Innovation Workshop Series
Beyond Bitcoin: What to do with Blockchain?

Presented by: Mike Myburgh, Office of the CTO | Strategic Enablement Group

Q2, 2017

Beyond Bitcoin: What to do with Blockchain?

Messaging:

Most people have heard of Bitcoin, and also know that blockchain is one of the underlying concepts behind this cryptocurrency. However, what does this mean for the broader enterprise? How can technologies related to blockchain be applied in various verticals, and what does this mean for traditional database-centric approaches? Join this session to hear about blockchain and associated concepts such as smart contracts, and what we, as technologists, should be thinking about as we look to apply these concepts across various use cases and verticals.

Beyond Bitcoin: What to do with Blockchain?

http://ericsammons.com/what-is-the-blockchain/

Beyond Bitcoin: The Tip of the Iceberg

Projected to Grow at 61.5% CAGR to 2021
USD 210.2 million (2016) to USD 2,312.5 million (2021)

http://www.marketwatch.com/story/blockchain-technology-market-growing-at-615-cagr-to-2021-2016-10-13-22203054

Beyond Bitcoin: The Tip of the Iceberg

Google Trends
Blockchain
Internet of Things
Machine Learning

Beyond Bitcoin: Why the Interest?

Digital Mesh*

- The digital mesh is a mesh of people, devices, content, and services.
- New business models and processes are needed to cope with a world that is increasingly connected and blended.

Decentralized Business Networks

- There is a need to automate business transactions via contracts across network participants in an efficient and cost-effective manner.
- The old "B2B exchanges" and third parties reduce speed & agility.

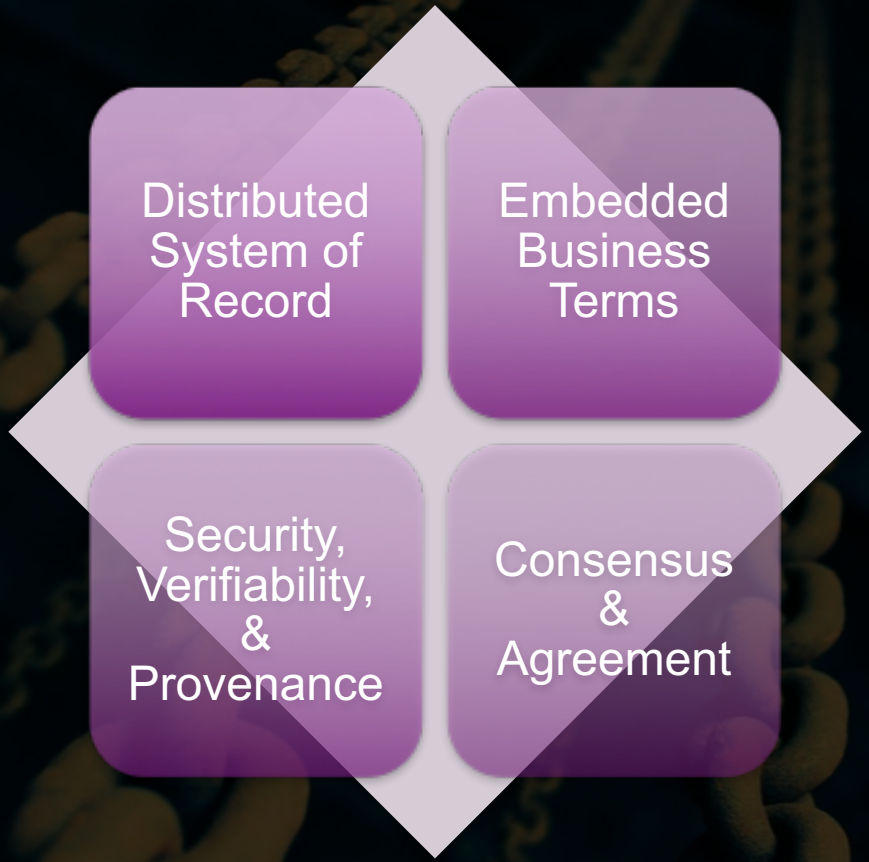
Need for Integrity & Visibility

- Transactions must be conducted openly and securely, with full integrity.
- Many business transactions require an immutable, agreed-upon log.

* https://www.gartner.com/doc/3471559?srcId=1-7484470122#-363727574

Core Concepts

Beyond Bitcoin: Core Concepts



Beyond Bitcoin: Core Concepts

Blockchain may be thought of as a **distributed data management platform** where data may be shared across a distributed network, securely and with (potentially) business logic.

Beyond Bitcoin: Core Concepts

Transaction is added to a “block”.

Block is replicated to the participants that need to validate the transactions.

All network parties validate the transaction.

Block is added to the “chain”, creating a tamper-proof audit log.

Beyond Bitcoin: Core Concepts

- **Distributed Ledger Technology (DLT)**
  - An database shared across blockchain participants via peer-to-peer replication.
  - No central server or node. Communication occurs between peers, and each peer usually has a copy of all data.
  - Transactions typically organized into “blocks”.

- **Cryptographic Hashes**
  - Industry standard methods of calculating a digital signature / representation of data (e.g. SHA-256).

Beyond Bitcoin: Core Concepts

- **Consensus Algorithms**
  - Techniques used to build agreement & verify / add transactions to the blockchain.
  - Proof of Work
    - Computationally intensive (and thus expensive) "guessing game", now often done on specialized hardware.
  - Proof of Stake
    - Creator of the block is chosen in deterministic fashion, weighted by stake.
  - PoET (Proof of Elapsed Time)
    - "Lottery protocol that builds on trusted execution environments (TEEs) provided by Intel's SGX". Each validator node waits a random amount of time before trying to claim a block. (Intel)

Beyond Bitcoin: Core Concepts

- **Permissioned vs. Permissionless**
  - "Private" vs. "Public"
  - Is anonymous participation allowed? Are validators known? Are modification rights restricted?

