Smart Contracts, Blockchain and Data Standards

April 4, 2016 | New York City

- Campell Pryde, President and CEO, XBRL US
- John Turner, CEO, XBRL International
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: 18bdsW2XFibQKk1yFmk718TeZPAb03aUeN)

• 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

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

The contract lays dormant with custody of the funds
Example: Simple Bet

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

A: Y  |  B: RS

getWinner()  🔴  🔴

Win: RS

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 acceptor;
  address penaltyCollector;
  uint8 reportHash;
  bool accepted;

  function QuarterlyReport(address accountableSignatory, address acceptor, address penaltyCollector, uint _penaltyEscrow) {
    accountableSignatory = _accountableSignatory;
    acceptor = _acceptor;
    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(uint8 _reportHash) {
    if(this.balance > penaltyEscrow || msg.sender != accountableSignatory
      || frozen == true) {
      return;
    }
    reportHash = _reportHash;
  }

  function freezeSubmissions() {
    if(msg.sender != acceptor) {
      return;
    }
    frozen = true;
  }

  function acceptReport() {
    if(msg.sender != acceptor || frozen != true) {
      return;
    }
    accountableSignatory.send(penaltyEscrow);
    accepted = true;
  }

  function rejectReport() {
    if(msg.sender != acceptor || 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? 😊
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 Funding Climate

Philip Moyer,
Managing Director Safeguard Scientifcics
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


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
Blockchain Funding Market

Over $1B in Blockchain Deals

**Institutional Investors**

- 177 Unique Investors
- Top 10 Most Active Blockchain Investors

<table>
<thead>
<tr>
<th>Investor</th>
<th>Deals</th>
</tr>
</thead>
<tbody>
<tr>
<td>Digital Currency Group</td>
<td>14</td>
</tr>
<tr>
<td>Blockchain Capital</td>
<td>8</td>
</tr>
<tr>
<td>Plug and Play Ventures</td>
<td>7</td>
</tr>
<tr>
<td>Pantera Capital</td>
<td>5</td>
</tr>
<tr>
<td>500 Startups</td>
<td>4</td>
</tr>
<tr>
<td>AME Cloud Ventures</td>
<td>4</td>
</tr>
<tr>
<td>Khosla Ventures</td>
<td>4</td>
</tr>
<tr>
<td>RRE Ventures</td>
<td>3</td>
</tr>
<tr>
<td>Coinsilium</td>
<td>3</td>
</tr>
<tr>
<td>SV Angel</td>
<td>3</td>
</tr>
</tbody>
</table>

**Corporate Investors**


**Global # of Deals**

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

Data Sourced From: VentureSource, Crunchbase
We are in the infrastructure build-out phase...
## Examples of Large Blockchain Deals

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

Data Sourced From: VentureSource, Crunchbase
Blockchain Presentations

- Nasdaq Linq for Private Securities Issuance
- ItBit Bankchain for Gold & Corporate Actions
- Ethereum Total Return Swap (eTRS)
THE INFLUENCE OF TECHNOLOGY AND RISK ON CAPITAL MARKETS STRUCTURES

- Brief History
- Current State
- Blockchain in the mix
- Linq
1960 - 1970
PAPER WORK CRISIS

1968
Centralized Securities Depository created to facilitate immobilization

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

1969
Arthur Little Study: nationwide clearance and settlement system

1970
BASIC advocates for Central Securities Depository System

1970
CCS -> DTC
American Stock Exchange joins CCS

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

1980-1990
DTC mergers and acquisitions

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

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 Financial Sector

FUTURE
Markets Everywhere
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

- Physical Bearer Tokens
- Gift Card
- One Dollar Chip

Digital Bearer Tokens

- Bitcoin: Exists
- Currencies
- Securities: Emerging
- Commercial IOUs
- Brand/Loyalty Points
- Etc..

Source: chain.com
WHERE DIGITAL ASSETS GET THEIR VALUE

Central Bank

Central Bank

Institutions

Institutions

Blockchain

Blockchain

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.

