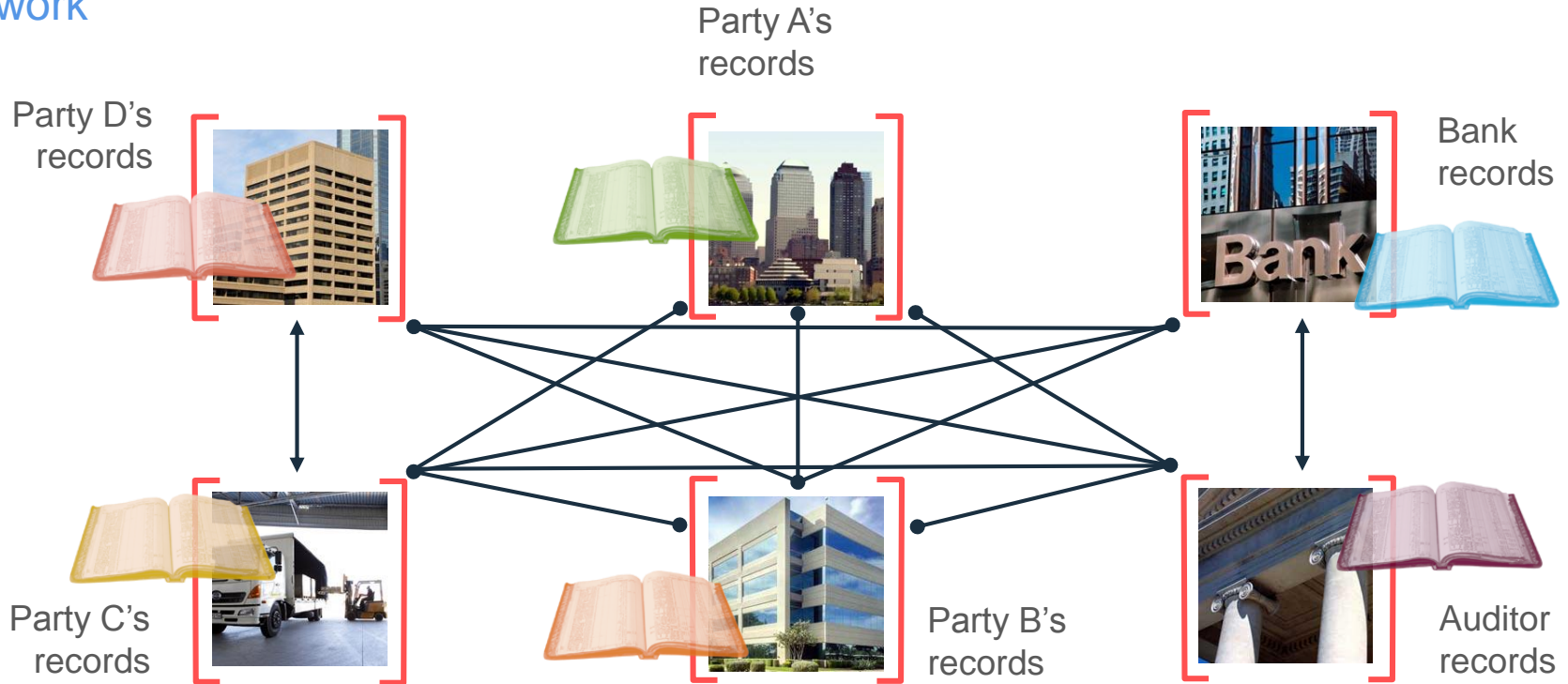# Making Blockchain Real for Business

A Blockchain discussion for ACM

April 17, 2017

Rebecca Gott, Ph.D.
IBM Systems Group
z Systems & LinuxONE Development
IBM Senior Technical Staff Member

Today's process of monitoring asset ownership and transfer is difficult in a business network

Party D's records

Party A's records

Bank records

Party C's records

Party B's records

Auditor records

… Inefficient, expensive, vulnerable

Ledgers are key …

Ledger is THE system of record for a business. Business will have multiple ledgers for multiple business networks in which they participate.