- **Consortium Blockchain**
  - Predefined or selected group of validators handle the consensus process (e.g. "consortium" of financial institutions).

Beyond Bitcoin: Smart Contracts

- Smart Contracts represent a way to introduce business logic into the blockchain.
  - May be triggered by transactions or external events.
- Logic may be executed "on-chain" by the participants in the network, with no central coordinator.
  - Code is run in parallel.
  - Results are compared and agreed upon.
- Opportunity to reduce risk, increase efficiency, and automate the execution of business logic across the network without a central party.

Beyond Bitcoin: Smart Contracts

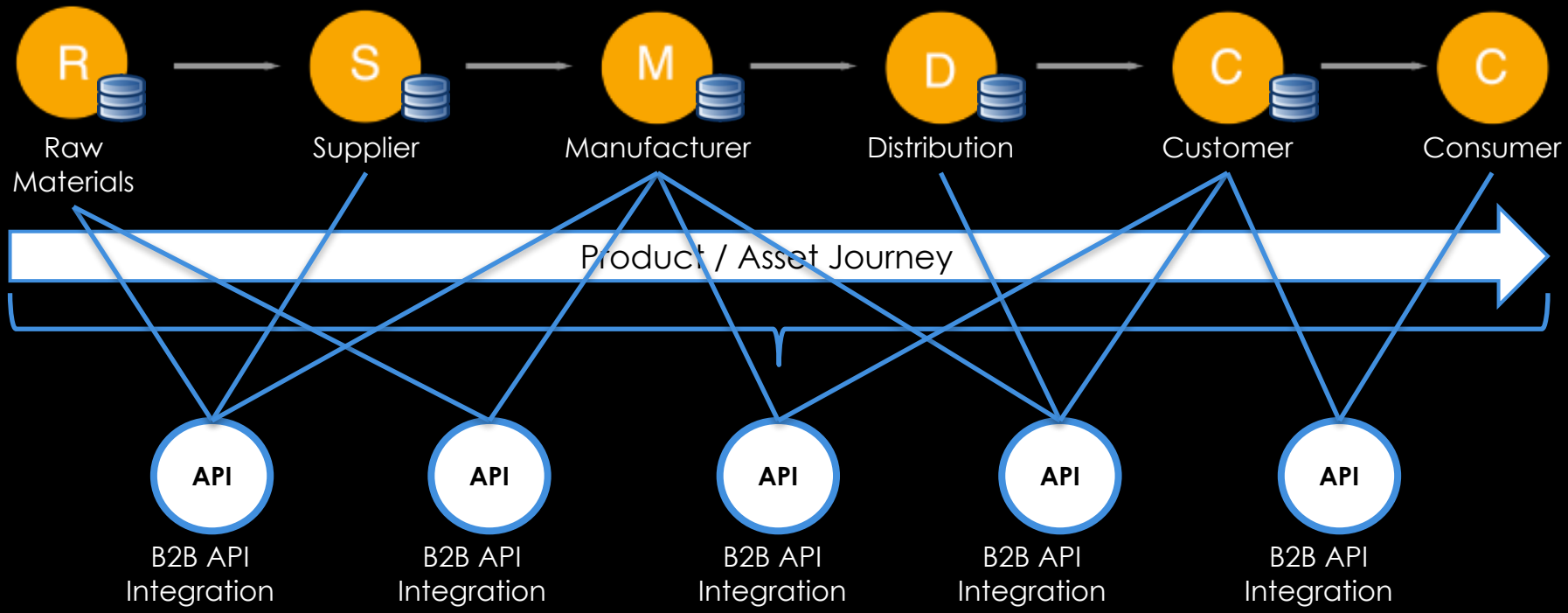
Smart Contracts represent **one of the biggest initial opportunities for this technology**, starting in the context of private / permissioned blockchains.

So What Can We Do With This?

