Bringing Blockchain to Global Enterprise

Ben Taylor, CEO, LedgerDomain
Orange County ACM Chapter
July 18, 2018
Blockchain: Hyped and Ridiculed

Cryptocurrencies: everything you don’t understand about money combined with everything you don’t understand about computers” John Oliver
How Bitcoins Get Transferred

Bob owes Alice money for lunch. He installs an app on his smartphone to create a new Bitcoin wallet. A wallet app is like a mobile banking app and a wallet is like a bank account.

To pay her, he needs two pieces of information: his private key and her public key.

Bob gets Alice’s public key by scanning a QR code from her phone, or by having her email him the payment address, a string of seemingly random numbers and letters.*

The app alerts Bitcoin ‘miners’ around the world of the impending transaction. ‘Miners’ provide transaction verification services.

The miners verify that Bob has enough bitcoins to make the payment.

Many transactions occur in the network at any time. All the pending transactions in a given timeframe are grouped (in a block) for verification. Each block has a unique identifying number, creation time and reference to the previous block.

*Anyone who has a public key can send money to a Bitcoin address, but only a signature generated by the private key can release money from it.

Graphic: Deloitte University Press. Source: American Banker
So What Have We Learned from Bitcoin?

• Human progress is anchoring through STIPULATION of an ASSUMPTION
• Bitcoin’s stipulation is that the tallest block is the right block
• 10 million members agree on a single version of the truth every 10 minutes

• Most corporations haven’t had a single version of the truth since 1987
Blockchain is the latest in a long line of financial computing innovations.

- **an Khipu**
- **Decimalized computer**
- **Permanent storage**
- **1st distributed database**

**Pacioli’s *Summa* (1494)**
- Double-entry bookkeeping

**MIT Whirlwind (1951)**
- Parallelized logic
- Magnetic core memory
- Real-time graphical output

8,000 Years of Accounting History
Blockchain enables multiple parties to jointly transact & settle in near real-time.
What is Blockchain / Distributed Ledger?

“We’ve always looked for a distributed database with a trust harness that allows multiple organizations to collaborate... Clearly, the blockchain and the distributed ledger that exists underneath it is a very novel implementation which can have massive implications.”

– Microsoft CEO Satya Nadella
Blockchain: data structure capturing events are immutably time-stamped.

Events: when parties agree to mutually e-sign a transaction in accordance with a smart contract.” Once notarized into a blockchain, the commitment is binding and irrevocable. Records in the blockchain are encrypted and linked, making alterations almost impossible.

The associated ledger is a consensus of complicated, shared, and synchronized digital data across multiple participants.
Distributed Ledger Variants

Important distinctions amongst different blockchain platforms

- **private vs. public blockchains** (commingled data)?
- **open or by invitation membership** (permissioned access)?
- **network costs borne by subscription or bounties** (mining)?

Bounties are typically paid in the form of cryptocurrency to successful “miners” with newly minted coins, thereby adding inflation to system.

- Permissioned blockchains may be warranted when access to information needs to be restricted based on necessity and privacy laws.
- **On-chain vs. off-chain?** Which data elements to store on the blockchain vs. store remotely? Cash register tape & stock ticker are blockchain precursors.
# Comparing Blockchain Platforms

<table>
<thead>
<tr>
<th></th>
<th>Ethereum</th>
<th>Hyperledger Fabric</th>
<th>Bitcoin</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Positioning</strong></td>
<td>Visionary</td>
<td>Enterprise-grade</td>
<td>Classic</td>
</tr>
<tr>
<td><strong>Governance</strong></td>
<td>Ethereum Foundation?</td>
<td>Linux Foundation</td>
<td>Hmmmm</td>
</tr>
<tr>
<td><strong>Participation</strong></td>
<td>Open with Velvet Ropes</td>
<td>Permissioned, private</td>
<td>Open</td>
</tr>
<tr>
<td><strong>Consensus</strong></td>
<td>PoW → PoS?</td>
<td>Pluggable consensus</td>
<td>PoW Mining</td>
</tr>
<tr>
<td><strong>Smart contracts</strong></td>
<td>Yes, typically Solidity</td>
<td>Yes, typically Go or Java</td>
<td>More basic</td>
</tr>
<tr>
<td><strong>Currency</strong></td>
<td>ether, gas, altcoins</td>
<td>None in native form</td>
<td>bitcoin</td>
</tr>
</tbody>
</table>

*Comparing Blockchain Platforms (Table)*

Partially sourced from SBC Working Paper, 6/2017
Enterprises went hard into Relational Database in the ’80s

- Client service and the web pushed the client points further and further
- Application servers managed & personalized client experiences

“Big data” is nice way of saying relational has failed

Wall Street: Algorithms (smart contracting) & High-frequency (real time)
Amazon and Google raised expectations….