Transaction – an asset transfer onto or off the ledger

John gives a car to Anthony (simple)
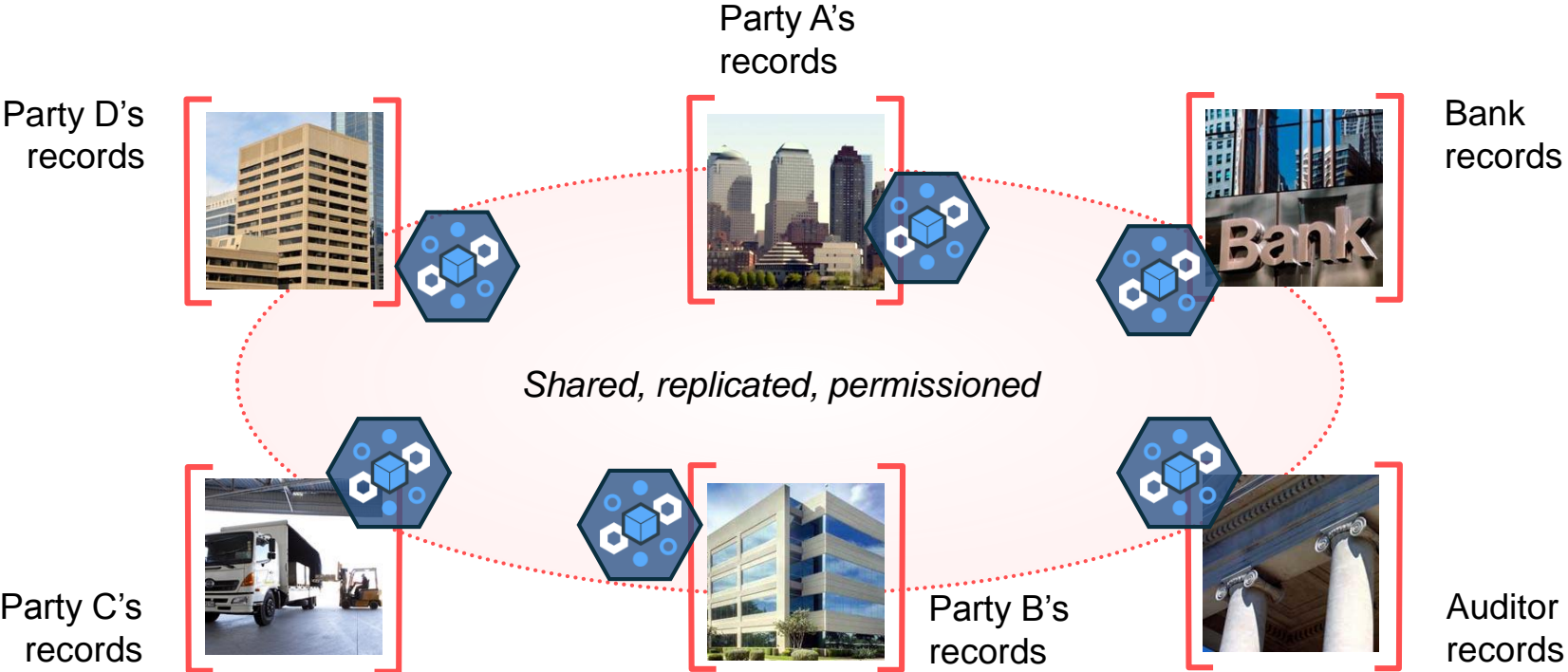
Contract – conditions for transaction to occur

If Anthony pays John money, then car passes from John to Anthony (simple)

If car won't start, funds do not pass to John (as decided by third party arbitrator) (more complex)

Blockchain's shared, replicated and permissioned ledger is the solution

Party D's records

Party A's records

Bank records

Shared, replicated, permissioned

Party C's records

Party B's records

Auditor records

… Consensus, provenance, immutability, finality

Blockchain underpins Bitcoin …

₿ *bitcoin*

An unregulated shadow-currency

The first blockchain application

Resource intensive

Blockchain for business differs in key areas:
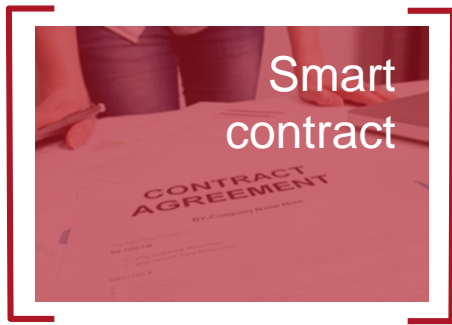
Identity over anonymity

Selective endorsement over proof of work
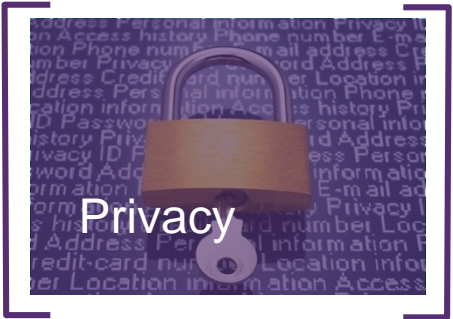
Assets over cryptocurrency