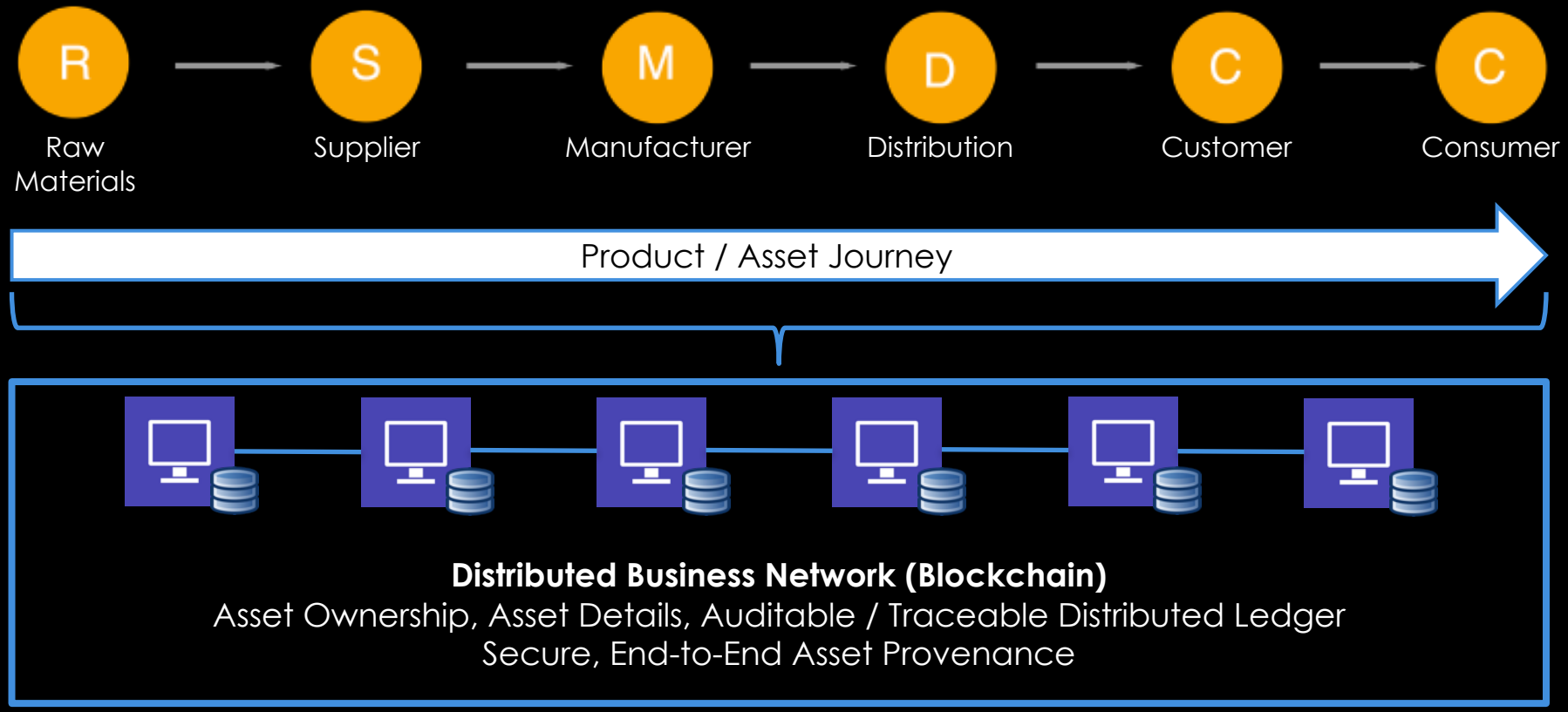
- Creation And real-time movement of assets
  - No clearing delays due to intermediaries
- Blockchains have the potential to
  - Reduce systemic risk, Financial fraud
- Audit Trail - Timestamp, rights and ownership proof
  - Cryptographically secured
- Self Execution of business logic
  - Self enforcement
- Blockchain protocols facilitate businesses new methods of processing digital tx
  - Payment system and digital currency, Facilitating Crowd sales
- Selective Transparency and privacy
- Resistance to Single point of failure

So What Can We Do With This?

Use Cases: Product Provenance

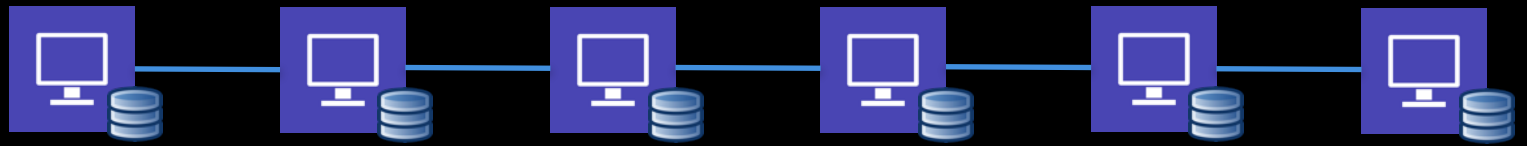


Use Cases: Product Provenance



Use Cases: IoT

Product / Asset Journey (e.g. Energy Distribution)



Distributed Business Network (Blockchain)
IoT Triggered Smart Contracts, IoT Augmented Asset Information
IoT Device Verification and Tracking

Use Cases: “Consumer Contract” Automation

Insurance Claims

Reimbursements and automatic claims processing for certain types of claims. Unemployment insurance payouts based on smart contract terms and verified employment history / data.

Airline Compensation

Automatic payout of compensation to airline passengers according to defined business rules (smart contracts) for situations such as flight delays, flight cancellations.

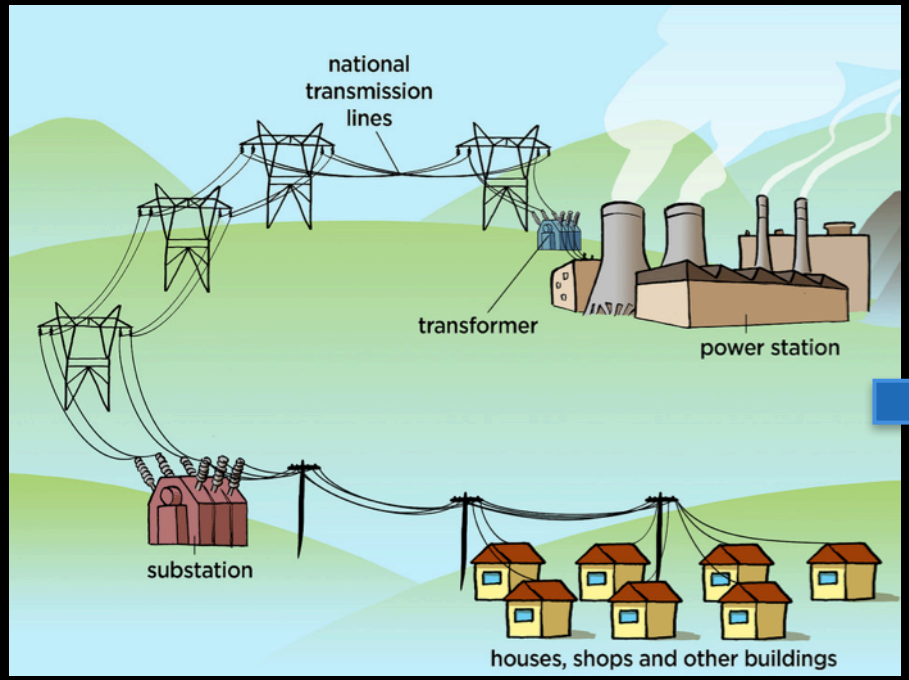
Apartment Rental

Execute smart contacts on verified rental contract to establish all required utilities and services such as water, power, gas, cable.

