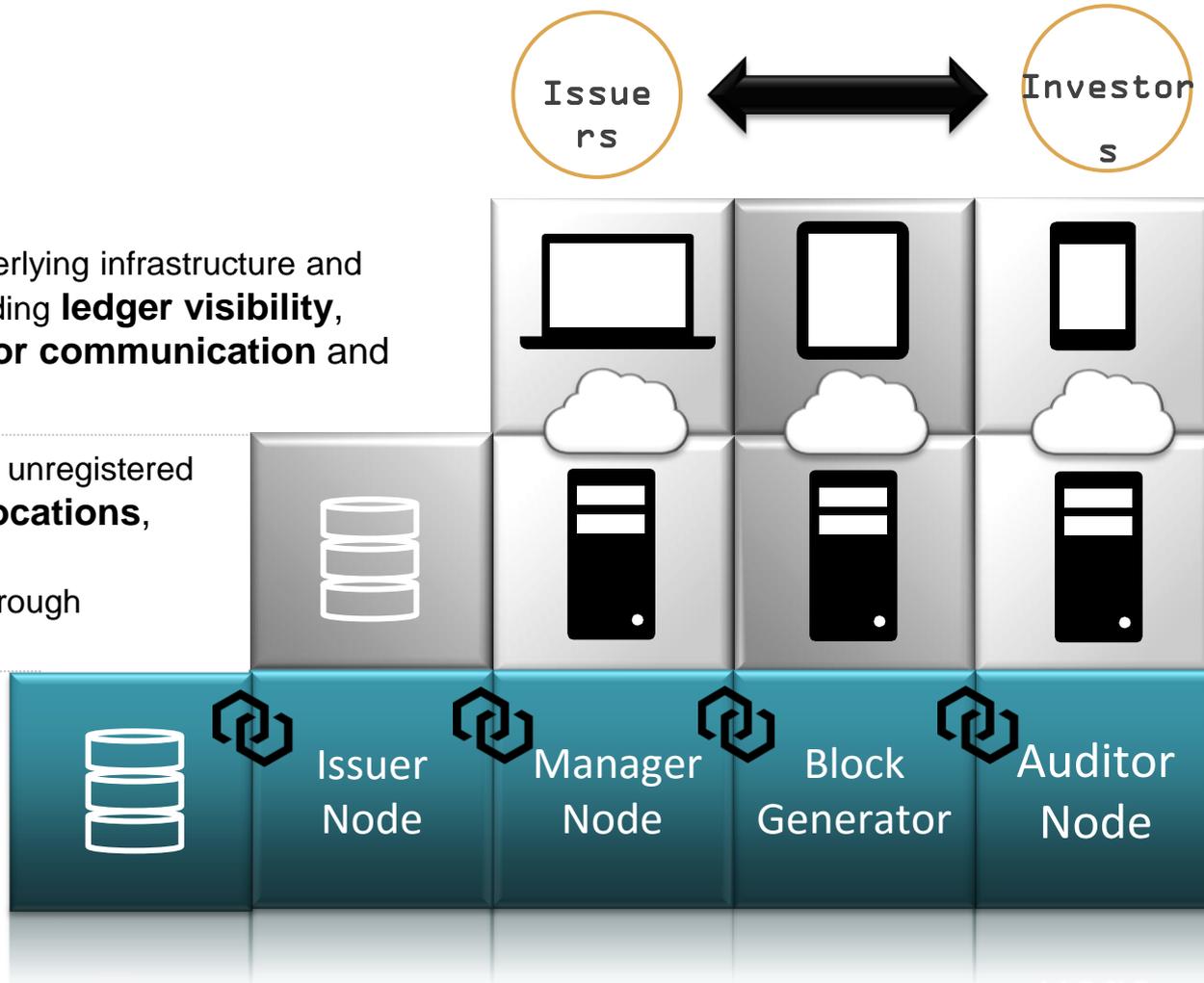
NATIVE ASSET ISSUANCE
FOR EACH CLASS OF SHARES

Key Financing Events

ROUND	ISSUED	ALLOCATED	UN-ALLOCATED	SHARE PRICE
SEED	9,716,729	4,719,465	4,997,264	$0.0001
SERIES A	3,611,984	2,013,267	1,598,717	$1.5555
SERIES B	5,889,714	3,827,840	2,061,874	$11.75

Nasdaq

FULL REGISTRAR RECORD KEEPING
EQUITY TIMELINE

AUCTION-BASED ORDER MATCHING
ALL POSITIONS VALIDATED FROM THE REGISTRAR

Chain 2016 Q1 Series B

MATCHED BUY TOTAL $18,068,597.75 | CLEARING PRICE $11.75

EXECUTE AUCTION

TOTAL SHARES TO BUY	TOTAL SHARES TO SELL	TOTAL SHARES MATCHED	TOTAL SHARES UNMATCHED	IMBALANCE SIDE	IMBALANCE SHARES
1,750,000	1,537,753	1,537,753	212,247	Buy	212,247

Buyers
3 BUYING 1,750,000 SHARES

ORDER	DATE	PARTICIPANT	ORDER SIZE	PRICE	MATCH SIZE	SPECIAL
336	2016-3-4	GRAMMAR BIO-MEDICAL GROUP	900,000	$15.00	900000	
338	2016-3-4	CALTEGRIS FUTURES INC	300,000	$14.00	300000	
337	2016-3-4	BLACKGEM INC	550,000	$13.00	337753	

Sellers
13 SELLING 1,537,753 SHARES

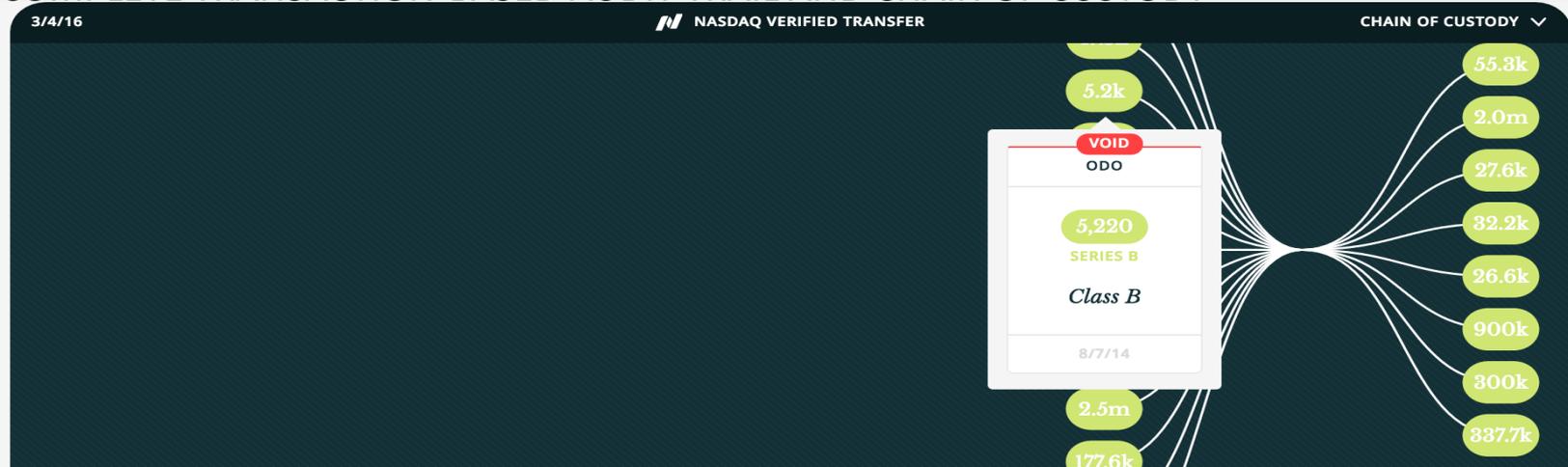| ORDER	DATE	PARTICIPANT	ORDER SIZE	PRICE	MATCH SIZE	SPECIAL
328	2016-3-4	VIC FONTAINE	17,504	$9.00	17504	
329	2016-3-4	WINN ADAMI	22,011	$9.00	22011	
330	2016-3-4	WILLIAM ROSS	17,560	$9.00	17560	
331	2016-3-4	ODO	5,220	$9.00	5220	
332	2016-3-4	BRUNT	43,332	$9.00	43332	
339	2016-3-4	EZRI DAX	17,263	$9.00	17263	
333	2016-3-4	ISHKA	7,031	$10.00	7031	
334	2016-3-4	WORF, SON OF MOGH	43,255	$10.00	43255	
335	2016-3-4	JADZIA DAX	14,577	$10.00	14577	
324	2016-3-4	DUKAT	500,000	$10.50	500000	
325	2016-3-4	WEYOUN	150,000	$10.50	150000	

12

Nasdaq

TRANSACTION EXECUTION

A SINGLE BLOCKCHAIN TRANSACTION REPRESENTS A MANY-TO-MANY TRANSFER
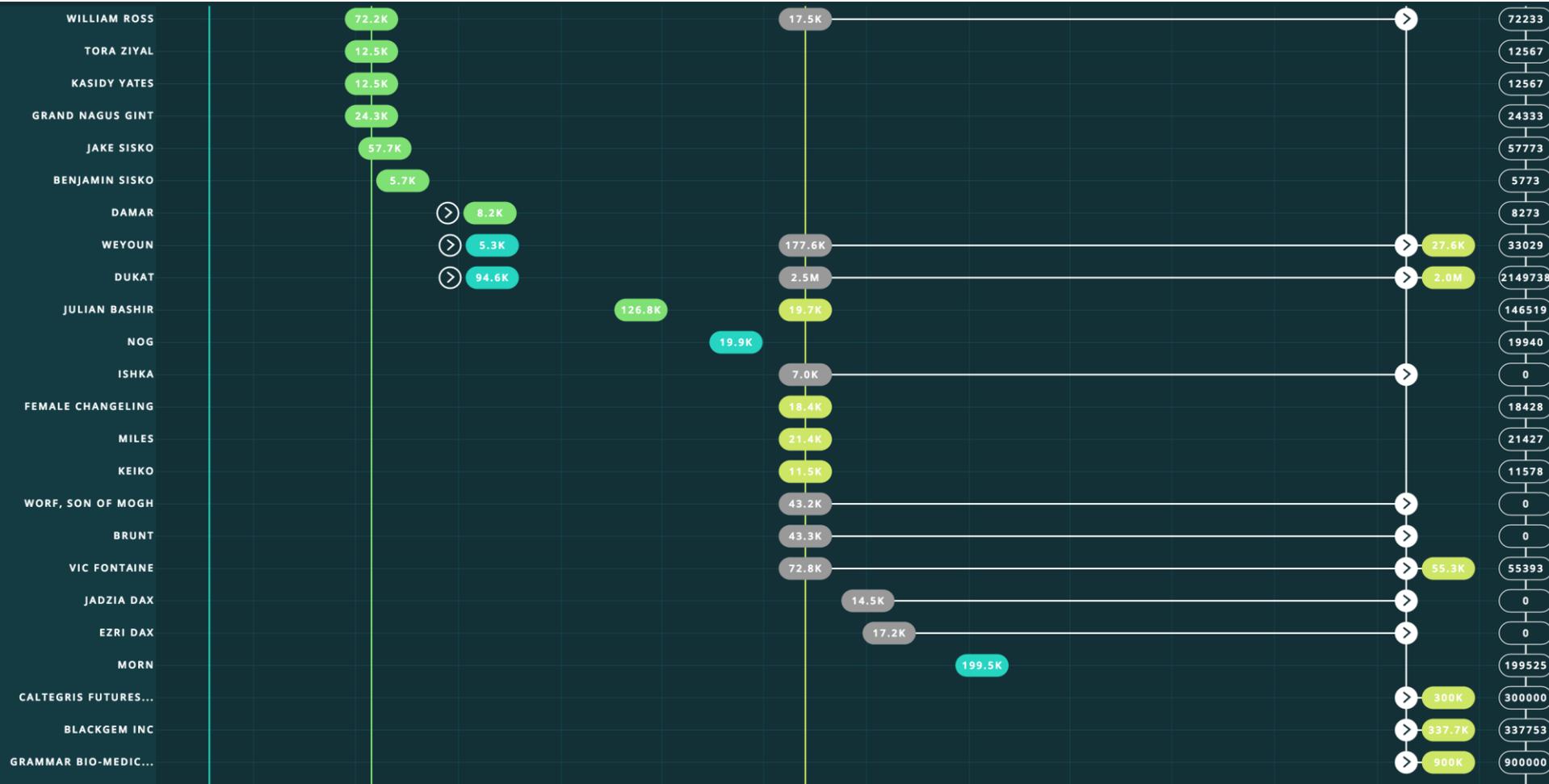
TRANSACTION EXECUTION