Blockchain for business …

Append-only distributed system of record shared across business network

Shared ledger

Smart contract

Shared business rules apply to transactions

Ensuring appropriate visibility; transactions are secure, authenticated & verifiable
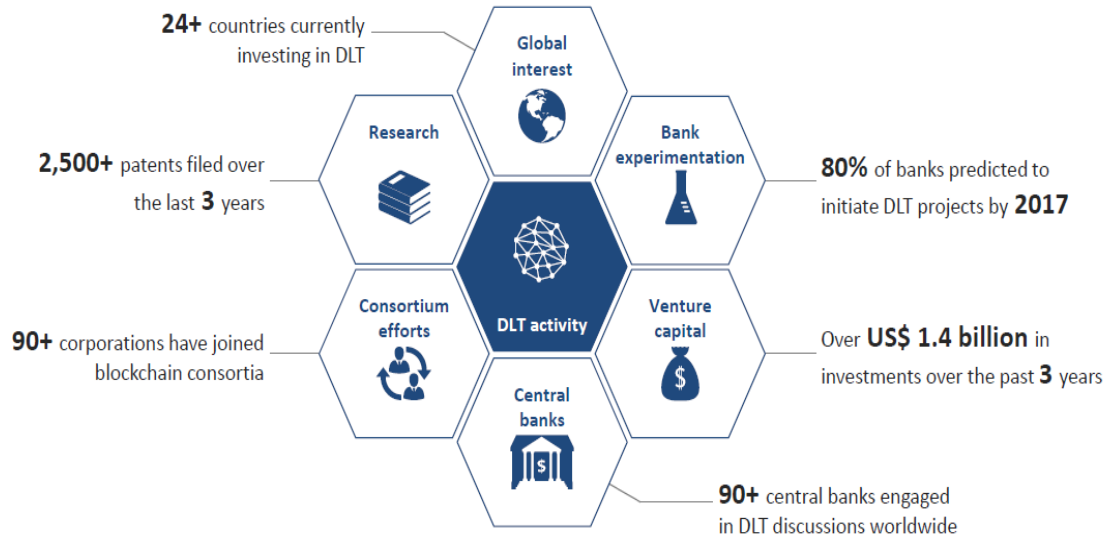
Privacy

Trust

Participants are able to trust the contents of the ledger

… Broader participation, lower cost, increased efficiency

Investment Interest in Blockchain
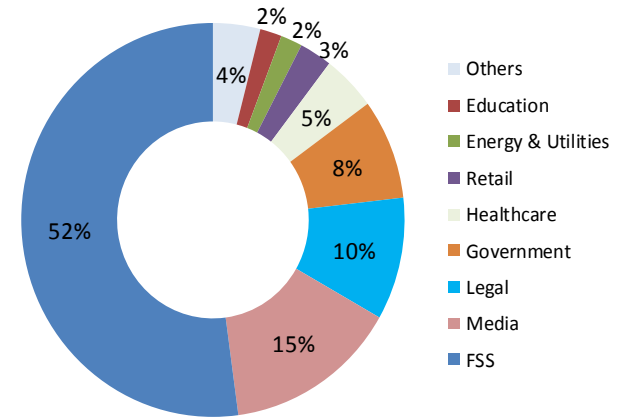
DLT: Distributed Ledger Technology

24+ countries currently investing in DLT

Global interest

Research

2,500+ patents filed over the last **3** years

Bank experimentation

80% of banks predicted to initiate DLT projects by **2017**

DLT activity

90+ corporations have joined blockchain consortia

Consortium efforts

Venture capital

Over **US$ 1.4 billion** in investments over the past **3** years

Central banks

90+ central banks engaged in DLT discussions worldwide

Use Cases by Industry

Broad appeal however; Financial Services Sector is 52% of the use cases

- Others
- Education
- Energy & Utilities
- Retail
- Healthcare
- Government
- Legal
- Media
- FSS

2% 2% 3% 4% 5% 8% 10% 15% 52%

Source – World Economic Forum | 2016

Hyperledger Fabric Overview

IBM is committed to the **Hyperledger Project**
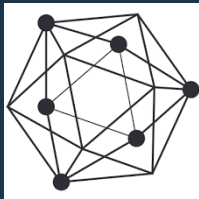
Successful Launch