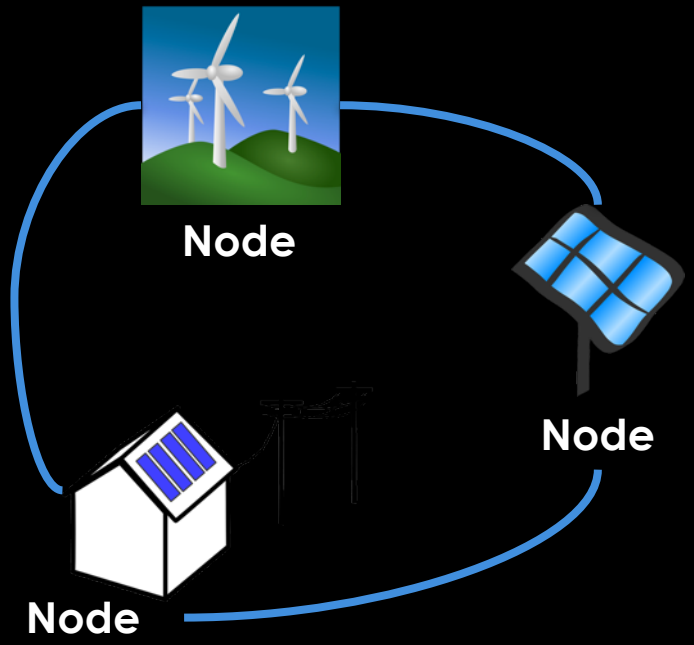
Use Cases: Government

- ***Government To Citizen***
  - Asset Registry and Asset Exchange
    - Track property ownership transactions in a secure, immutable fashion over time. Reduce property ownership fraud.
  - Licenses & other citizen services.
  - Identity management.
- ***Government To Vendor***
  - Contract compliance, budgeting, and payments.
  - Invoice fraud prevention & regulatory compliance (automate legal requirements).
- ***Government To Government***
  - Intra-agency information sharing & process automation through smart contracts
  - Contract management.

Use Cases: Energy Distribution



Power created by a central source, and transmitted to end consumers, often over long distances.



Power generated locally, and distributed in a peer-to-peer fashion via smart contracts. (see Brooklyn microgrid as an example)

Use Cases: Health Care & Pharma

Electronic Health Record
Electronic Medical Record
Personal Health Record

Secure, distributed patient health records.

Claims Processing

Business network of payer, providers, and financial institutions, fraud prevention.