COMPLETE TRANSACTION-BASED AUDIT TRAIL AND CHAIN OF CUSTODY

INVESTOR VISIBILITY

Leeta
Investor

466.6k *Shares*

1 *Certificates*

LEETA	VOID LEETA
466,667	**500,000**
SEED	SEED
Common Class	*Common Class*
10/31/13	2/20/13

CLASS	SHARES	PRICE	AMT. INVESTED
CO COMMON CLASS	466,667	$0.000001	$0.47
TOTAL	**466,667**		**$0.47**

Nasdaq

BLOCKCHAIN BACKED RECORDS

EACH RECORD OF OWNERSHIP BACKED BY BLOCKCHAIN TRANSACTION

Certificate #2085

466,667 shares of Common Class issued on October 31st, 2013 to Leeta .

NASDAQ VERIFIED CERTIFICATE | TRANSACTION ID 29D042CF06142AD711AF3C0532E66863C9493055AC8C4CE290D813E1D1AB5252

⟨⟩ Chain

THIS CERTIFIES THAT

Leeta

IS THE OWNER OF

466,667

Fully paid and non-assessable shares of the Common Class stock of Leeta

PRICE PER SHARE:

$0.0001

INVESTMENT AMOUNT:

$46.67

THESE SECURITIES HAVE NOT BEEN REGISTERED UNDER THE SECURITIES ACT OF 1933, AS AMENDED. THEY MAY NOT BE SOLD, OFFERED FOR SALE, PLEDGED OR HYPOTHECATED IN THE ABSENCE OF A REGISTRATION STATEMENT IN EFFECT WITH RESPECT TO THE SECURITIES UNDER SUCH ACT OR AN OPINION OF COUNSEL SATISFACTORY TO THE COMPANY THAT SUCH REGISTRATION IS NOT REQUIRED OR UNLESS SOLD PURSUANT TO RULE 144 OF SUCH ACT.

THE SECURITIES REPRESENTED BY THIS CERTIFICATE ARE SUBJECT TO A LOCK-UP PERIOD AFTER THE EFFECTIVE DATE OF THE ISSUER'S REGISTRATION STATEMENT FILED UNDER THE SECURITIES ACT OF 1933, AS AMENDED, AS SET FORTH IN AN AGREEMENT BETWEEN THE COMPANY AND THE ORIGINAL HOLDER OF THESE SECURITIES, A COPY OF WHICH MAY BE OBTAINED AT THE ISSUER'S PRINCIPAL OFFICE. SUCH LOCK-UP PERIOD IS BINDING ON TRANSFEREES OF THESE SHARES. THE SHARES EVIDENCED HEREBY ARE SUBJECT TO A VOTING AGREEMENT (A COPY OF WHICH MAY BE OBTAINED UPON WRITTEN REQUEST FROM THE ISSUER), AND BY ACCEPTING ANY INTEREST IN SUCH SHARES THE PERSON ACCEPTING SUCH INTEREST SHALL BE DEEMED TO AGREE TO AND SHALL BECOME BOUND BY ALL THE PROVISIONS OF SAID VOTING AGREEMENT.

THE COMPANY IS AUTHORIZED TO ISSUE MORE THAN ONE CLASS OR SERIES OF STOCK. A COPY OF THE PREFERENCES, POWERS, QUALIFICATIONS AND RIGHTS

IN-SYSTEM CONTRACT FLOWS
REDUCE ANY POTENTIAL FOR DOUBLE ENTRY OF INFORMATION

Pending Certificate

1 shares of Common Class issued on March 4th, 2016 to Leeta .

All contracts are signed. **AUTHORIZE PAYMENT**

LEGEND

FIRST REFUSAL & CO-SALE   INVESTOR RIGHTS   PURCHASE AGREEMENT   VOTING AGREEMENT

⬡ Chain

THIS CERTIFIES THAT

Leeta

IS THE OWNER OF

1

Fully paid and non-assessable shares of the Common Class stock of Quark Inc.

PRICE PER SHARE:

$0.01

SECOND AMENDED AND RESTATED FIRST REFUSAL AND CO-SALE AGREEMENT

This **SECOND AMENDED AND RESTATED FIRST REFUSAL AND CO-SALE AGREEMENT** (the "Agreement") is entered into as of the 31st day of August, 2015 by and among CHAIN, INC., a Delaware corporation (the "Company"), the holders of Common Stock of the Company (the "Common Stock") listed on Exhibit A attached hereto (the "Common Holders") and the holders of Series A Preferred Stock, Series B Preferred Stock, Series C Preferred Stock and Series C-1 Preferred Stock of the Company (collectively, the "Preferred Stock") listed on Exhibit B attached hereto (the "Investors").

W I T N E S S E T H :

WHEREAS, the Company and certain of the Investors (the "Series C Investors") are parties to that certain Series C and Series C-1 Preferred Stock Purchase Agreement of even date herewith (the "Series C Agreement"), pursuant to which the Series C Investors are purchasing shares of the Company's Series C Preferred Stock and Series C-1 Preferred Stock;

WHEREAS, each Common Holder is the beneficial owner of the number of shares of Common Stock set forth opposite his name on Exhibit A attached hereto;

WHEREAS, the Company, the Common Holders and certain of the Investors (the "Existing Investors") are parties to that certain Amended and Restated First Refusal and Co-Sale Agreement, dated as of August 7, 2014 (the "Prior Agreement"); and

Nasdaq

NASDAQ LINQ AS A PLATFORM ACROSS ASSETS

Given the platform capabilities, Linq can become the foundation to support a wide variety of asset types and market structures.

PLATFORM CAPABILITIES

Issuers

Ledger Recordkeeping

Investor Communication

Price Discovery Auctions

Contracts and Agreements

Payment Settlement

Investors

Workflows that tie these together

Nasdaq

Sponsoring organizations

BaruchCOLLEGE
ZICKLIN SCHOOL OF BUSINESS

CFA Institute

xBRL
US

Bankchain

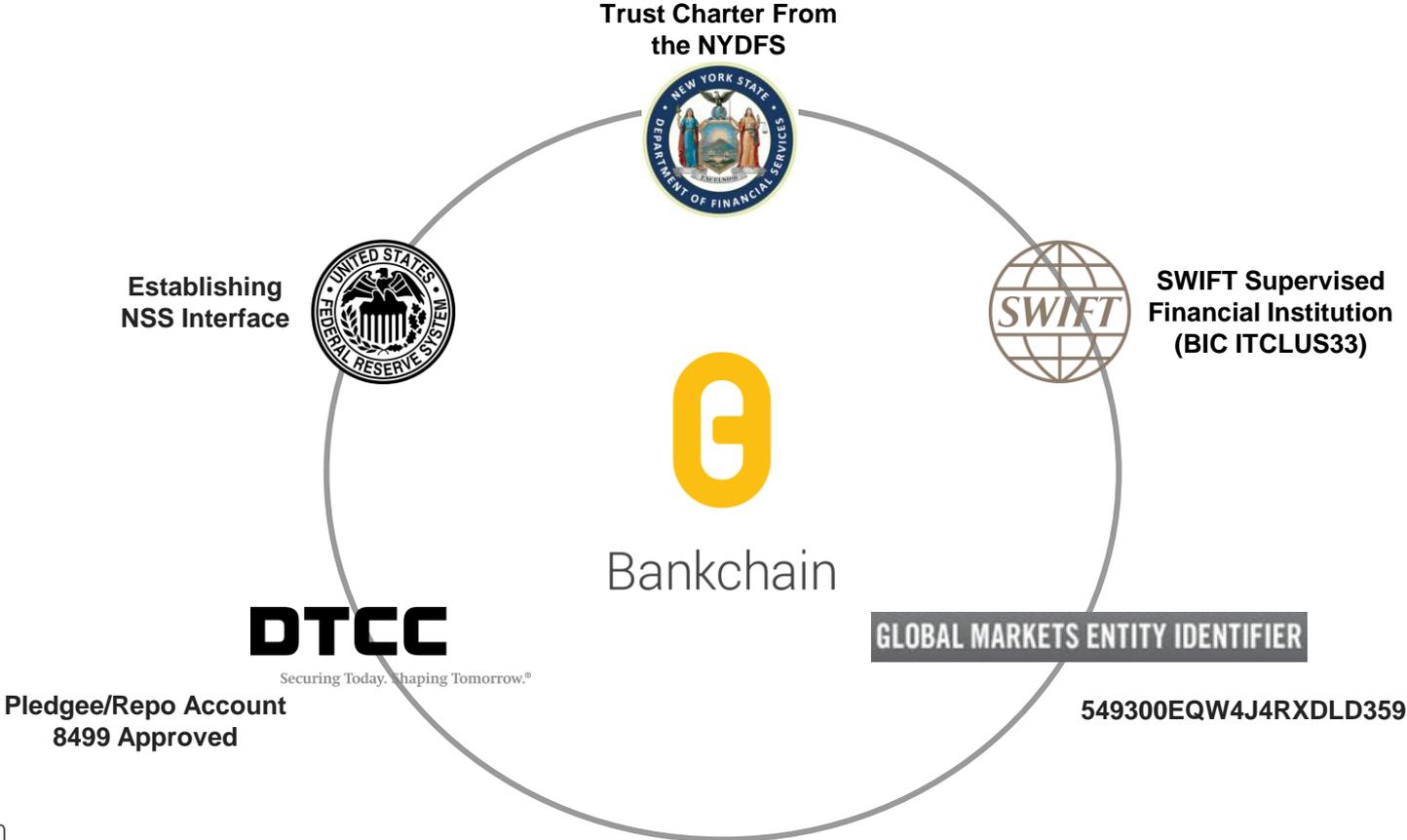T+0 Delivery-versus-Payment Settlement
for Gold and Listed Securities
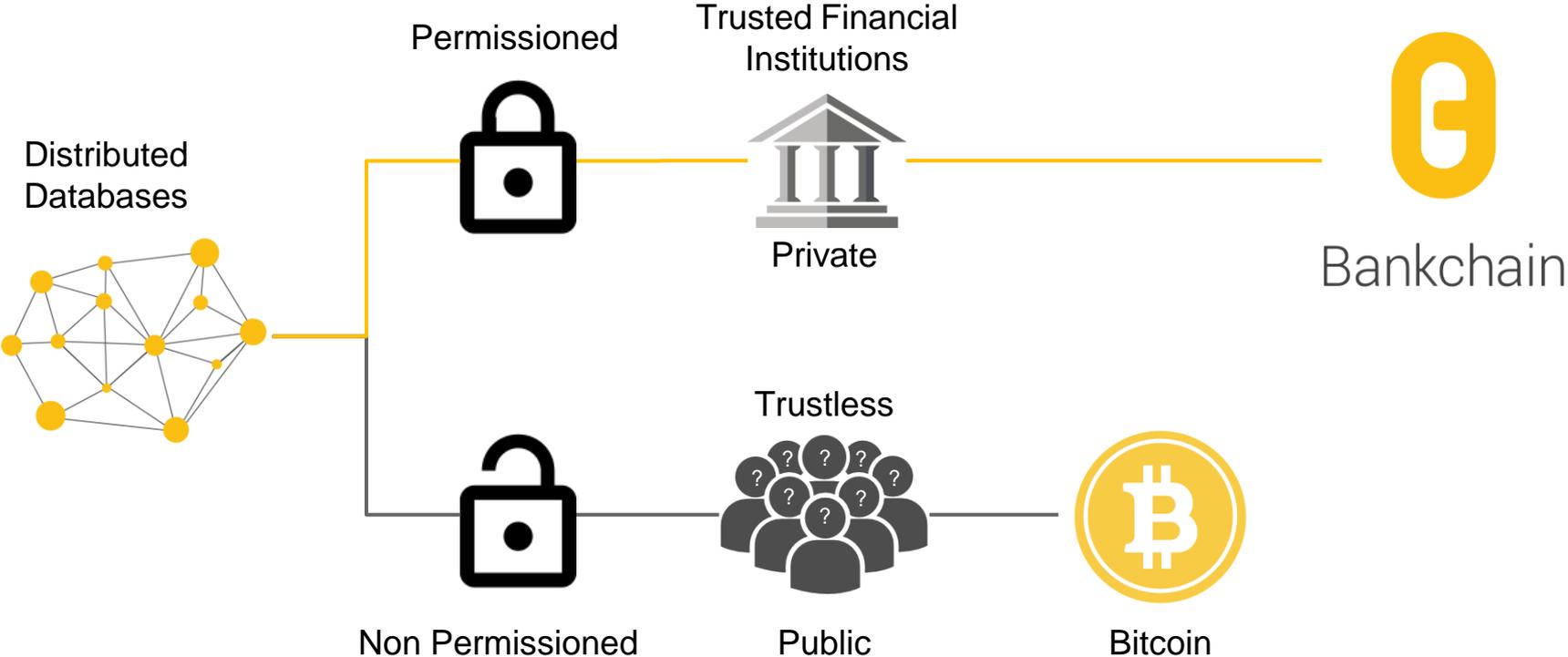
What is Bankchain?