30
Founding members

90
Additions since

>$6m
funding

2,300
membership requests

5x
more requests than next largest in LF history

IBM Key Contributions

Open fabric

Asset Agnostic

Permissioned

Enable adoption of shared ledger technology at a pace and depth not achievable by any one company or industry
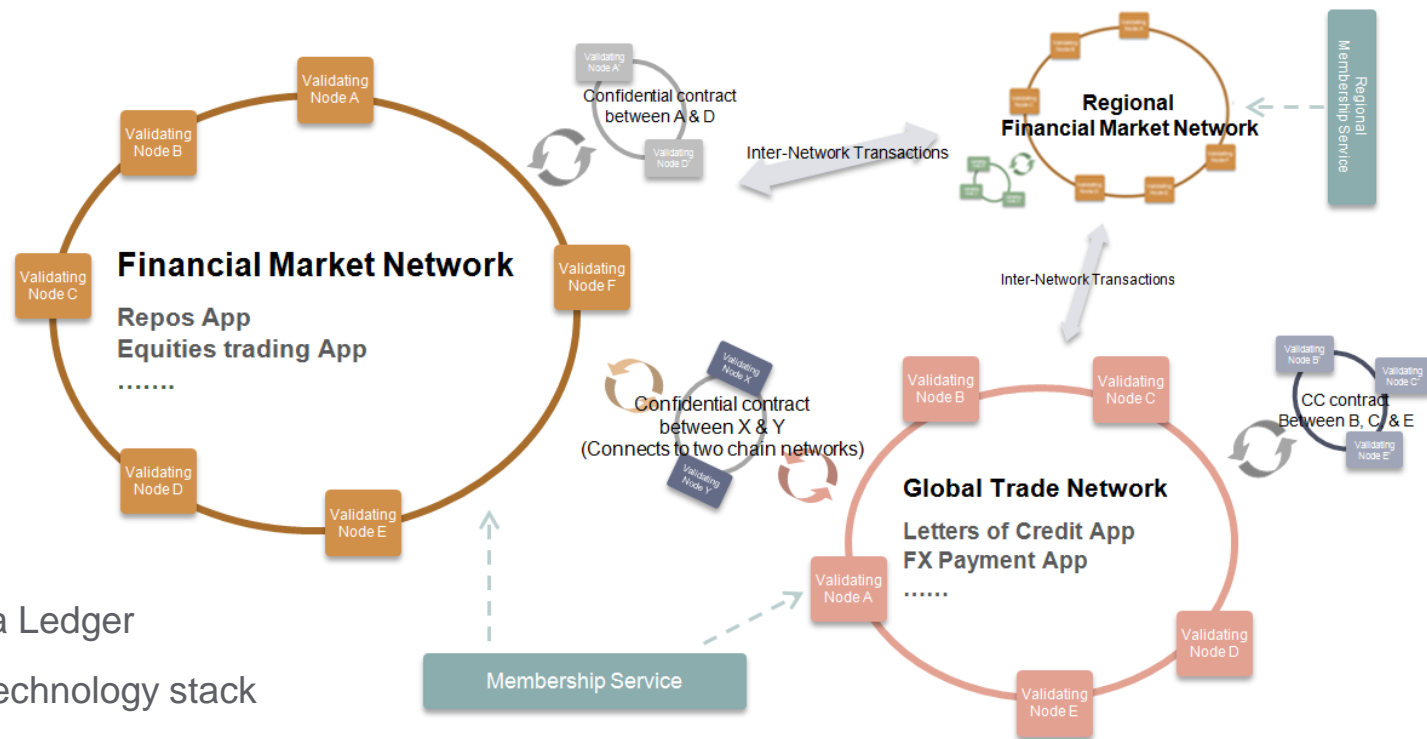
PREMIER