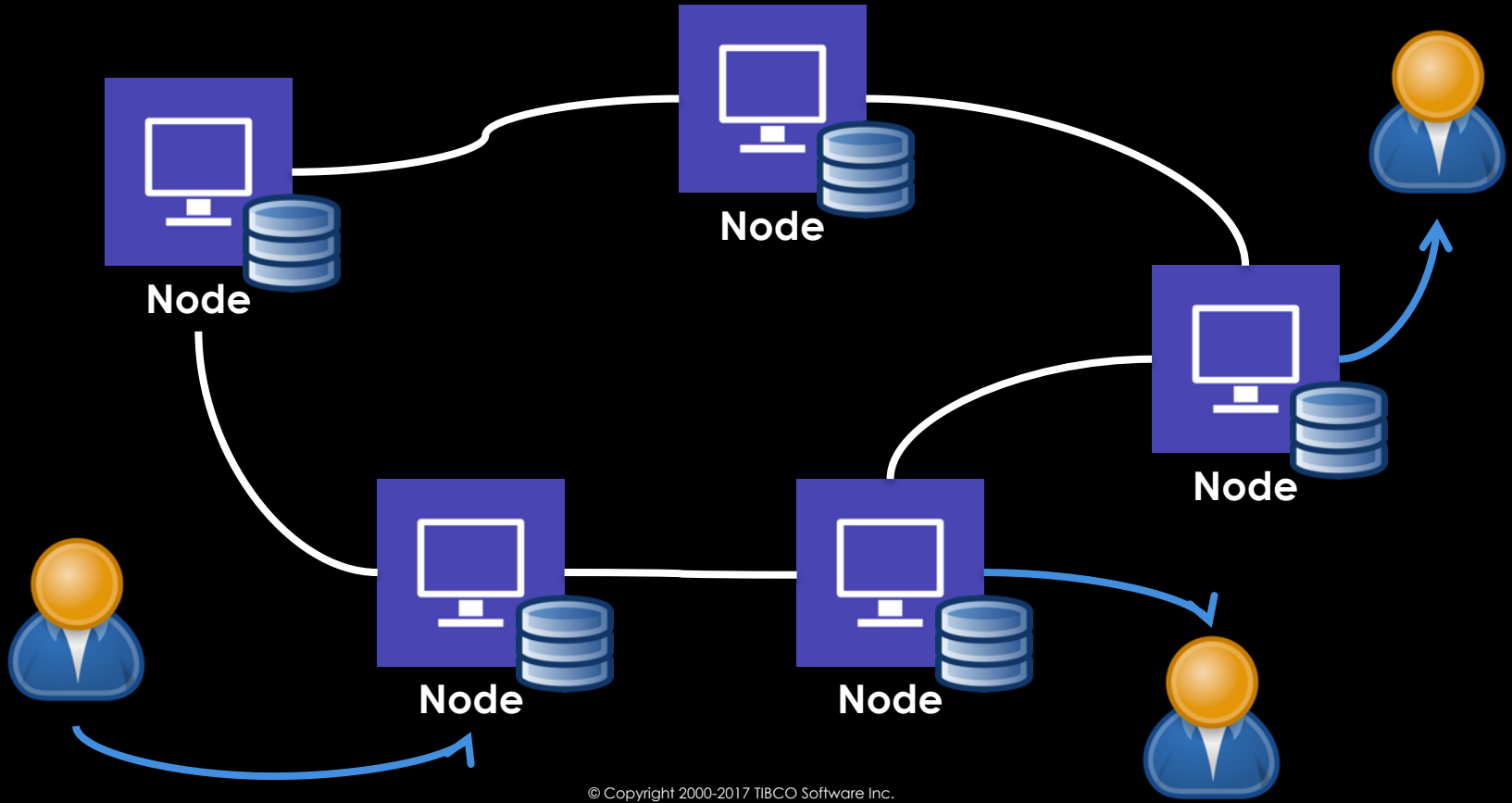
Provider Registry / Directory

Distributed, verified network of provider information.

Prescription Drug Provenance

Capturing the complete drug supply chain, from raw materials to consumer distribution.

Use Cases: Async, Global Publishing Layer



Beyond Bitcoin: Related Technologies (Sample)

BlockApps

symbiont

Gem

ripple

ethereum

MONAX

HYPERLEDGER

IBM

Microsoft

MultiChain

Beyond Bitcoin: Ethereum (https://www.ethereum.org/)

- Blockchain platform for executing smart contracts.
  - Programmable blockchain that may be used to create operations of any complexity.
  - Turing complete
  - Requires "proof of work" ("Ethash") in order to successfully mine a block.
- "Suited for applications that automate direct interaction between peers or facilitate coordinated group action across a network" (ethdocs.org)
- Contracts typically are written in "Solidity" (similar to Javascript).
- Native value token: "ether" (ETH).
  - Various denominations
  - Used for pay for computation by purchasing "gas".

Beyond Bitcoin: Hyperledger Project (https://www.hyperledger.org/)

- Open source effort to advance cross-industry blockchain technologies.
  - Hosted under the Linux Foundation.
  - Community for multiple projects related to blockchain.
  - Encourages interoperable components.
- "Hyperledger Fabric": implementation of blockchain technology intended as a foundation for developing blockchain applications.
  - Designed as a modular architecture.
  - Hosts smart contracts called "chaincode", run in containers.
  - Other projects: Sawtooth Lake, Iroha, Burrow.
- Not a single blockchain, and has no "built-in" cryptocurrency tokens.

Beyond Bitcoin: Hyperledger Project (https://www.hyperledger.org/)

- Underpinned by modular architecture
  - Provides resiliency, Flexibilit, Scalability
- Default DB is LevelDB
  - Can be replaced by CouchDB
  - Provides Rich Query Language, Stores JSON Data
- Multiple channels to separate solutions,
- Channel's Ledger contains
  - Config block for policies
  - Access control list (ACL)
  - Other pertinent info
- Channels contains Membership Service Provider instances
  - Crypto materials to be derived from Certificate Authorities (CA)
- Transactions consists of versions of in Key/Values read and write sets in chain code

Is a Blockchain All I Need?

Beyond Bitcoin: Additional Capabilities

- For the appropriate use case, blockchain can provide "part" of the solution.
- However, there are still questions to answer:

How Do I Get Data In/Out of the Blockchain?	**How Do I Extend Smart Contract Logic To My Enterprise?**	**How Do I Respond To Events from my Ledger?**	**How Do I Analyze Data Contained Within the Ledger?**	**Can I Provide Controlled, Managed Access to Blockchain Capabilities?**

Beyond Bitcoin: Additional Capabilities

Off-Chain Execution

Off-Chain Storage

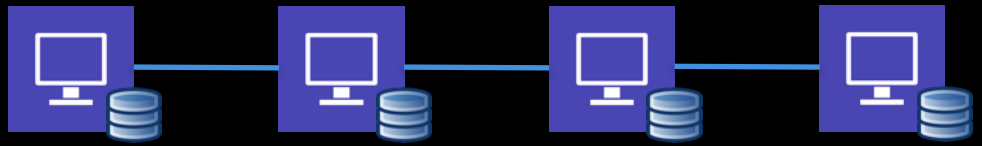
API Management | Analytics

Microservices | Event Handlers

Data Distribution Transport

Blockchain Proxy Layer | Smart Contracts ChainCode, Solidity, …

HFC SDK | REST HTTP | JSON RPC | Web3 | Blockchain APIs



On-Chain Execution & Storage

Distributed Ledger Blockchain Security

Beyond Bitcoin: Additional Capabilities

API Management
TIBCO Mashery

Analytics
TIBCO Spotfire, Live Datamart

Microservices & Process Automation
TIBCO Hybrid Integration, AMX BPM

Event Handlers
TIBCO BusinessEvents, StreamBase

Data Distribution Transport
TIBCO FTL / eFTL

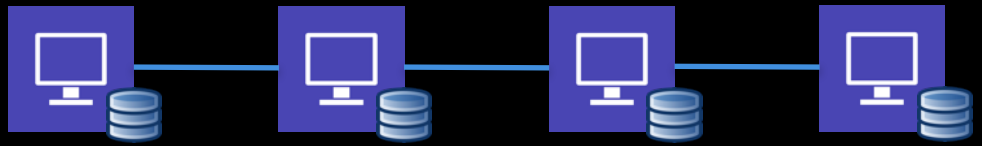
Off-Chain Execution
TIBCO (Various)

Blockchain Proxy Layer
TIBCO Hybrid Integration

Smart Contracts
ChainCode, Solidity, …
TIBCO BusinessEvents

Off-Chain Storage
TIBCO GraphDB ActiveSpaces

Blockchain APIs



On-Chain Execution & Storage

Distributed Ledger Blockchain Security

Beyond Bitcoin: TIBCO Messaging

TIBCO EMS

- Industry leading JMS solution for store and forward messaging services.
- Available as an appliance, with no requirements for additional third party components.
- Core backbone of a datacenter-led integration strategy.