Bankchain is a permissioned, distributed ledger, engineered specifically for financial institutions as the next generation post-trade platform.

- Verified, shared books and records amongst financial institutions
- Fault tolerant: multi-node, decentralized system
- Provides perfect asset provenance
- Removes need for multiple reconciliations

Bankchain

2

Bankchain's Regulated Infrastructure Connectivity

Trust Charter From the NYDFS

Establishing NSS Interface

SWIFT Supervised Financial Institution (BIC ITCLUS33)

Bankchain

Pledgee/Repo Account 8499 Approved

549300EQW4J4RXDLD359

Bankchain

Ledger Landscape

Distributed Databases

Permissioned

Trusted Financial Institutions

Private

Bankchain

Non Permissioned

Trustless

Public

Bitcoin

Architecture
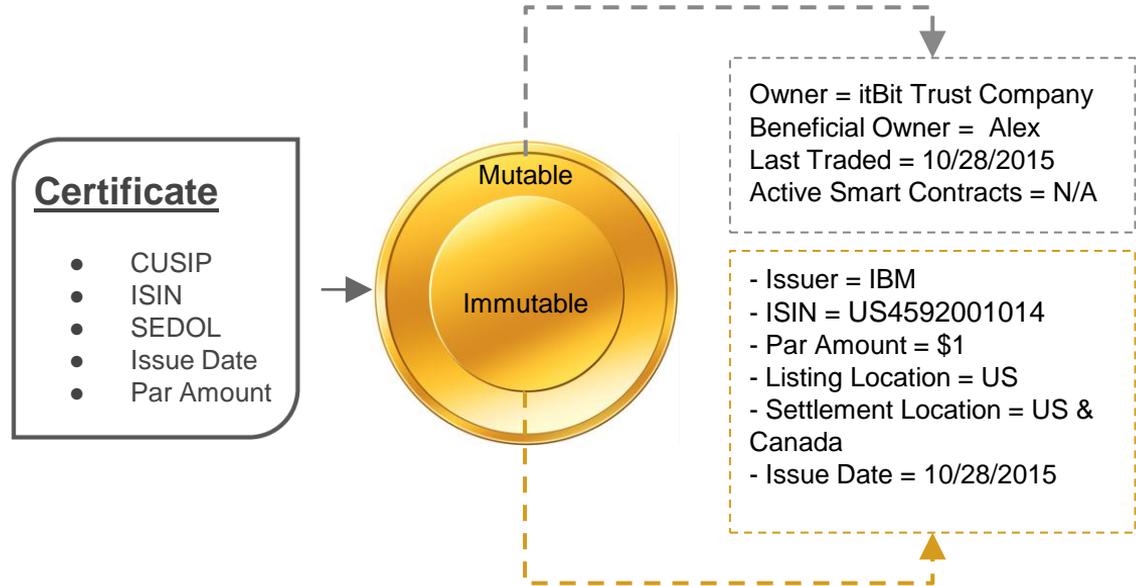
Bankchain's Native Tokens

Overview:

Tokens are digital representations of assets which convey a perfected interest in the underlying security.*

Primary Types:

- Asset Tokens
- Cash Notional Tokens

Characteristics:

- Enhanced Database Entries
- Valueless
- Unlimited

Certificate

- CUSIP
- ISIN
- SEDOL
- Issue Date
- Par Amount

Mutable

Immutable

Owner = itBit Trust Company
Beneficial Owner = Alex
Last Traded = 10/28/2015
Active Smart Contracts = N/A

- Issuer = IBM
- ISIN = US4592001014
- Par Amount = $1
- Listing Location = US
- Settlement Location = US & Canada
- Issue Date = 10/28/2015