Enterprises: feet in relational concrete and heads in the big data clouds?
Challengers in Enterprise Blockchain Development

Linux Foundation and IBM driving Hyperledger Fabric

Amazon Web Services, IBM, HP, Microsoft, Oracle, and SAP styling themselves as blockchain-as-a-service (BaaS) providers

Financial services companies have formed consortia while pioneers like Northern Trust are in production with blockchain internally

Ethereum enterprise edition under way, while JPMorgan has launched Quorum initiative off Ethereum

Standalone proprietary blockchains such as Ripple have emerged
# How Can Enterprises Move Incrementally?

<table>
<thead>
<tr>
<th>Blockchain Attributes</th>
<th>Strengths</th>
<th>Weaknesses</th>
<th>Opportunities</th>
<th>Threats</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Shared data model</td>
<td>Key partnership</td>
<td>Hard to change</td>
<td>Future-proof</td>
<td></td>
</tr>
<tr>
<td>Shared client and data model</td>
<td>Site efficiency</td>
<td>Maintainability</td>
<td></td>
<td>Viral Infection</td>
</tr>
<tr>
<td>Shared permissioned system</td>
<td>Industry control</td>
<td>Less flexible</td>
<td>Upgradability</td>
<td></td>
</tr>
<tr>
<td>5. Shared permissioned and partitioned system</td>
<td>Gold standard</td>
<td>Expensive</td>
<td>Upgradability</td>
<td></td>
</tr>
</tbody>
</table>
Blockchain Solution Process Flow

**STAKEHOLDERS**
- Role Identification
- User Stories
- Tiers & Privacy

**REQUIREMENTS**
- User Stories
- Barcode/Access
- Transactions
- Events & Callouts

**DESIGN STUDIO**
- Transactions
- Wireframes
- Animations
- Focus & Pilot

**MEMBERS**
- Authorization
- Certificates
- Privileges
- Access

**CONTRACTS**
- Language
- Generic
- Private

**DATA SCIENCE** (Fields, Formats, Privacy)

**ON CHAIN/OFF** (Barcode; Private; Encrypted)

**BLOCKCHAIN** (Permission; Partitioning)

**SERVER** (App, CA, DevOps, Identity, A&A)

**INFRASTRUCTURE** (Host, Container, QOS)

**BI** (Reporting; Data Sharing)
Enterprise Use Cases for Blockchain

**Global supply chains:** pharmaceuticals, electronics, national security procurement, etc. The blockchain-based supply chain opportunity for discrete finished products will exceed $424 million globally by 2023 (*ABI Research*).

**Private transactions between banks:** Currently while a million wires shoot back and forth between two banks in the course of a day, the money itself moves only in single massive net transfers (e.g. the SWIFT system).

**Patient records:** Encrypted patient records would allow for real-time access with greater security.
LedgerDomain Simplified Architecture

CLIENT SIDE
WITH TIERED CLIENTS

- Organization
- Member
- 3rd Party

SERVER SIDE
WITH SELVEDGE & HYPERLEDGER FABRIC

- SPONSOR
  - Admin Console
- SELVEDGE
  - Initialize, Configure & Deploy
  - Runtime
- OFF-CHAIN
  - Encrypted & Syndicated

HYPERLEDGER FABRIC

LedgerDomain
Smart Contracts

FABRIC SDK
- Membership
- Transactions
- Event Hub
- Consensus
- Blockchain

Infrastructure
Supply Chain Demo
LedgerDomain Architectural Cascade

CLIENT FOCUS
WITH TIERED CLIENTS

SERVER FOCUS
WITH SELVEDGE & HYPERLEDGER FABRIC

SPONSOR
Root of Trust

SPONSOR
Admin Console

LedgerDomain
Smart Contracts

FABRIC CA
Organization
(1,2,X)

SELVEDGE
Initialize, Configure & Deploy

MEMBERSHIP
Transactions

PEER & NODES
Organization
Member

SELVEDGE
Runtime

Event Hub
Consensus

3rd Party

OFF-WORLD
Credentials & Administration (LDAP, AD)

OFF-CHAIN
Encrypted & Syndicated

Blockchain

Infrastructure for Members & Clients

Infrastructure for Orderer

Infrastructure for Node 1

Infrastructure for Node 2

Infrastructure for Node X
Where is Development Heading?

- Chaincode portability, blockchain federation and integrability
- More robust models for organizations and permissions
- Analytics on chaincode data
- Next-generation crypto and data models
- Integration with enterprise systems such as ERP & MES
- Designing for compliance with privacy laws (e.g. HIPAA, GDPR)

*Blockchain, artificial intelligence & IoT combine to make every transaction*

*...instantaneous, confidential, unforgeable & trackable*
Feedback and Questions?
Where to Learn More

How Blockchain Unlocks the Fourth Wave of Financial Computing

Hyperledger Fabric