TIBCO FTL

- Ultra low latency, peer-to-peer distributed messaging with centralized management and administration.
- Supports guaranteed and reliable message delivery with dynamically pluggable delivery transports.
- On-premise, cloud, and IoT use cases.

TIBCO eFTL

- Easiest way to extend the messaging infrastructure to web and mobile devices using HTML5 and web sockets.
- Can be deployed standalone, facilitating pure web sockets communications.

Beyond Bitcoin: TIBCO Hybrid Integration

BusinessWorks

BusinessWorks Container Edition

Cloud Integration

Mashery

FLOGO™ by TIBCO Software Inc.

Flogo

On Premise → Hybrid Cloud → Public Cloud → API → IoT

Blockchain Services

Beyond Bitcoin: TIBCO Event Processing

TIBCO BusinessEvents

- Build event driven applications for contextual control, utilizing event-driven architecture (EDA) principles.
- Rule-driven / declarative intelligence system with embedded analytics model execution.
- Combines state, time, and rules into a single platform.

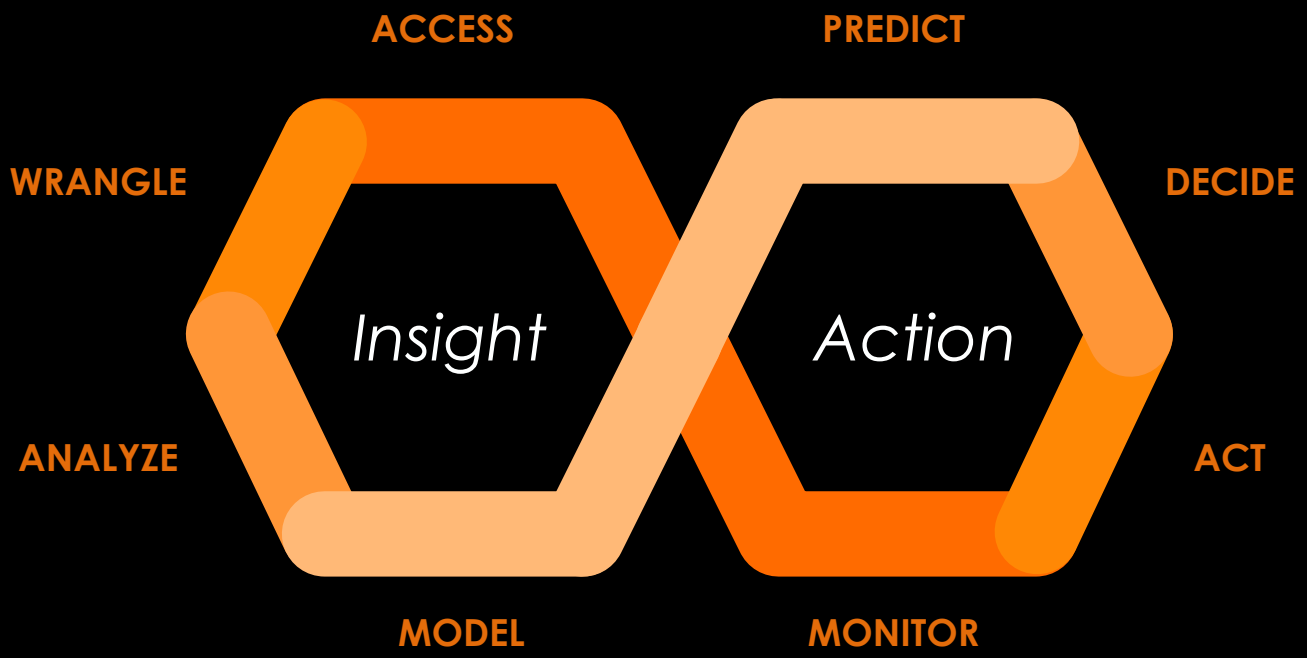
TIBCO StreamBase

- Build streaming analytics applications for pre-processing and model scoring.
- Pre-process Big Data streams to enrich, transform, aggregate, or filter.
- Execute analytics models in-line for making decisions on streaming data.

TIBCO Live Datamart

- Provide real-time insight, command, and control.
- Utilize continuous queries to identify threats or opportunities immediately.
- Create mash-ups of historical and real-time data.
- Interact with live visualizations and alerts.

Beyond Bitcoin: TIBCO Analytics / Spotfire



Main BPM Use Cases

Process Documentation

Improve collaboration with business users, formalize processes and operating procedures.

Process Automation

Improve the effectiveness of processes. Flawless execution, Reduce costs, delays, errors, provide traceability of instances

Work Management and Workforce Optimization

Improve operational efficiency, distribute the workload between teams, monitor deadlines and manage the prioritization of activities

Digitalization and Case Management

Build enterprise low-code applications, customer-centric, collaborative, dynamic, less prescriptive and mixed processes. Enabling the knowledge worker and improve customer experience.