Bankchain

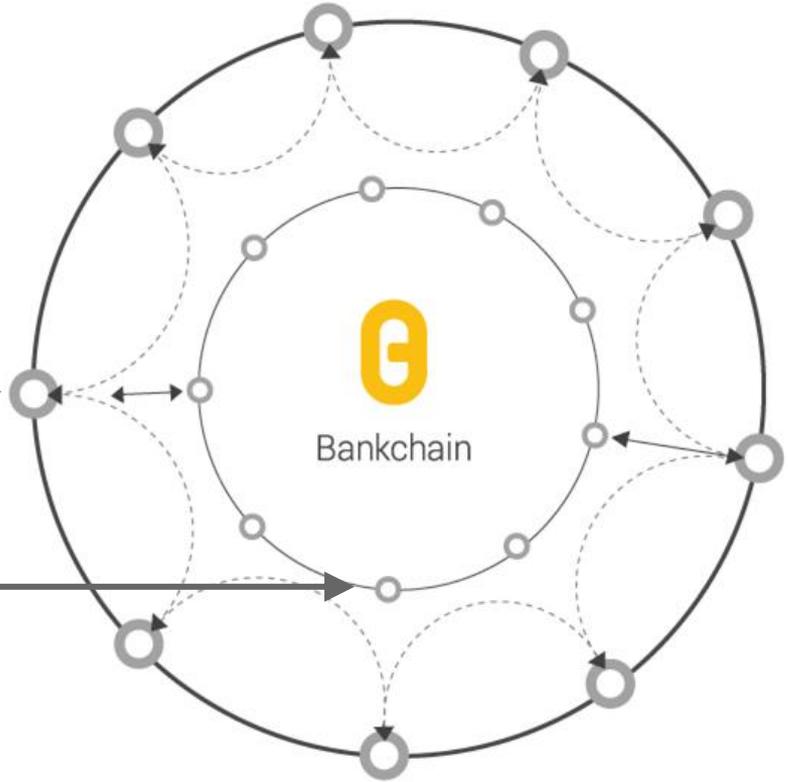* Legal Opinion via Cleary Gottlieb

6

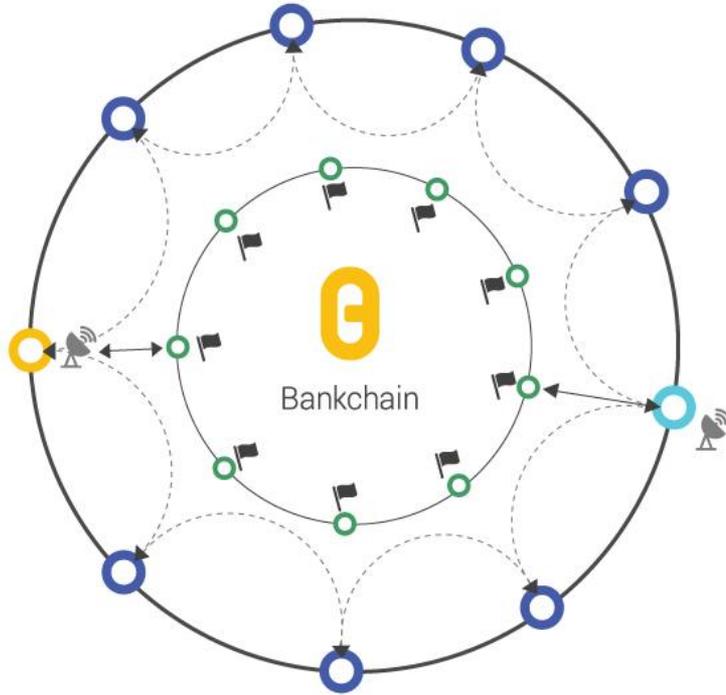# Messaging and Consensus

Messaging Layer

Clearing / Matching Trades
Fund Verification
Messaging
Netting

Consensus Layer

Performs consensus and adds
blocks to the chains in 30 second
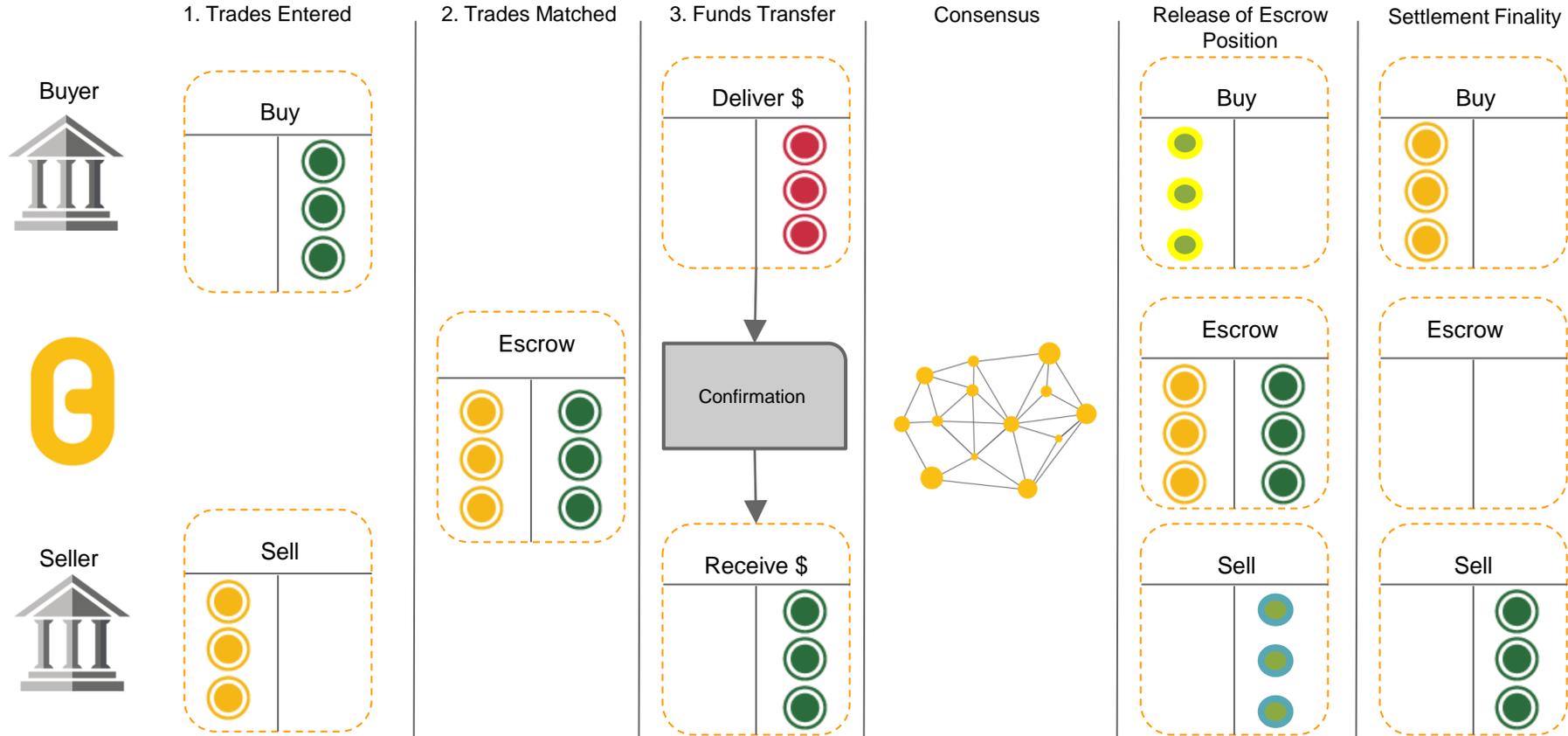intervals. Maintains ownership
states across the ledger.

Bankchain

Bankchain

7

Trade Validation (for OTC Transactions)
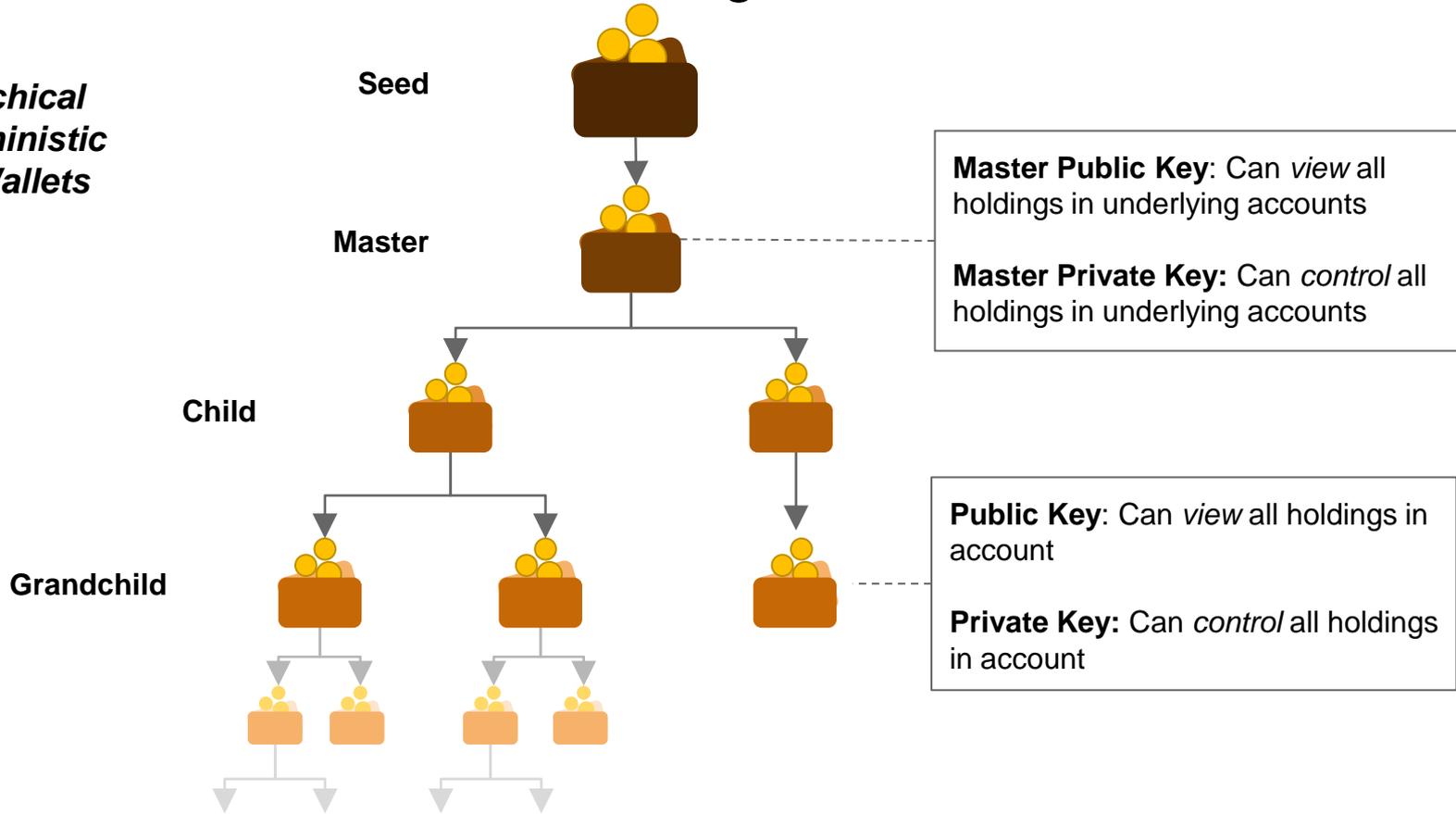

Node / Bankchain Activities

○ Transmits MT541/RvP (Buyer) - Encrypted Matching Instruction

○ Transmits MT543/DvP (Seller) - Encrypted Matching Instruction

⊘ No Matching Instructions

○○ Hash and Key Match

e Performs Key Field Matching and Balance Check

e Confirms Match (or Fail) via MT548 (Trade Status)

○○ Submit Confirmed Hash for Consensus

○ Bankchain Nodes Perform Consensus

e Transactions Posted to Bankchain

Bankchain

8

Settlement and Funding Flows

Next Generation Sub-Accounting

Hierarchical Deterministic (HD) Wallets

Seed

Master

Child

Grandchild

Master Public Key: Can *view* all holdings in underlying accounts

Master Private Key: Can *control* all holdings in underlying accounts

Public Key: Can *view* all holdings in account

Private Key: Can *control* all holdings in account

Bankchain

10

The Bankchain Advantage

- **Risk Mitigation and Next Generation Analytics**
  - Increased transparency
  - Regulatory adaptability
  - Stability via the distributed ledger system
  - Trusted network of permissioned participants
  - Full inventory control
  - Real-time credit tracking
  - Perfect asset provenance

- **Increased Speed & Improved Economics**
  - Integration and synchronization with participant platforms
  - Near instantaneous clearing and settlement
  - True Delivery vs Payment (DvP)
  - High level of automation through smart contracts
  - Promptly announced and synchronized corporate actions -- *revive initiatives to have issues use XBRL to tag corporate actions in prospectuses?   More on this later…*

Bankchain

11

Precious Metals

Current Market Landscape

- Wide recognition that infrastructure needs to be improved

- Concern about transparency / liquidity / cost: LBMA RFPs

- Potential for the fracturing of the market: WGC and other initiatives

- Our **proprietary RWA study**: for every $100 worth of an unallocated gold balance, a participant is charged approx. $1.20 for capital usage

- London's clearing and settlement service to global participants constricted by London business hours

- Buildout of competitive Asian infrastructure

- Departure of trading houses (Most recently Mitsui)

Bankchain

13

# Challenges to Today's Infrastructure

!

The cornerstone of London trading is unallocated gold which has a bifurcated settlement process with inherent risk:

- Large intraday credit exposure amongst clearers, between clearers and clients, and between market participants
- Inefficient balance sheet utilization
- Unallocated positions possibly irrecoverable in insolvency
- Settlement concentration risk: *what if a clearer fails?*
- Insufficient transparency
- Deutsche, Barclays exits

Bankchain

Features & Benefits of Precious Metals on Bankchain

FEATURES	BENEFITS
Automated DvP for the first time in the gold market	Risk reduction
Faster settlement times	Capital savings; better capital utilization
Automated clearing and settlement solutions for allocated and unallocated gold	Error reduction; Lower operational cost
Dematerialized Gold	Efficient use in collateral and financing