accenture
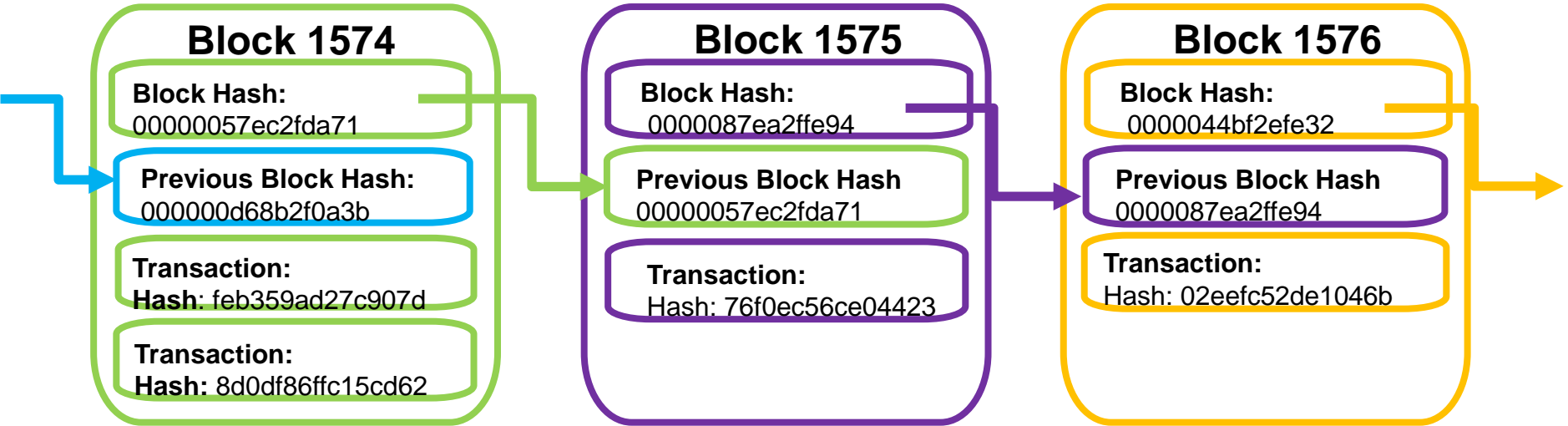High performance. Delivered.

CME Group

DEUTSCHE BÖRSE GROUP

Digital Asset

DTCC

FUJITSU

HITACHI
Inspire the Next

IBM

intel

J.P.Morgan

R3

GENERAL

ABN·AMRO

ANZ

NTT Digital

belink

bitse

BLOCKCHAIN

Blockstream

bloq

BNY MELLON

Broadridge

Calastone

CISCO

cloudsoft

CLS
Fundamental to FX

coinplug

CONSENSYS

CREDITS

Cuscal
The complete payments partner

Founding Digital

eVUE
digital labs

Gem

guardtime

intellect

INVeSHARE

itBit

Milligan Partners

MonetaGo

ML

MOSCOW EXCHANGE

Orchestrating a brighter world
NEC

norbloc

NTT DaTa

onchain

redhat

Ribbit.me

Skry

SORAMITSU

STATE STREET

SWIFT

symbiont

tequa creek

THOMSON REUTERS

vmware

WELLS FARGO

Fabrics and Networks

Financial Market Network

Repos App
Equities trading App
....

Confidential contract between A & D

Inter-Network Transactions

Regional Financial Market Network

Regional Membership Service

Inter-Network Transactions

Confidential contract between X & Y (Connects to two chain networks)

Global Trade Network

Letters of Credit App
FX Payment App
......

CC contract Between B, C, & E

Membership Service

- A network is a Ledger
- A fabric is a technology stack
  - e.g. Bitcoin, <u>Hyperledger</u>, Ripple, Ethereum

Block Creation
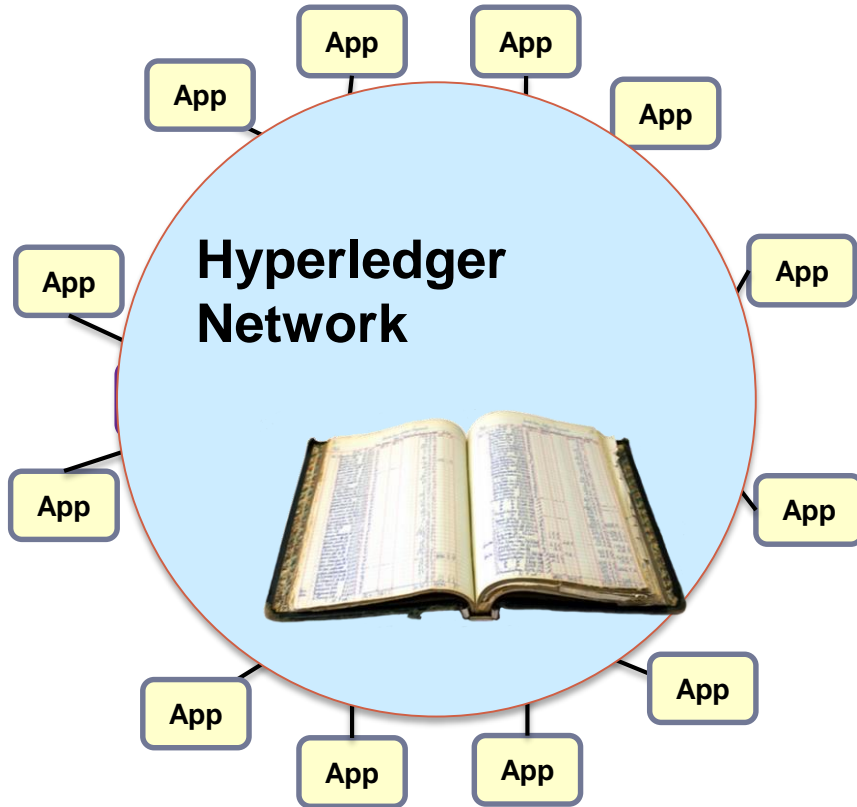
- Applications are written in Node.js and use a Hyperledger Software Development Kit