All transactions are enabled and secured by **cryptography**.
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
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.
## Key Financing Events

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

<table>
<thead>
<tr>
<th>Total Shares To Buy</th>
<th>Total Shares To Sell</th>
<th>Total Shares Matched</th>
<th>Total Shares Unmatched</th>
<th>Imbalance Side</th>
<th>Imbalance Shares</th>
</tr>
</thead>
<tbody>
<tr>
<td>1,750,000</td>
<td>1,537,753</td>
<td>1,537,753</td>
<td>212,247</td>
<td>Buy</td>
<td>212,247</td>
</tr>
</tbody>
</table>

### Buyers
3 buying 1,750,000 shares

<table>
<thead>
<tr>
<th>Order</th>
<th>Date</th>
<th>Participant</th>
<th>Order Size</th>
<th>Price</th>
<th>Match Size</th>
<th>Special</th>
</tr>
</thead>
<tbody>
<tr>
<td>386</td>
<td>2016-3-4</td>
<td>GRAMMAR BIO-MEDICAL GROUP</td>
<td>900,000</td>
<td>$10.00</td>
<td>900000</td>
<td></td>
</tr>
<tr>
<td>388</td>
<td>2016-3-4</td>
<td>CALTEGRIS FUTURES INC</td>
<td>800,000</td>
<td>$14.00</td>
<td>300000</td>
<td></td>
</tr>
<tr>
<td>387</td>
<td>2016-3-4</td>
<td>BLACKGEM INC</td>
<td>500,000</td>
<td>$18.00</td>
<td>337533</td>
<td></td>
</tr>
</tbody>
</table>

### Sellers
13 selling 1,537,753 shares

<table>
<thead>
<tr>
<th>Order</th>
<th>Date</th>
<th>Participant</th>
<th>Order Size</th>
<th>Price</th>
<th>Match Size</th>
<th>Special</th>
</tr>
</thead>
<tbody>
<tr>
<td>338</td>
<td>2016-3-4</td>
<td>VIC FONTAINE</td>
<td>17,304</td>
<td>$9.00</td>
<td>17304</td>
<td></td>
</tr>
<tr>
<td>339</td>
<td>2016-3-4</td>
<td>WINN ADAMI</td>
<td>22,011</td>
<td>$9.00</td>
<td>22011</td>
<td></td>
</tr>
<tr>
<td>340</td>
<td>2016-3-4</td>
<td>WILLIAM ROSS</td>
<td>17,560</td>
<td>$9.00</td>
<td>17560</td>
<td></td>
</tr>
<tr>
<td>333</td>
<td>2016-3-4</td>
<td>DODI</td>
<td>5,220</td>
<td>$8.00</td>
<td>3220</td>
<td></td>
</tr>
<tr>
<td>332</td>
<td>2016-3-4</td>
<td>BRUNT</td>
<td>43,332</td>
<td>$9.00</td>
<td>43332</td>
<td></td>
</tr>
<tr>
<td>339</td>
<td>2016-3-4</td>
<td>EZRI DAX</td>
<td>17,268</td>
<td>$9.00</td>
<td>17268</td>
<td></td>
</tr>
<tr>
<td>333</td>
<td>2016-3-4</td>
<td>ISHEK</td>
<td>7,081</td>
<td>$10.00</td>
<td>7081</td>
<td></td>
</tr>
<tr>
<td>344</td>
<td>2016-3-4</td>
<td>WORF, SON OF MOGH</td>
<td>48,255</td>
<td>$10.00</td>
<td>48255</td>
<td></td>
</tr>
<tr>
<td>335</td>
<td>2016-3-4</td>
<td>JADZIA DAX</td>
<td>14,377</td>
<td>$10.00</td>
<td>14377</td>
<td></td>
</tr>
<tr>
<td>324</td>
<td>2016-3-4</td>
<td>DUKEAT</td>
<td>500,000</td>
<td>$10.50</td>
<td>500000</td>
<td></td>
</tr>
<tr>
<td>325</td>
<td>2016-3-4</td>
<td>WEYOUN</td>
<td>150,000</td>
<td>$10.50</td>
<td>150000</td>
<td></td>
</tr>
</tbody>
</table>
TRANSACTION EXECUTION

A SINGLE BLOCKCHAIN TRANSACTION REPRESENTS A MANY-TO-MANY TRANSFER
TRANSACTION EXECUTION
COMPLETE TRANSACTION-BASED AUDIT TRAIL AND CHAIN OF CUSTODY