Bankchain

Envisaged Strategic Solution
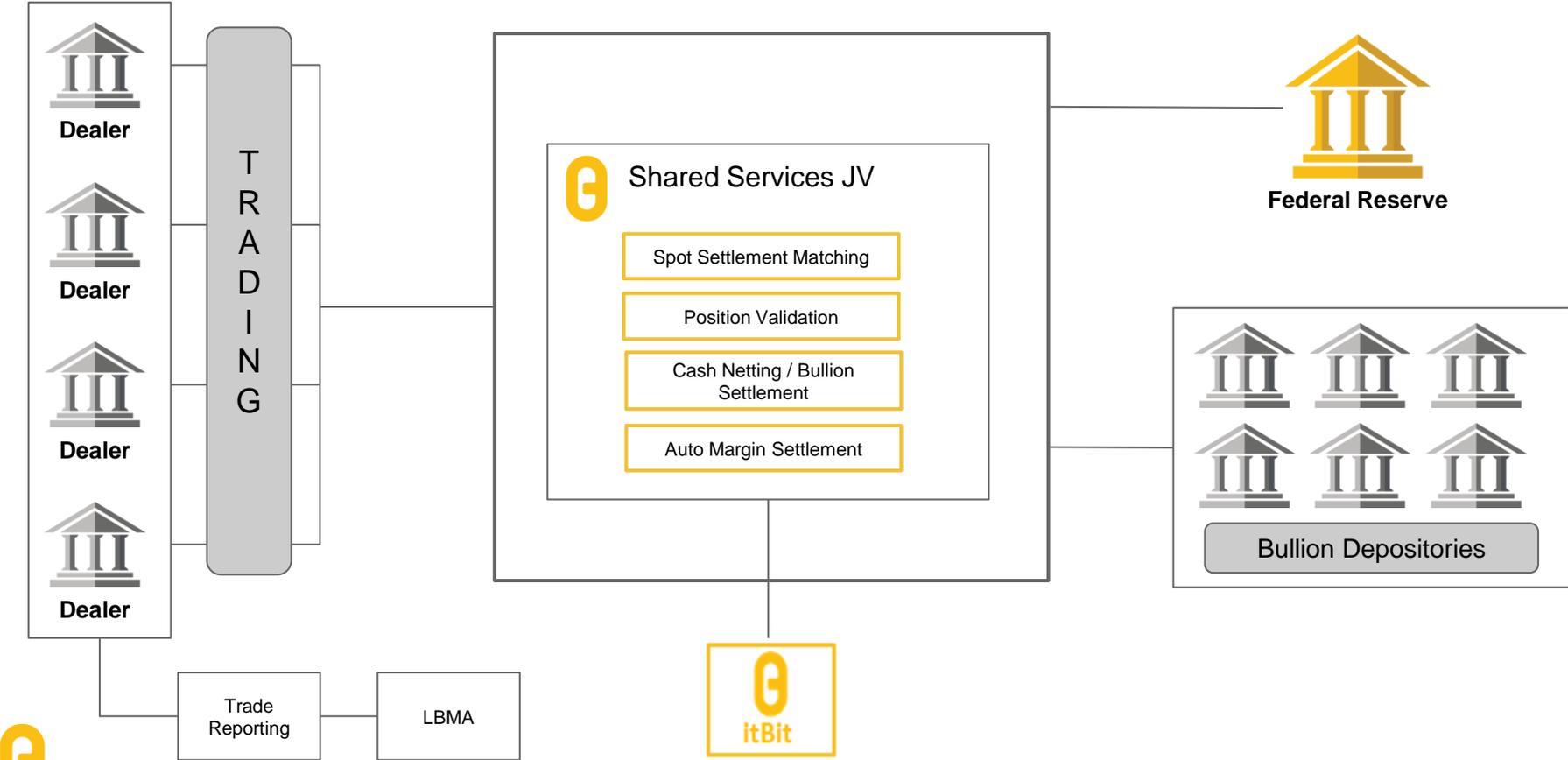
Allocated, Unallocated…or the best of *both?*

Our joint solution marries the best qualities of allocated and unallocated for the wholesale market

Allocated qualities

- Perfected ownership
- Use for collateral
- Use for liens
- Credit exposure to clearer eliminated
- Risk weighted asset (RWA) cost eliminated

Unallocated qualities

- Convenience of settling without a bar list
- Settle amounts different than bar sizes
- Speed and simplicity of settlement
- Reduced vaulting fees

Leveraging these best qualities will strengthen London as a clearing and settlement hub

Bankchain

Fractionalization

400 oz.of Gold Tokens

400 oz. of Gold Tokens
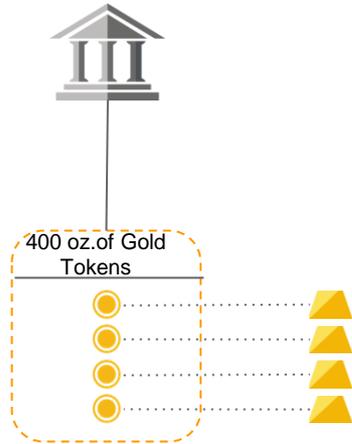
Intra-settlement cycle participants can own fractional positions in numerous gold bars
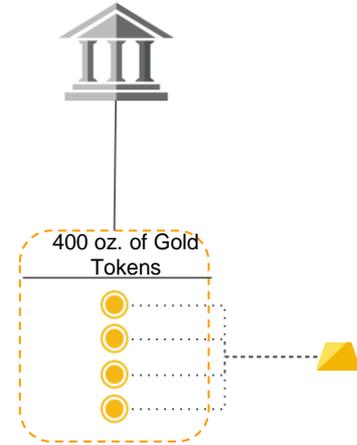
At the end of settlement cycle, the bars are reconstituted to consolidate positions back into whole bars

Bankchain

18

Reduction in Capital Charges

Bankchain will reduce/ eliminate credit risk capital charges associated with unallocated gold, increasing profit by ~1.2% of unallocated gold assets

Unallocated

Asset	Liability
$100 unallocated loan to dealer (RWA = 100%)	$100 unallocated deposit from customer
	Equity
	~$13 capital for unallocated gold

Bankchain

Asset	Liability
$100 allocated (RWA = 0%)	$100 allocated deposit from customer
	Equity
	~$0 capital for allocated gold

Reduction in capital charge improves profitability of gold

If a market participant extends $100mn in intraday credit to counterparties for unallocated gold processing, Bankchain could save $1.2M in capital charges

Bankchain

19

Future-Proofing of London Clearing

itBit proposes an evolution of traditional settlement by keeping key benefits, eliminating risky weaknesses, and adding potent attributes.

- Bankchain enables the market to trade with the ease of unallocated while settling with the safety of allocated.

- Our solution reflects the increasing preference for allocated storage in recent years, which addresses increasingly important credit and balance sheet concerns

- Allocated storage is approaching unallocated rates, minimizing friction between allocated and unallocated.

Bankchain

A Game Changer for the Front Office

Expand profitability through new relationships and products.

- Lower credit names that otherwise meet account opening standards can be serviced with Delivery vs. Payment (DvP) and same day settlement (T+0)

- Residual arbitrage positions from these trades provide "an ax to grind" with other clients - increasing trade velocity and profitability

- Revenue growth in other business units (Advisory, etc.) from these new relationships

- Solve for customer risk by innovating solutions using Bankchain tools

Bankchain

Next Generation Operational Efficiencies

- Risk reduction from DvP

- Errors swiftly identified at market level

- Significantly lower transaction costs

- Front and back office integration

- Real-time status of the settlement cycle

- Dynamic inventory and credit exposure management

- Simplified process of using gold as collateral, which will be useful as collateral needs arise

Bankchain

Opt-In T+0 Listed Securities

Listed Securities DVP on Bankchain

Overview:
Bankchain can provide near instant clearing and settlement for all listed securities by integrating the current financial infrastructure with next-generation distributed ledger technology.

Advantages:
- Near instantaneous settlement finality
- Increased liquidity
- Full automation
- Big data analytics

Bankchain

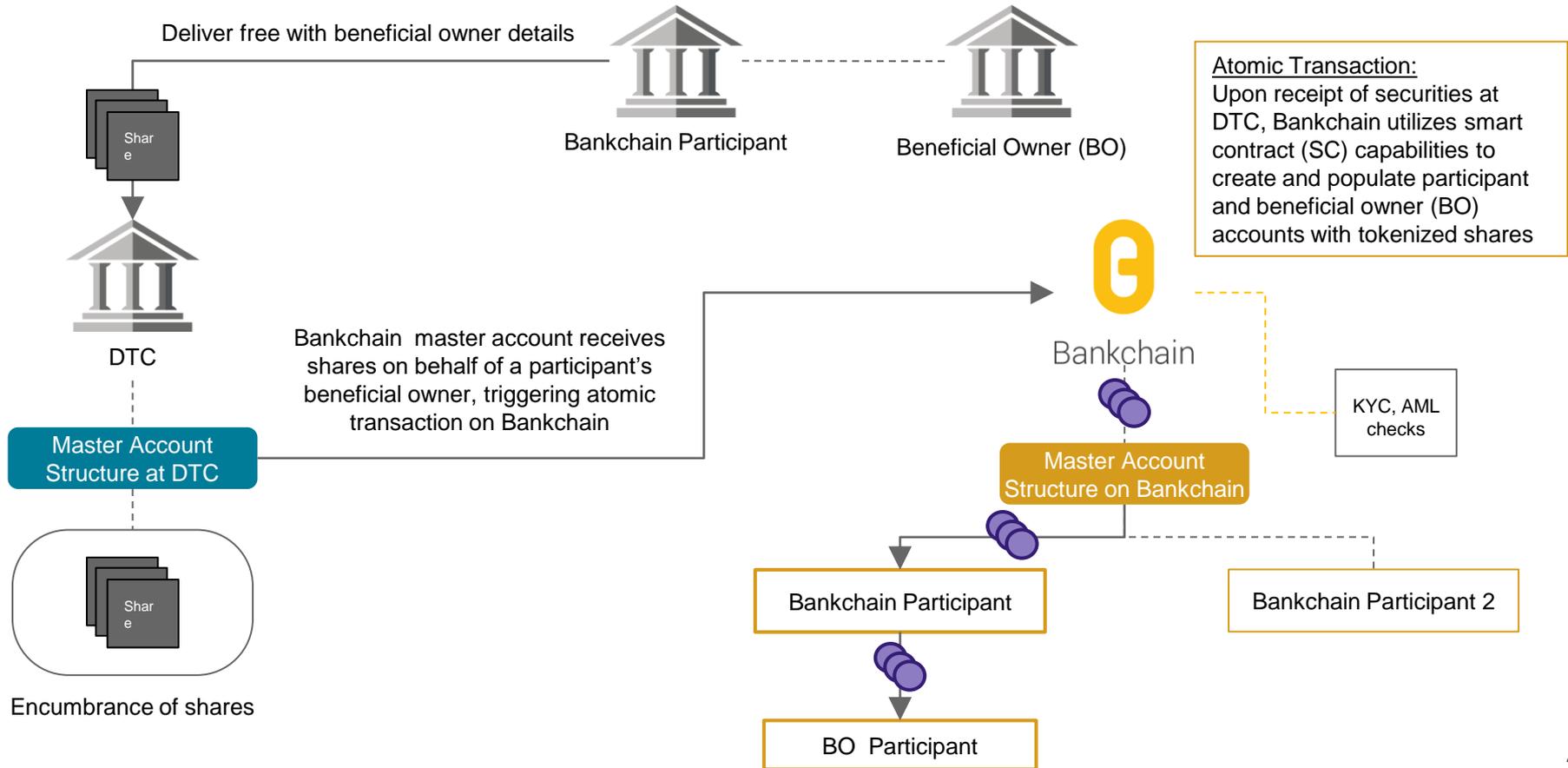# The Architecture of T+0

Achieving Same-Day Settlement

Bankchain offers participants T+0 via the use of "Master Account Structure". This new entity will be created within the DTC and designed to hold and manage listed securities. These securities will then be tokenized and traded on Bankchain.

In choosing to make use of the "Master Account Structure", participants would be opting into T+0. With this comes the advantages of:

- Same day settlement/DvP
- Automated allocation and corporate actions
- True beneficial owner level information

Participants would agree to meet the requirements of facilitating T+0 settlement.