- Applications interface to the Hyperledger network through a set of APIs using Transport Layer Security (TLS)

  - Creates transactions - either code invoking or code deploying

  - Invokes Chaincode (Smart Contracts – logic running in the network). Chaincode can be developed using the Fabric Composer

- Transactions run against a distributed ledger

  - Held in Key Value Store on the Hyperledger nodes

- Transactions which change the ledger are endorsed and sent to the consensus process

- Passing the consensus process the transactions are grouped in a block and committed to the chain
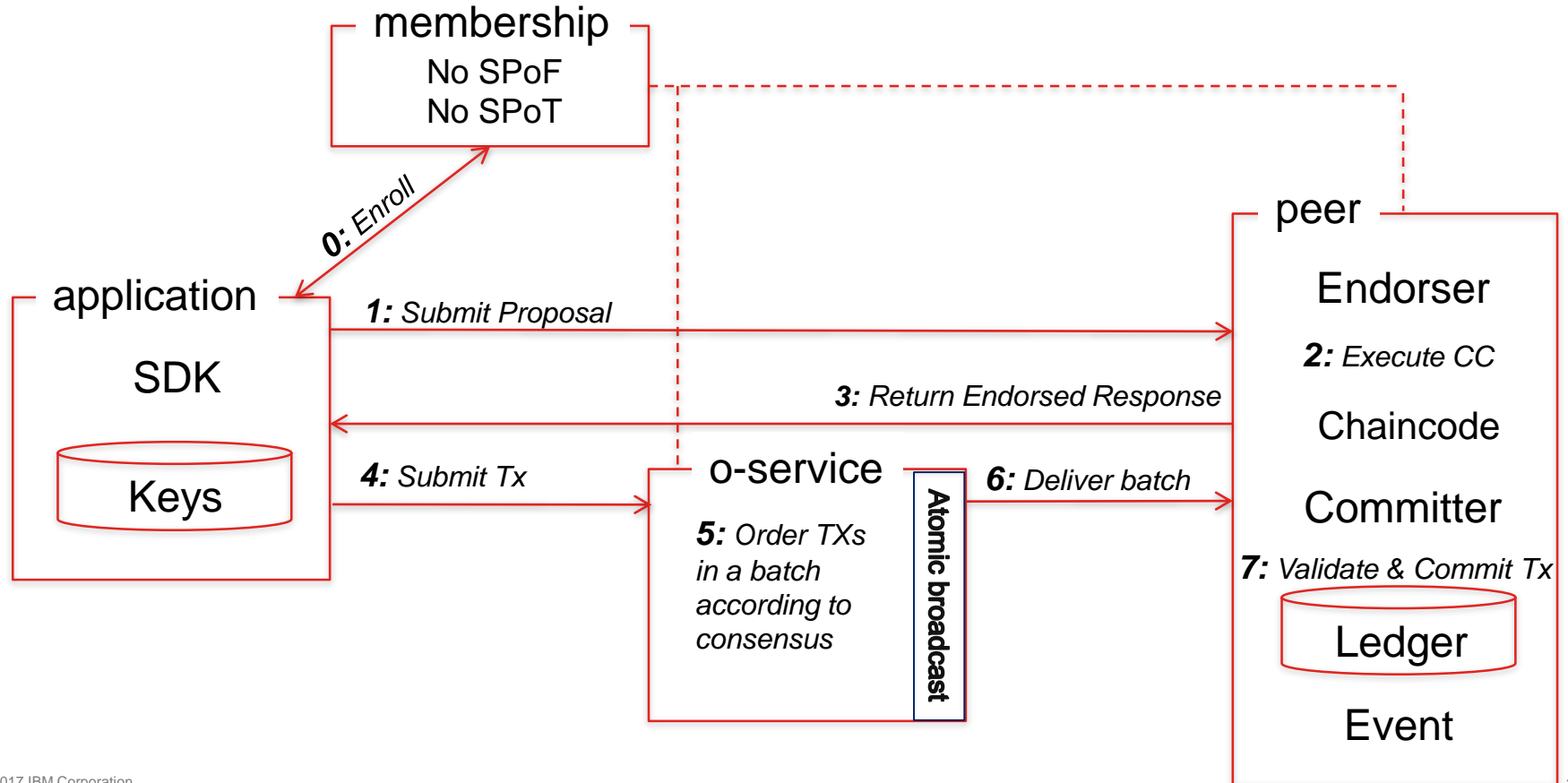
This result is Blockchain