VICTORIA FONTAINE 79,897 SERIES B SHARES
WINN ADAMI 22,011 SERIES B SHARES
WILLIAM ROSS 17,560 SERIES B SHARES
ODO 5,220 SERIES B SHARES
BRUNT 48,332 SERIES B SHARES
EZRI DAX 17,263 SERIES B SHARES
ISHKA 7,031 SERIES B SHARES
WORF, SON OF MOGH 48,253 SERIES B SHARES

DUKAT 2,055,109 SERIES B SHARES
WEYOUN 27,688 SERIES B SHARES
GOWRON 32,225 SERIES B SHARES
MICHAEL EDDINGTON 26,656 SERIES B SHARES
GRAMMAR BIO-MEDICAL GROUP 900,000 SERIES B SHARES
CALTEGRIS FUTURES INC 300,000 SERIES B SHARES
BLACKGEM INC 337,758 SERIES B SHARES
INVESTOR VISIBILITY

Leeta

Investor

466.6k Shares
1 Certificates

<table>
<thead>
<tr>
<th>CLASS</th>
<th>SHARES</th>
<th>PRICE</th>
<th>AMT. INVESTED</th>
</tr>
</thead>
<tbody>
<tr>
<td>COMMON CLASS</td>
<td>466,667</td>
<td>$0.000001</td>
<td>$0.47</td>
</tr>
<tr>
<td>TOTAL</td>
<td>466,667</td>
<td></td>
<td>$0.47</td>
</tr>
</tbody>
</table>
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.

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 PRECEDENCES, 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

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 RESTATEFIRST REFUSAL AND CO-SALE AGREEMENT

This SECOND AMENDED AND RESTATEFIRST 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”).

WITNESSETH:

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

WHEREAS, the Company, the Common Holders and the Existing Investors wish to

NASDAQ
Given the platform capabilities, Linq can become the foundation to support a wide variety of asset types and market structures.
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’s Regulated Infrastructure Connectivity

Trust Charter From the NYDFS

Establishing NSS Interface

SWIFT Supervised Financial Institution (BIC ITCLUS33)

Pledgee/Repo Account 8499 Approved

GLOBAL MARKETS ENTITY IDENTIFIER 549300EQW4J4RXDLD359
Ledger Landscape

Distributed Databases

Permissioned

Trusted Financial Institutions

Private

Trustless

Non Permissioned

Public

Bitcoin

Bankchain
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

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

* Legal Opinion via Cleary Gottlieb
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.
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
  - Performs Key Field Matching and Balance Check
  - Confirms Match (or Fail) via MT548 (Trade Status)
- Submit Confirmed Hash for Consensus
- Bankchain Nodes Perform Consensus
- Transactions Posted to Bankchain
Settlement and Funding Flows

1. Trades Entered

Buyer

Buy

Seller

Sell

2. Trades Matched

Escrow

3. Funds Transfer

Deliver $

Receive $

Confirmation

4. Creating DvP

Consensus

Release of Escrow Position

Settlement Finality

Buy

Buy

Escrow

Escrow

Sell

Sell
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
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…*
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)
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
# Features & Benefits of Precious Metals on Bankchain

<table>
<thead>
<tr>
<th>FEATURES</th>
<th>BENEFITS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Automated DvP</strong> for the first time in the gold market</td>
<td>Risk reduction</td>
</tr>
<tr>
<td><strong>Faster settlement times</strong></td>
<td>Capital savings; better capital utilization</td>
</tr>
<tr>
<td><strong>Automated clearing and settlement</strong> solutions for allocated and unallocated gold</td>
<td>Error reduction; Lower operational cost</td>
</tr>
<tr>
<td><strong>Dematerialized Gold</strong></td>
<td>Efficient use in collateral and financing</td>
</tr>
</tbody>
</table>
Envisaged Strategic Solution

Shared Services JV
- Spot Settlement Matching
- Position Validation
- Cash Netting / Bullion Settlement
- Auto Margin Settlement