Bankchain

Tokenization of Listed Securities

Deliver free with beneficial owner details

Bankchain Participant

Beneficial Owner (BO)

DTC

Bankchain master account receives shares on behalf of a participant's beneficial owner, triggering atomic transaction on Bankchain

Master Account Structure at DTC

Share

Encumbrance of shares

Atomic Transaction:
Upon receipt of securities at DTC, Bankchain utilizes smart contract (SC) capabilities to create and populate participant and beneficial owner (BO) accounts with tokenized shares

Bankchain

KYC, AML checks

Master Account Structure on Bankchain

Bankchain Participant

Bankchain Participant 2

BO Participant

26

Bankchain as a Settlement Location

Counterparty 1

Trades matched and agreed

Counterparty 2

T+3 settlement timeframe selected

Exchange

NSCC

Clearing

DTC

Bankchain

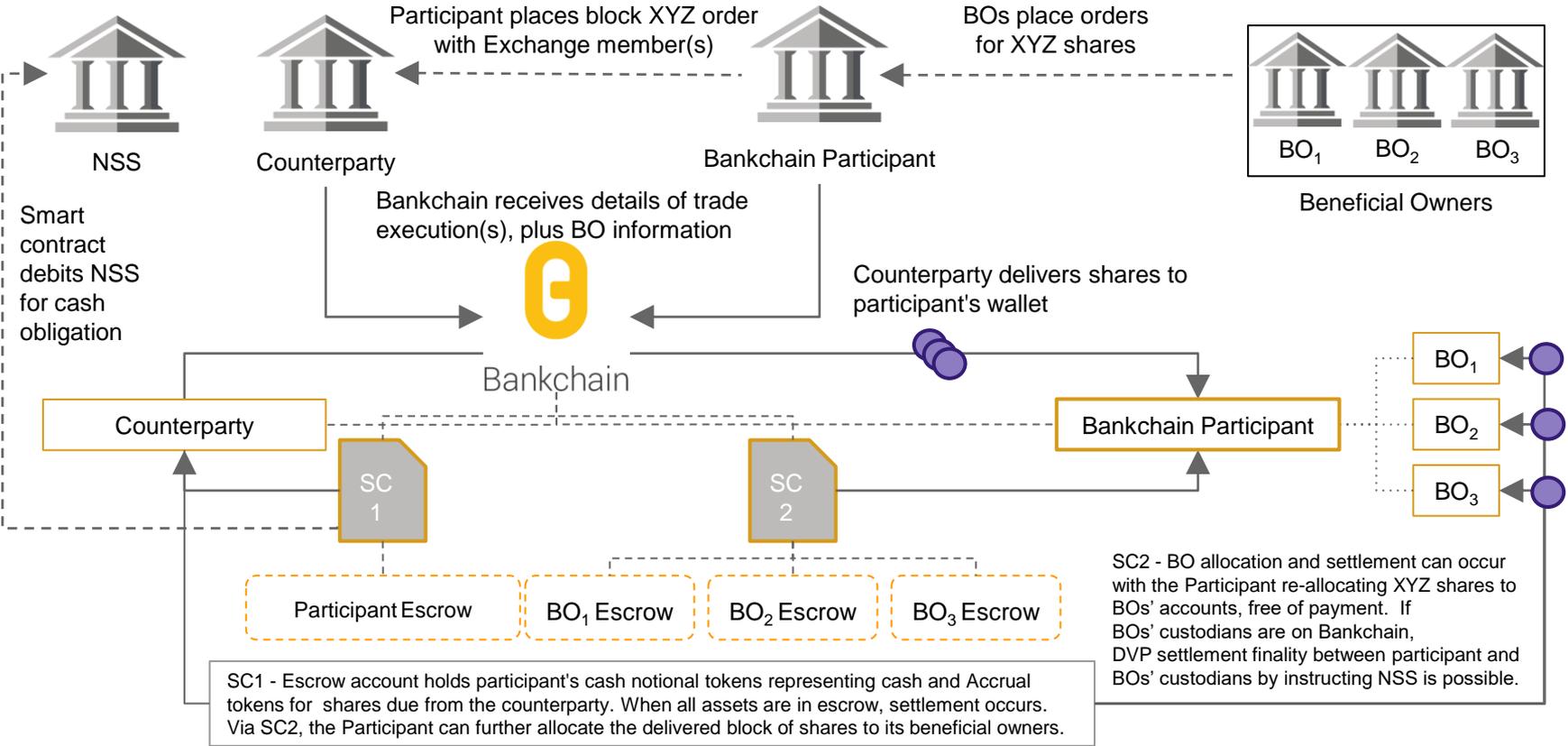T+0 settlement timeframe preferred

Legacy Processing

After market execution, matched trades are transmitted to NSCC using its Universal Trade Capture indicating "regular-way" T+3 settlement. Trades are recorded, novated, margined for NSCC Clearing Fund and guaranteed at end of T+1 (effectively T+2). Securities are multilaterally netted per issue per participant and instructed to DTC for securities settlement versus NSCC intraday cash ledger. Net NSCC cash ledger passes to DTC for renetting with the depository net settlement obligations in DTC's settlement file to the Fed's NSS, with end-of-day T+3 settlement finality.

Bankchain Straight-Through Processing

After market execution, matched trades are transmitted to NSCC using its Universal Trade Capture indicating T+0 settlement. NSCC records and passes trades to Bankchain for same-day DVP settlement. Bankchain instructs cash obligations via Fed NSS in frequent intervals (available up to 20.5 hours a day) to immediately settle Bankchain securities obligations with T+0 finality.

Bankchain

27
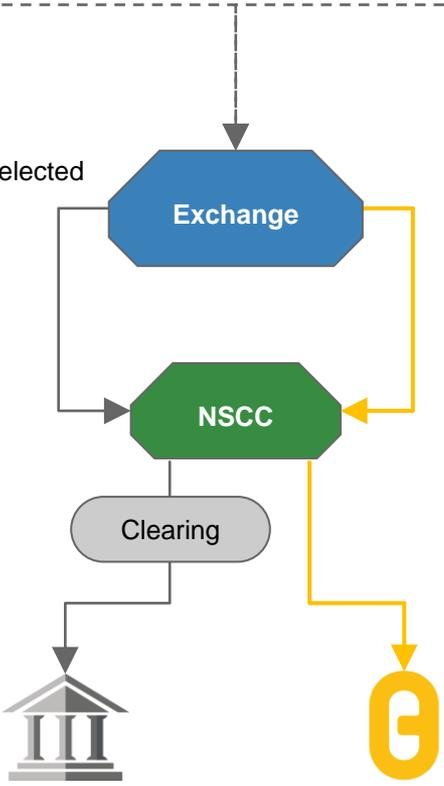
How the Trade is Made on Bankchain

Participant places block XYZ order with Exchange member(s)

BOs place orders for XYZ shares

NSS

Counterparty

Bankchain Participant

BO_1 BO_2 BO_3

Beneficial Owners

Smart contract debits NSS for cash obligation

Bankchain receives details of trade execution(s), plus BO information

Counterparty delivers shares to participant's wallet

Bankchain

Counterparty

Bankchain Participant

BO_1

BO_2

BO_3

SC 1

SC 2

Participant Escrow

BO_1 Escrow

BO_2 Escrow

BO_3 Escrow

SC2 - BO allocation and settlement can occur with the Participant re-allocating XYZ shares to BOs' accounts, free of payment. If BOs' custodians are on Bankchain, DVP settlement finality between participant and BOs' custodians by instructing NSS is possible.

SC1 - Escrow account holds participant's cash notional tokens representing cash and Accrual tokens for shares due from the counterparty. When all assets are in escrow, settlement occurs. Via SC2, the Participant can further allocate the delivered block of shares to its beneficial owners.

28

Why Use XBRL for Corporate Actions?

The Problem

"Losses on corporate actions worldwide were between $400 and $900 million U.S. dollars each year"

2006 study by the U.K. independent research firm Oxera

- Manual process
- Re-keying of data
- Time consuming
- Inefficient
- Significant financial impact

The XBRL Solution

DTCC, SWIFT and XBRL US are building a corporate actions XBRL taxonomy aligned with ISO 20022 repository elements

- Automates the process
- Eliminates re-keying
- Faster process
- More efficient process
- Reduces losses

Corporate Actions API via XBRL-Tagged ISO 20022?

BUSINESS STANDARDS

XBRL Standard

XBRL TAXONOMY (data dictionary, metadata)
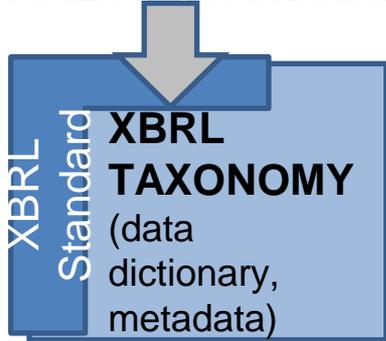
Examples:
IFRS, US GAAP, JP GAAP
UK HMRS, US FDIC,
US Corporate Actions

Features: machine readable, structured, comparable, analyzable, consistent, verifiable, usable data

Business Facts

XBRL Instance

=

Business Reports

INTERPRETATION

DATA

RE-ENTRY
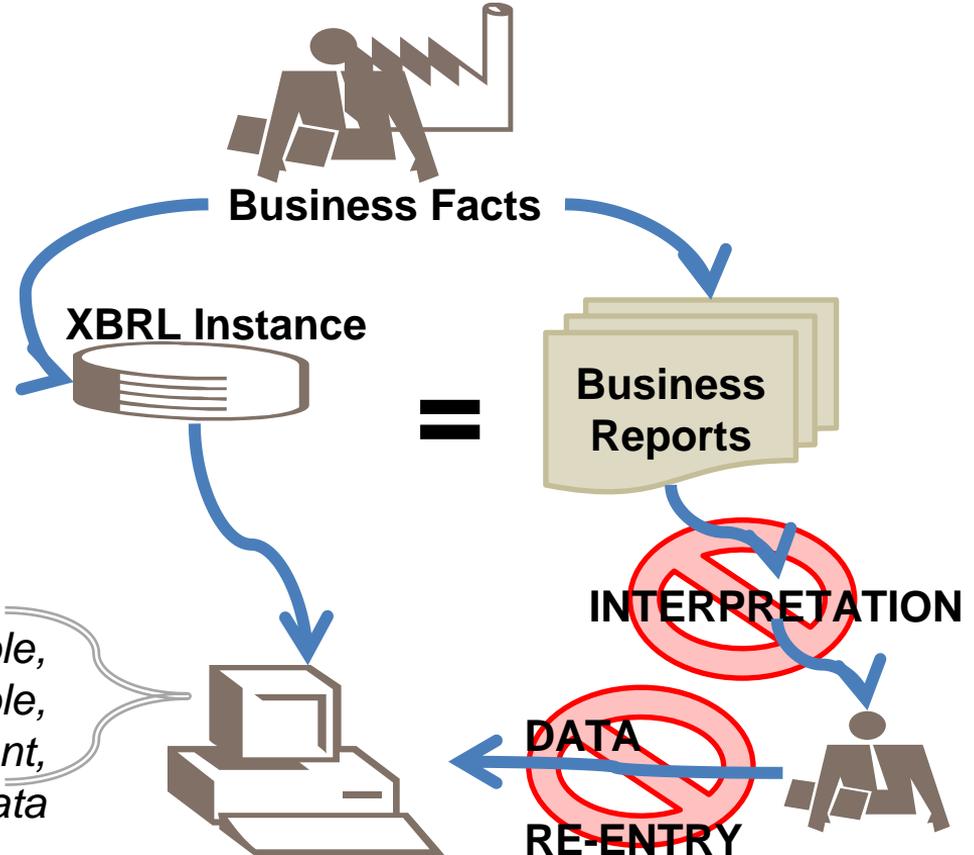
Bankchain will automate, accelerate and enhance post-trade processes across the financial services industry, saving institutions time and money.

Visit bankchain.com or contact us at bankchain@itbit.com to learn more.