Block 1574

Block Hash:
00000057ec2fda71

Previous Block Hash:
000000d68b2f0a3b

Transaction:
Hash: feb359ad27c907d

Transaction:
Hash: 8d0df86ffc15cd62

Block 1575

Block Hash:
0000087ea2ffe94

Previous Block Hash
00000057ec2fda71

Transaction:
Hash: 76f0ec56ce04423

Block 1576

Block Hash:
0000044bf2efe32

Previous Block Hash
0000087ea2ffe94

Transaction:
Hash: 02eefc52de1046b

Made up of a series of blocks added in chronological order
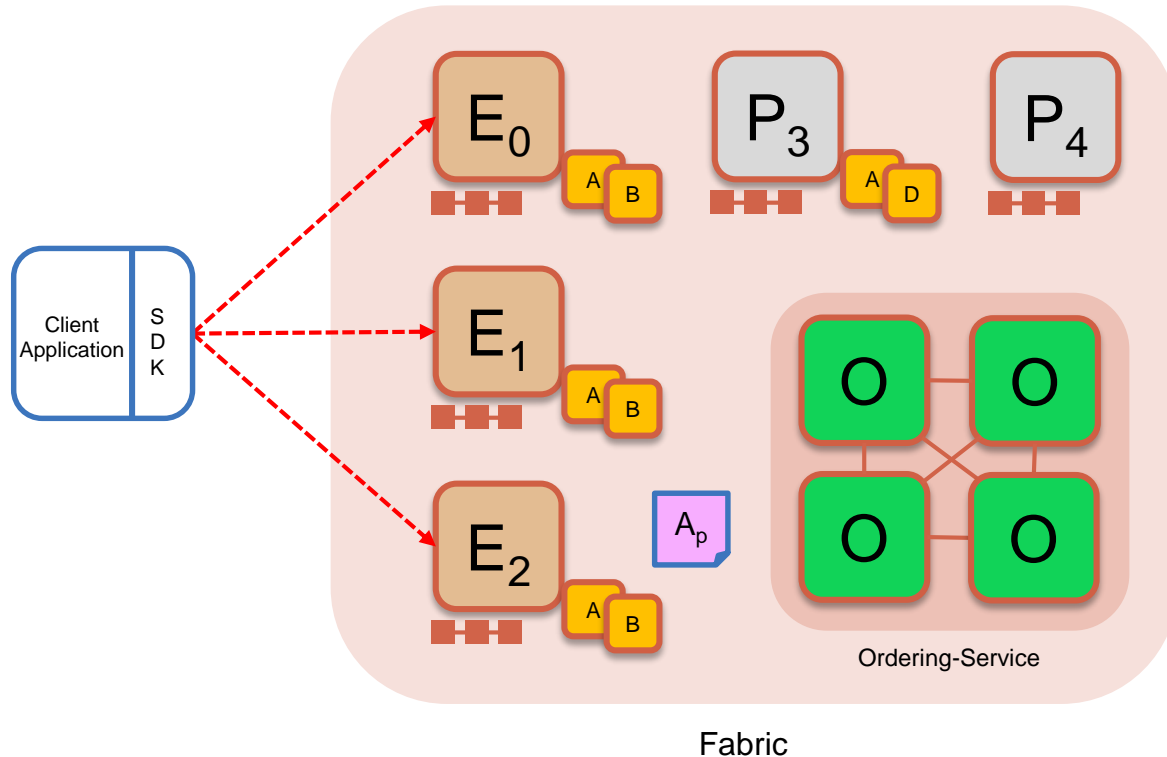
Nodes and roles

	Committing Peer: Maintains ledger and state. Commits transactions. May hold smart contract (chaincode).
	Endorsing Peer: Specialized committing peer that receives a transaction proposal for endorsement, responds granting or denying endorsement. Must hold smart contract
	Ordering Nodes (service): Approves the inclusion of transaction blocks into the ledger and communicates with committing and endorsing peer nodes. Does not hold smart contract. Does not hold ledger.