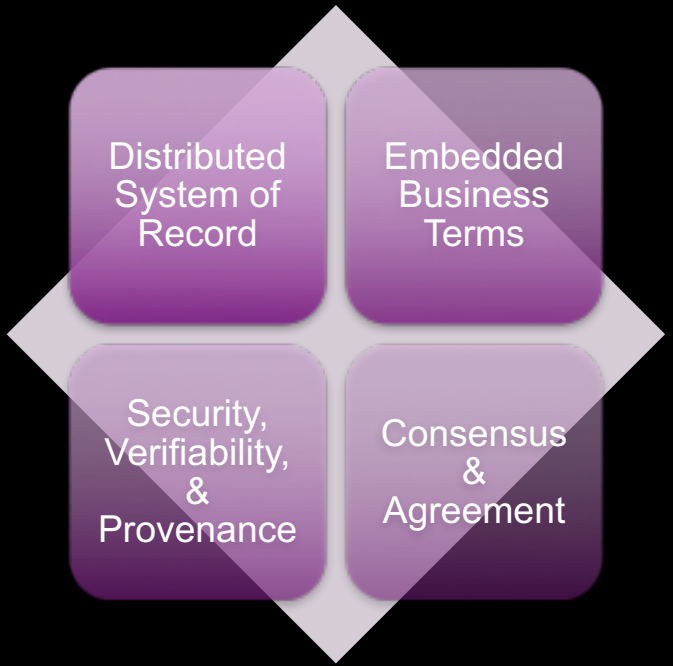
TIBCO ActiveMatrix BPM Highlights

Beyond Bitcoin: Recommendations

- **Not every problem requires a blockchain!**
  - Peer to peer networking, distributed data stores, and cryptography have been around for some time.
- Need to **look at a number of factors**. For example:
  - Number of network participants.
  - Required trust and integrity levels.
  - Amount of data to be stored.
  - Performance requirements and transaction processing times.
  - Ability to automate business interactions across a network.
- **A blockchain is only part of the equation.**

Beyond Bitcoin: Recommendations

- **Gain awareness through experimentation.**
  - Cloud based services make it easier to get started.
- Answer the factors (previous slide), and **identify use cases / value** appropriate for your business.
- Determine how the **key characteristics** of a blockchain can be **beneficial to the business network**.



TIBCO

TIBCO Software Meetups

We are **4,301** members across **56** Meetups

TIBCO Software takes businesses to their digital destinations by interconnecting everything in real time and providing augmented intelligence for everyone, from business users to data scientists. This combination delivers faster answers, better decisions, and smarter actions. For nearly 20 years, thousands of businesses around the globe have relied on TIBCO technology to differentiate themselves through compelling customer experiences, optimized assets, and innovative new business models. Learn how TIBCO brings data alive at
www.tibco.com