Federal Reserve

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

<table>
<thead>
<tr>
<th>Unallocated</th>
<th>Liability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset</td>
<td></td>
</tr>
<tr>
<td>$100 unallocated loan to dealer (RWA = 100%)</td>
<td>$100 unallocated deposit from customer</td>
</tr>
<tr>
<td>Equity</td>
<td>~$13 capital for unallocated gold</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Bankchain</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset</td>
<td>Liability</td>
</tr>
<tr>
<td>$100 allocated deposit from customer (RWA = 0%)</td>
<td>~$0 capital for allocated gold</td>
</tr>
</tbody>
</table>

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.
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.
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
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
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
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.
Tokenization of Listed Securities

Deliver free with beneficial owner details

Bankchain Participant

Beneficial Owner (BO)

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

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

Master Account Structure at DTC

Encumbrance of shares

DTC

Bankchain

Master Account Structure on Bankchain

Bankchain Participant

Bankchain Participant 2

BO Participant

KYC, AML checks
Bankchain as a Settlement Location

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 netting 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.
How the Trade is Made on Bankchain

NSS

Counterparty

Bankchain Participant

BOs place orders for XYZ shares

BO1
BO2
BO3

Beneficial Owners

Counterparty delivers shares to participant's wallet

Bankchain

Participant places block XYZ order with Exchange member(s)

Smart contract debits NSS for cash obligation

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

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.

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.
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 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**

94 of 136
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.
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
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.
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

<table>
<thead>
<tr>
<th>Year</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jan 2009</td>
<td>Bitcoin blockchain released</td>
</tr>
<tr>
<td>Nov 2013</td>
<td>Vitalik Buterin releases the Ethereum blockchain White Paper</td>
</tr>
<tr>
<td>Jul 2014</td>
<td>Ethereum crowdsale raises $18M worth of BTC for development</td>
</tr>
<tr>
<td>Jul 2015</td>
<td>Ethereum 1.0 launched, Genesis block created</td>
</tr>
<tr>
<td>Jan 2016</td>
<td>40+ banking consortium used Ethereum to transfer digital assets</td>
</tr>
</tbody>
</table>
Price: ~$12.50 (up from $0.30 at genesis sale)

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

2nd largest crypto currency
Types of Blockchains

- **Permissionless chain**
- **Permissioned chain**
- **Consortium chain**
Technology Stack

// Application
DApps, Balanc3 Triple Entry Accounting, eTRS, eSign
Smart Document and Mgt. Sys, Business Logic

// Core components
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
Virtualized Network Node & API

// Blockchain
2 of 6 Ethereum Clients: Java and Haskell, Private
Blockchains (ETH BaaS)
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
1 Access uPort Wallet

Brought to you by:
CONTRACT TERMS
Please enter TRS terms below

Counterparty B: Macy Hawkins

Notional Amount (USD): $1000000
Term (minutes): 4

Underlying Asset Long:
- MSFT
- SPOT PRICE ORACLE: 53.53

Underlying Asset Short:
- GOLD
- SPOT PRICE ORACLE: 1069.35

Counterparty B Collateral %: 12.00%

Collateral %: 5.00%

Blockchain Asset Account:
- Counterparty B Blockchain Asset Account: $3,000,000
- Blockchain Asset Account: $2,500,000

Special Terms: Reputation Credit

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

Global Reputation Score: 79/FEU
SMART CONTRACT

The counterparties agree to the following:

<table>
<thead>
<tr>
<th></th>
<th>Nigel Woolworth</th>
<th>Macy Hawkins</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>NOTIONAL AMOUNT</strong></td>
<td>$10,000,000</td>
<td>$10,000,000</td>
</tr>
<tr>
<td><strong>POSITION</strong></td>
<td>MSFT / Gold</td>
<td>Gold / MSFT</td>
</tr>
<tr>
<td><strong>REQUIRED COLLATERAL AMOUNT</strong></td>
<td>$500,000 <strong>NOT FUNDED</strong></td>
<td>$1,200,000 <strong>NOT FUNDED</strong></td>
</tr>
<tr>
<td><strong>BLOCKCHAIN ASSET ACCOUNT</strong></td>
<td>$2,500,000</td>
<td>$3,000,000</td>
</tr>
</tbody>
</table>