Smart Contracts, Blockchain and Data Standards

APRIL 4, 2016 | NEW YORK CITY

Sponsoring organizations

BaruchCOLLEGE
ZICKLIN SCHOOL OF BUSINESS

CFA Institute

xBRL US

ConsenSys Blockchain Highlight Use Case: Ethereum Total Return Swap

James Slazas

– ConsenSys Head of Capital Markets

– James.Slazas@ConsenSys.net

Agenda

- Ethereum

- Ethereum eTRS/Collateral Management

  – Blockchain Core Components

  – Step by Step Demo

SMART CONTRACTS, BLOCKCHAIN AND DATA STANDARDS
April 4, 2016 | New York City
97 of 136
Sponsoring Organizations
BaruchCOLLEGE
ZICKLIN SCHOOL OF BUSINESS
CFA Institute
xBRL US

General Purpose Computer

There are **5 interacting technological elements that are common between the Bitcoin and Ethereum Protocols.**

1. Blockchain Data Structure = entire history of transactions

2. Cryptographic Tokens = bitcoin and ether

3. Peer 2 Peer Networks = every node is both a client and server

4. Consensus Forming Algorithm = 10 min and 15 seconds

5. A Turing Complete Virtual Machine
   a. A virtual machine enables programmable money in both Bitcoin and Ethereum plus decentralized applications on Ethereum.

SMART CONTRACTS, BLOCKCHAIN AND DATA STANDARDS
April 4, 2016 | New York City
Sponsoring Organizations
Baruch COLLEGE
ZICKLIN SCHOOL OF BUSINESS
CFA Institute
xBRL US
98 of 136

Ethereum = Smart Contracts

When we speak about smart contracts on the blockchain, we are talking about the Ethereum blockchain.

Bitcoin   transfers value

Ethereum   transfers value and enables non-specialist programmers to build decentralized applications (Smart Contracts) easily

programming digital money only to be spent on food

Ethereum's History

Jan 2009   Bitcoin blockchain released

Nov 2013   Vitalik Buterin releases the Ethereum blockchain White Paper

Jul 2014   Ethereum crowdsale raises $18M worth of BTC for development

Jul 2015   **Ethereum 1.0 launched, Genesis block created**

Jan 2016   40+ banking consortium used Ethereum to transfer digital assets

slide 5

Sponsoring Organizations
BaruchCOLLEGE
ZICKLIN SCHOOL OF BUSINESS

CFA Institute

xBRL US

7 Months After Launch…

Price:

~$12.50 (up from $0.30 at genesis sale)

Monetary base:
~ $1,000,000,000

2nd largest crypto currency

SMART CONTRACTS, BLOCKCHAIN AND DATA STANDARDS
April 4, 2016 | New York City

Sponsoring Organizations
BaruchCOLLEGE
ZICKLIN SCHOOL OF BUSINESS
CFA Institute
xBRL US

101 of 136

Types of Blockchains

PRIVATE ← → PUBLIC

ethereum

A Network

Permissionless Network

Permission less Network

A

B

C

D

Permissioned chain   Consortium chain   Permissionless chain

slide 7

SMART CONTRACTS, BLOCKCHAIN AND DATA STANDARDS
April 4, 2016 | New York City
Sponsoring Organizations
BaruchCOLLEGE ZICKLIN SCHOOL OF BUSINESS
CFA Institute
xBRL US

Technology Stack

// Application	BALANCE	DApps, Balanc3 Triple Entry Accounting, eTRS, eSign Smart Document and Mgt. Sys, Business Logic
// Core components	uport	**Wallet, Identity, Persona, Reputation, Registries, Token Issuance, Glue-BTC Relay, Token Issuance and Management Systems, EtherEx Token Exchange System (Native and Subtoken), Stable Token Systems**
// Interface		Tooling, Integrated Development Environments & Testbeds
// Infrastructure	BlockApps	Virtualized Network Node & API
// Blockchain	ethereum	**2 of 6 Ethereum Clients: Java and Haskell, Private Blockchains (ETH BaaS)**

Sponsoring Organizations
Baruch COLLEGE ZICKLIN SCHOOL OF BUSINESS
CFA Institute
xBRL US

Use Case: Core Components

- **uPort-Digital Identity**
  - Attributes-information controlled by individual
- **uPort-Reputation and Persona**
  - Attestations-information others have said of the individual
- **Oracles for Pricing and Reputation**
- **Balanc3-Triple Entry Accounting**
- **eSign-Smart Documentation Management**
- **Digital Assets**
- **Smart Contracts**
  - Business processes

Sponsoring Organizations

BaruchCOLLEGE
ZICKLIN SCHOOL OF BUSINESS

CFA Institute

xBRL US

slide 10

WELCOME NIGEL

uPort Public Address

0x58415ffcb3a993cc3c702af21b3cb356237caccb

1 Public Address

✔ AML/KYC Verified

2 Attribute: AML/KYC

4 Attestation: Reputation

Normalized Oracle Reputation

94/SD

3 Attribute: Regulatory Swap Dealer

INPUT CONTRACT TERMS »

CONTRACT TERMS

Please enter TRS

slide 12

CONTRACT TERMS

Please enter TRS terms below

1 Canonical Name

Global Reputation Score: 79/FEU

Counterparty B Macy Hawkins

Notional Amount (USD) $ 10000000

Term (minutes) 4

2 Asset Class Sensitivity

Underlying Asset Long	Underlying Asset Short
MSFT	GOLD
SPOT PRICE ORACLE 53.53	SPOT PRICE ORACLE 1069.35

3 SC Collateral Formula

Counterparty B Collateral % 12.000 *

5 Blockchain Asset Account

Counterparty B Blockchain Asset Account 3,000,000

Collateral % 5.000 *

Blockchain Asset Account 2,500,000

Special Terms Reputation Credit ▾

4 SC Business Process; Reputation

* Special Terms - Reputation Credit: each 5 point reduction in reputation will increase collateral required by 5%

SMART CONTRACTS, BLOCKCHAIN AND DATA STANDARDS
April 4, 2016 | New York City

Sponsoring Organizations
Baruch COLLEGE ZICKLIN SCHOOL OF BUSINESS   CFA Institute   XBRL US

SMART CONTRACT

The counterparties agree to the following:

Nigel Woolworth

NOTIONAL AMOUNT	$10,000,000
POSITION	MSFT / Gold
REQUIRED COLLATERAL AMOUNT	$500,000 NOT FUNDED
BLOCKCHAIN ASSET ACCOUNT	$2,500,000

1 Unfunded Collateral

Macy Hawkins

NOTIONAL AMOUNT	$10,000,000
POSITION	Gold / MSFT
REQUIRED COLLATERAL AMOUNT	$1,200,000 NOT FUNDED
BLOCKCHAIN ASSET ACCOUNT	$3,000,000

SPOT PRICE

MSFT : 53.52

Gold : 1069.43

SWAP TERM

4 minutes

NEXT STEPS:

FUND COLLATERAL ACCOUNT

Upload ISDA/CSA File

ESIGN CONTRACT

SEND TO COUNTERPARTY

When both parties have E-Signed & funded collateral,
Balanc3 will send confirmation and
swap will begin.

slide 14

SMART CONTRACTS, BLOCKCHAIN AND DATA STANDARDS
April 4, 2016 | New York City
109 of 136

Sponsoring Organizations
BaruchCOLLEGE
ZICKLIN SCHOOL OF BUSINESS
CFA Institute
XBRL US

SMART CONTRACT

The counterparties agree to the following:

Nigel Woolworth

NOTIONAL AMOUNT	$10,000,000
POSITION	MSFT / Gold
REQUIRED COLLATERAL AMOUNT	$500,000 FUNDED
BLOCKCHAIN ASSET ACCOUNT	$2,000,000

Macy Hawkins

NOTIONAL AMOUNT	$10,000,000
POSITION	Gold / MSFT
REQUIRED COLLATERAL AMOUNT	$1,200,000 NOT FUNDED
BLOCKCHAIN ASSET ACCOUNT	$3,000,000

1b Funded Collateral

SPOT PRICE

MSFT : 53.60

Gold : 1067.91

SWAP TERM

4 minutes

NEXT STEPS:

1a Fund Collateral

2 IPFS: ISDA, CSA, Confirmation

FUND COLLATERAL ACCOUNT — ✔ FUNDED

Upload ISDA/CSA File — ✔ IPFS HASH: QMC5TERVUVK9YPUNMKKZ7KUD55EFY5Q2SKZWCJHITBF1LJ

3 eSign

ESIGN CONTRACT — ✔ SIGNED IPFS DOCUMENT

4 Send to CP

SEND TO COUNTERPARTY — ✔ SENT TO COUNTERPARTY

5 Balanc3

When both parties have E-Signed & funded collateral, Balanc3 will send confirmation and swap will begin.

le 15

slide 16

SMART CONTRACTS, BLOCKCHAIN AND DATA STANDARDS
April 4, 2016 | New York City

Sponsoring Organizations
BaruchCOLLEGE
ZICKLIN SCHOOL OF BUSINESS
CFA Institute
xBRL US

slide 17

Use Case Benefits

- Next Generation IT Security

- Cost Reduction of AML/KYC

- Counterparty and Internal Risk Reduction

- Trade and Settlement T+0

- Efficient Capital Deployment

- Automated Collateral Re-balancing

- Regulatory Adherence

- Transparency and Immutability

James Slazas
james.slazas@consensys.net

Sponsoring Organizations
BaruchCOLLEGE
ZICKLIN SCHOOL OF BUSINESS
CFA Institute
xBRL US

Sponsoring organizations

Baruch COLLEGE
ZICKLIN SCHOOL OF BUSINESS

CFA Institute

xBRL US

James Allen, CFA, Head of Capital Markets Policy for CFA Institute

Blockchain Industry Panel Discussion

- Steve Wager, EVP, Operations and Development, ItBit

- James Slazas, CFO, Consensys

- Alex Zinder, Senior Director, Corporate Solutions Technology, Nasdaq

Smart Contracts

Smart Contract Fundamentals

Smart Contracts

A smart contract is a programmatically enforceable arrangement in which the contractual clauses are written in code rather than legal-ese