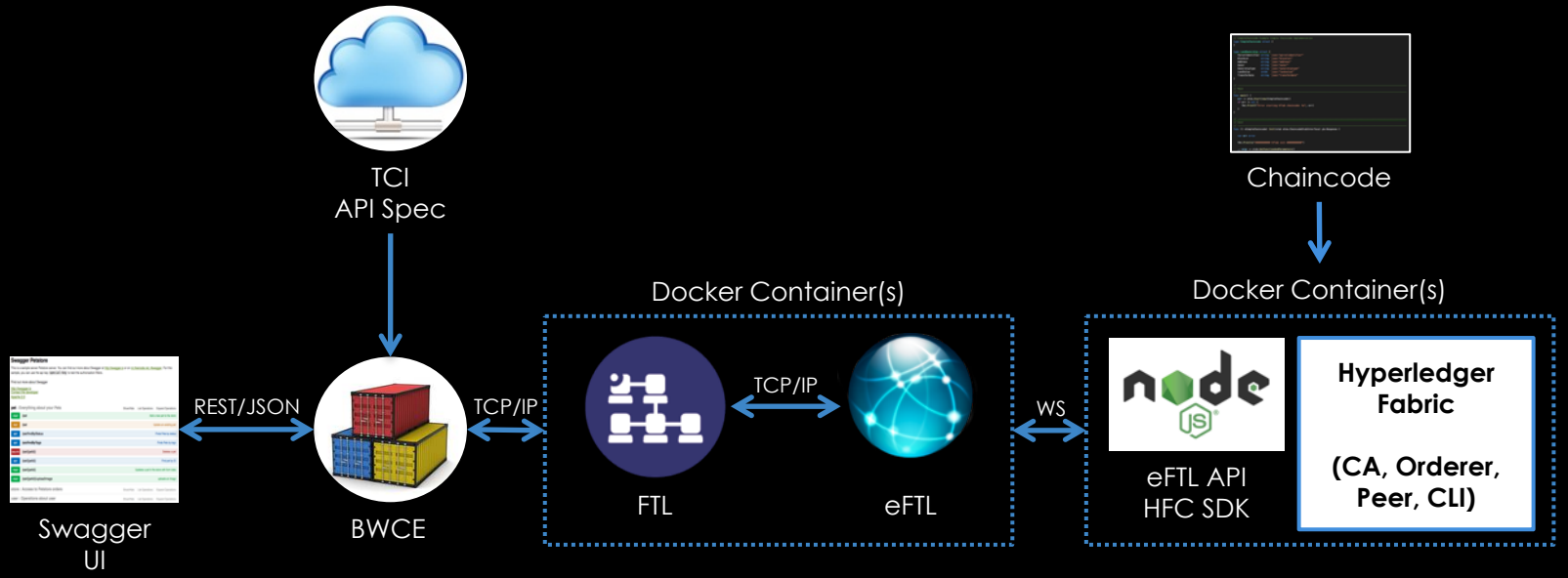
TIBCO® NOW™ 2017

DIGITAL SMARTER

SINGAPORE Mar. 27-28 BERLIN Jun. 6-7 SAN DIEGO Oct. 25-26

Demonstration

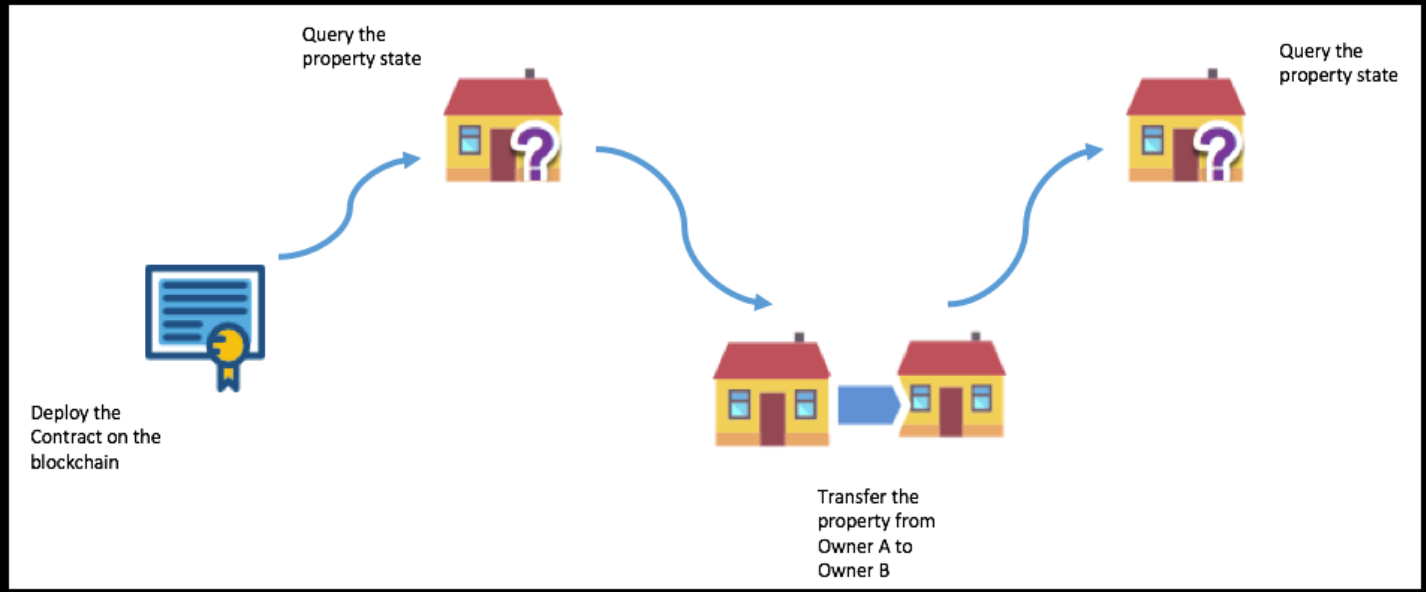
Demonstration: Use Case and Architecture



Lab Storyboard

Property Transfer from Owner A to Owner B

1. Deploy the Contract on the blockchain
2. Query the property state
3. Transfer the property from Owner A to Owner B
4. Query the property state



Hands-On Session (Optional)

More Information

TIBCO Blog and Community:
http://www.tibco.com/blog/
https://community.tibco.com/

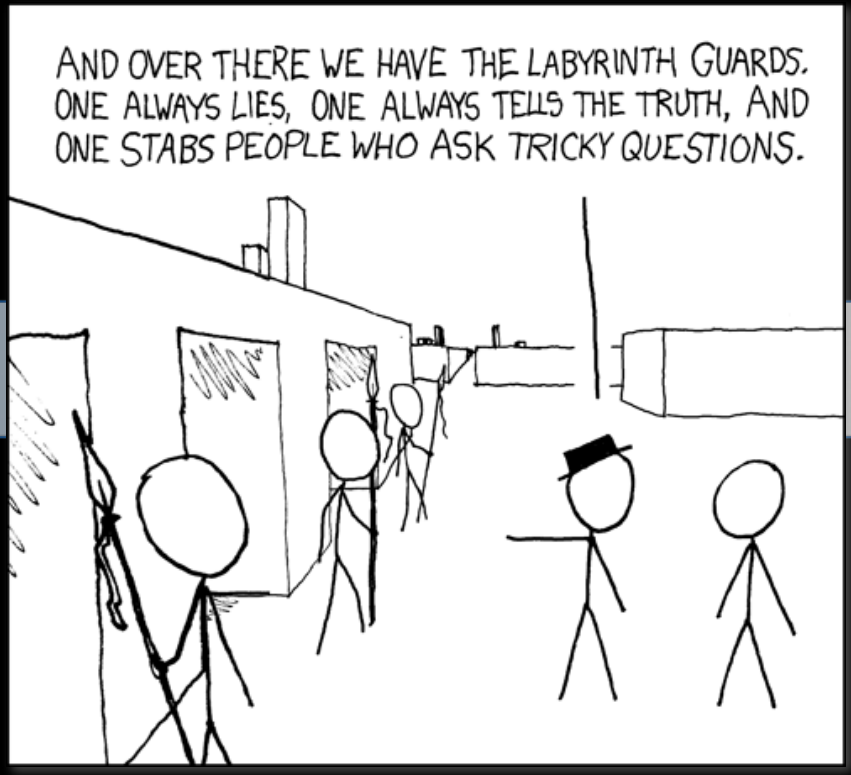
TIBCO Cloud Integration:
http://cloud.tibco.com/

TIBCO BusinessWorks / Container Edition (BWCE):
http://www.tibco.com/products/automation/application-integration/activematrix-businessworks

TIBCO Flogo
https://community.tibco.com/products/project-flogo

TIBCO Mashery
https://www.mashery.com/

Questions?


AND OVER THERE WE HAVE THE LABYRINTH GUARDS. ONE ALWAYS LIES, ONE ALWAYS TELLS THE TRUTH, AND ONE STABS PEOPLE WHO ASK TRICKY QUESTIONS.