- **SPOT PRICE**
  - MSFT: 53.62
  - Gold: 1069.43

- **SWAP TERM**
  - 4 minutes

**NEXT STEPS:**

- **FUND COLLATERAL ACCOUNT**
  - Upload ISDA/CSA File
  - E-SIGN CONTRACT
  - SEND TO COUNTERPARTY

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

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

The counterparties agree to the following:

1b Funded Collateral

1a Fund Collateral

2 IPFS: ISDA, CSA, Confirmation

3 eSign

4 Send to CP

5 Balanc3

When both parties have e-Signed & funded collateral, Balanc3 will send confirmation and swap will begin.
1 Oracle for Prices

<table>
<thead>
<tr>
<th>MSFT PRICE</th>
<th>GOLD PRICE</th>
<th>% CHANGE</th>
<th>RETURN DIFFERENCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>$ 52.82</td>
<td>$ 1093.31</td>
<td>2.306%</td>
<td>-3.577%</td>
</tr>
</tbody>
</table>

2 Collateral Rebalancing

<table>
<thead>
<tr>
<th>NOTIONAL AMOUNT</th>
<th>RETURN DIFFERENCE</th>
<th>CURRENT SWAP VALUE</th>
</tr>
</thead>
<tbody>
<tr>
<td>$ 10,000,000</td>
<td>-3.577%</td>
<td>$ -357,700.00</td>
</tr>
</tbody>
</table>

3 Triple Entry Accounting

Oracle for MSFT/Gold:
- **Nigel Woolworth**
  - Notional Amount: $10,000,000
  - Position: MSFT/Gold
  - Required Collateral Amount: $857,700
  - Blockchain Asset Account: $1,642,300
- **Macy Hawkins**
  - Notional Amount: $10,000,000
  - Position: Gold/MSFT
  - Required Collateral Amount: $1,557,700
  - Blockchain Asset Account: $1,442,300
<table>
<thead>
<tr>
<th></th>
<th>Nigel Woolworth</th>
<th>Macy Hawkins</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>NOTIONAL AMOUNT</strong></td>
<td>$10,000,000</td>
<td>$10,000,000</td>
</tr>
<tr>
<td><strong>POSITION</strong></td>
<td>MSFT / Gold</td>
<td>Gold / MSFT</td>
</tr>
<tr>
<td><strong>REQUIRED COLLATERAL AMOUNT</strong></td>
<td>$792,300</td>
<td>$1,992,300</td>
</tr>
<tr>
<td><strong>BLOCKCHAIN ASSET ACCOUNT</strong></td>
<td>$1,707,700</td>
<td>$1,007,700</td>
</tr>
</tbody>
</table>

Normalized Oracle Reputation

*94/SD*

Normalized Oracle Reputation

*74/FEU*

---

**REPUTATION DOWNGRADED**

**COLLATERAL REBALANCING EVENT**

**FUNDS TAKEN FROM BLOCKCHAIN ASSET ACCOUNT**

---

**MSFT**

**Gold**

---

*2 Collateral Rebalancing*

*2 Reputation Downgraded from 79*

*1 Oracle for Reputation*
SWAP SETTLEMENT

FINAL OUTCOME

Nigel Woolworth

NOTIONAL $10,000,000

Reputation Score
94/SD
MSFT / Gold
+ $94,400.00

Macy Hawkins

NOTIONAL $10,000,000

Reputation Score
74/FEU
Gold / MSFT
- $94,400.00

FINAL RETURN DIFFERENCE

0.944 %

COLLATERAL ACCOUNTS RELEASED

1 Triple Entry Accounting
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
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
A smart contract is a programmatically enforceable arrangement in which the contractual clauses are written in code rather than legal-eses.

- Predetermined logic
- Typically replicated across a distributed ledger
- Removes the need for trust
- Automated / self executing
Example
Example
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
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
How Smart Contracts Work
Example Smart Contract on a Blockchain
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
Data Standards
Most smart contracts rely upon oracles for external data in order to execute upon their programming.
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
Risks / Outstanding Issues
Replicability depends on code standards, and code standards depend on a legal framework.
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
Future of Smart Contracting
Future of Smart Contracting

Digital Assets

Digital Currencies

Internet of Things
Questions