- Predetermined logic

- Typically replicated across a distributed ledger

- Removes the need for trust

- Automated / self executing

Bankchain | **markit**

3

Example

Bankchain | markit

4

Example

Bankchain | markit®
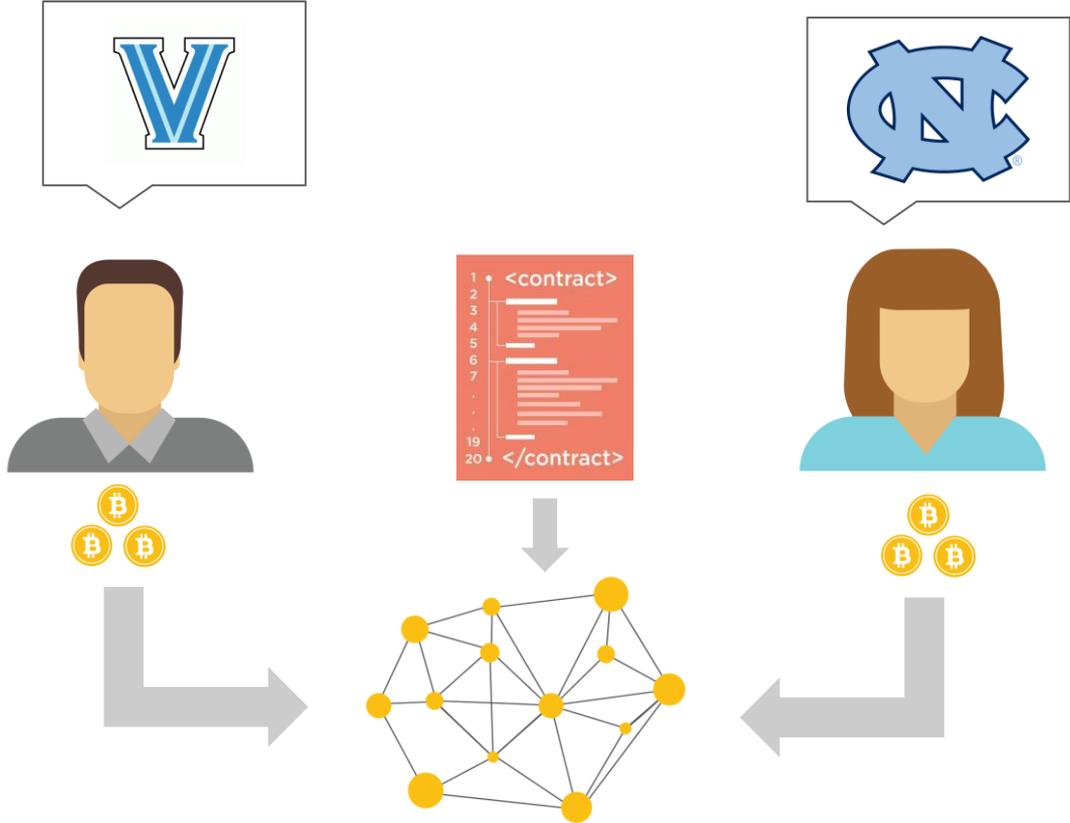
Why Smart Contracts

Safety

- Removes the need to trust your counterparty or escrow agent
- Ability to verify contract code
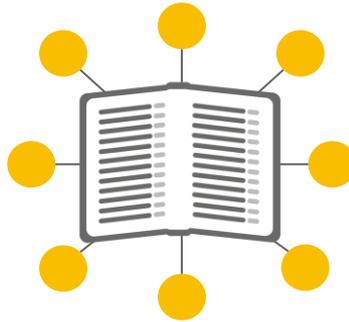
Replicability

- Code execution is absolute
- Contracts are no longer up for interpretation amongst parties

Agility

- Removes reconciliation latency
- Can execute contractual clauses in real time

Bankchain | markit

Smart Contracts vs Automation

- Guarantees the terms of an agreement

- Maintains full control of the asset

- Primarily used today to enter into agreements with untrusted counterparties
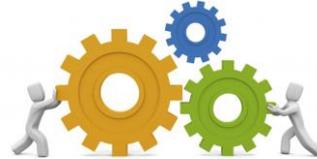
- The use of programs / scripts to reduce the need of human input

- Does not provide a guarantee of a transaction

7

How Smart Contracts Work

Bankchain | markit

Example Smart Contract on a Blockchain

Bankchain | markit®

9

Applications in Financial Services

Oil Options Contract

- Margining

- Automatic Exercise

- Executed on a decentralised basis

Repo

- Enforces pre arranged collateral schedule

- Ensures compliance
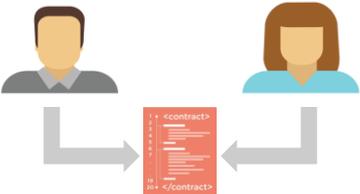
- Provides DvP

- Automates contract logistics

Reference Data

Code / Logic

STOCK

Bankchain | markit

12

Data Standards

Bankchain | markit
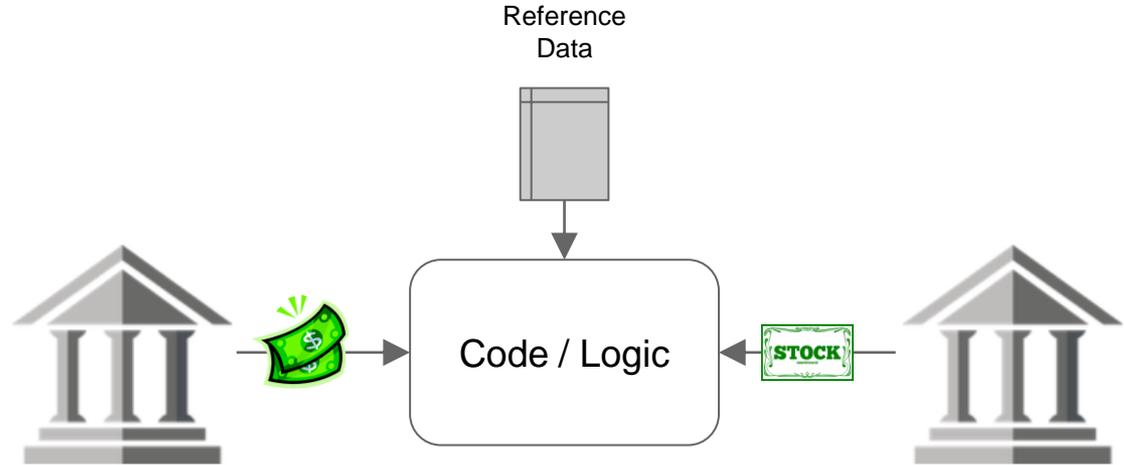
Reference Data / Oracles

Most smart contracts rely upon oracles for external data in order to execute upon their programming
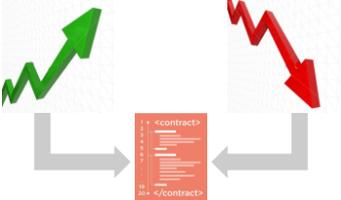
Bankchain | markit
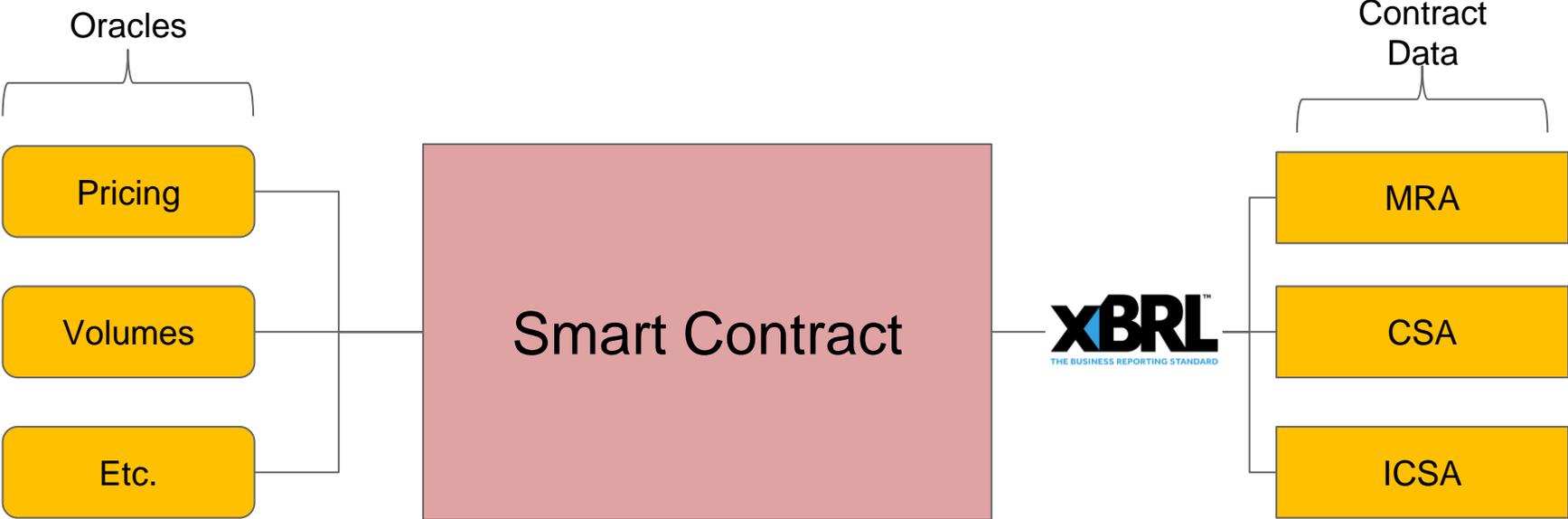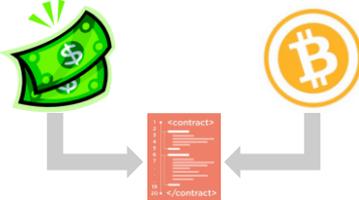
Defining Contract Components

Peer Transactions

Transactions that are initiated by one or more parties to a contract

Market Transactions

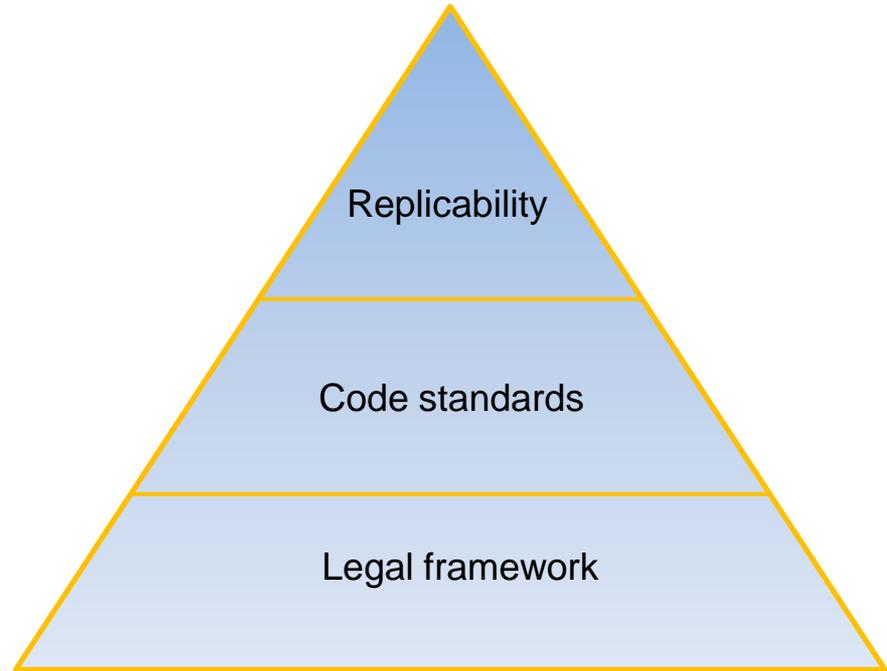Transactions that are unanticipated and change contract characteristics

Asset Transactions

Transactions that are future-dated and anticipated but discretionary

Bankchain | markit

15

Risks / Outstanding Issues

Smart Contract Code Hierarchy

Replicability depends on code standards, and code standards depend on a legal framework.

Bankchain | markit

Risks and Outstanding Issues

- Smart Contracts: a runaway train?
  - Gate checks
  - Optionality
  - Reversibility

- Who sees what?
  - Information secrecy
  - Data privacy
  - Counterparty validation

- Who controls the assets?
  - Managing collateral
  - Managing credit
  - Fungibility of assets

Bankchain | markit

Future of Smart Contracting

Bankchain | **markit**

Future of Smart Contracting

Digital Assets

Digital Currencies

Internet of Things

Bankchain | markit

20

Questions

Bankchain | markit