Architecture of Hyperledger Fabric v1

membership
No SPoF
No SPoT

application

SDK

Keys

0: Enroll

1: Submit Proposal

3: Return Endorsed Response

4: Submit Tx

o-service

5: Order TXs in a batch according to consensus

Atomic broadcast

6: Deliver batch

peer

Endorser

2: Execute CC

Chaincode

Committer

7: Validate & Commit Tx

Ledger

Event

Based on Source : https://jira.hyperledger.org/browse/FAB-37

Sample transaction: Step 1/7 – Propose transaction

Fabric

Application proposes transaction

Endorsement policy:
- "E_0, E_1 and E_2 must sign"
- (P_3, P_4 are not part of the policy)

Client application submits a transaction proposal for **Smart Contract A.** It must target the required peers {E_0, E_1, E_2}

Key:

Endorser	▨	▬▬▬ Ledger
Committing Peer	▨	▢ Application
Ordering Node	▨	
Smart Contract (Chain code)	▨	◈ Endorsement Policy

Ordering-Service

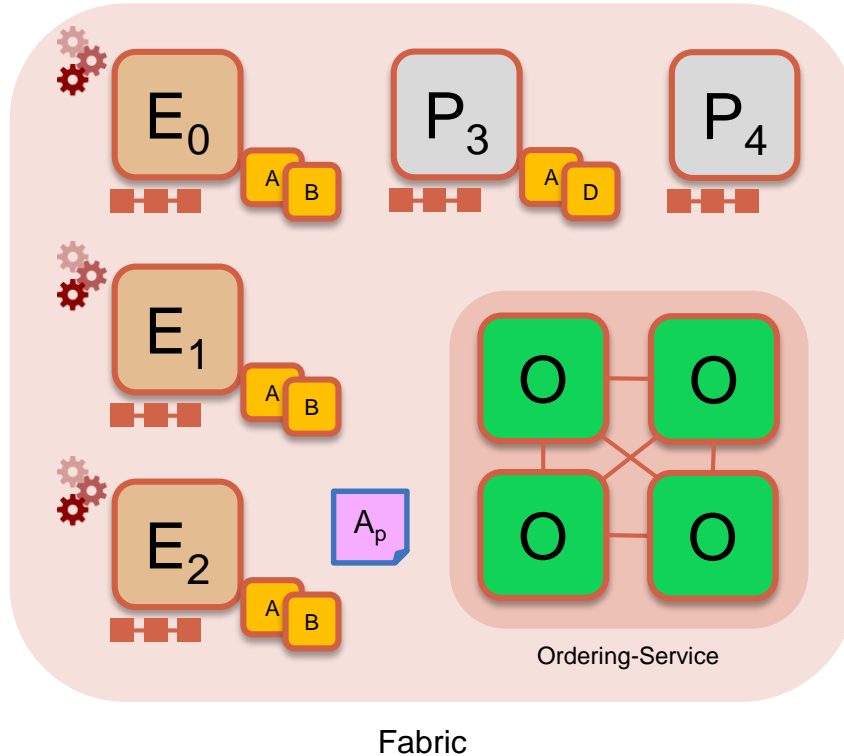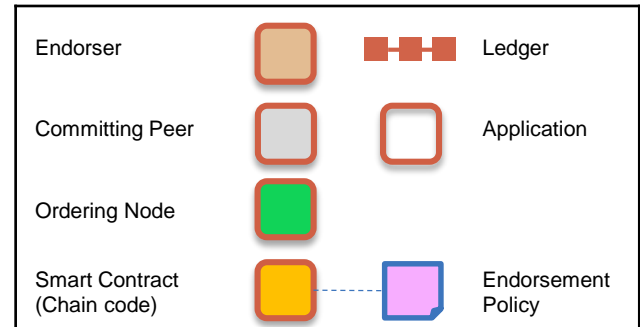# Sample transaction: Step 2/7 – Execute proposal

Fabric

Endorsers Execute Proposals

E_0, E_1 & E_2 will each execute the *proposed* transaction. None of these executions will update the ledger
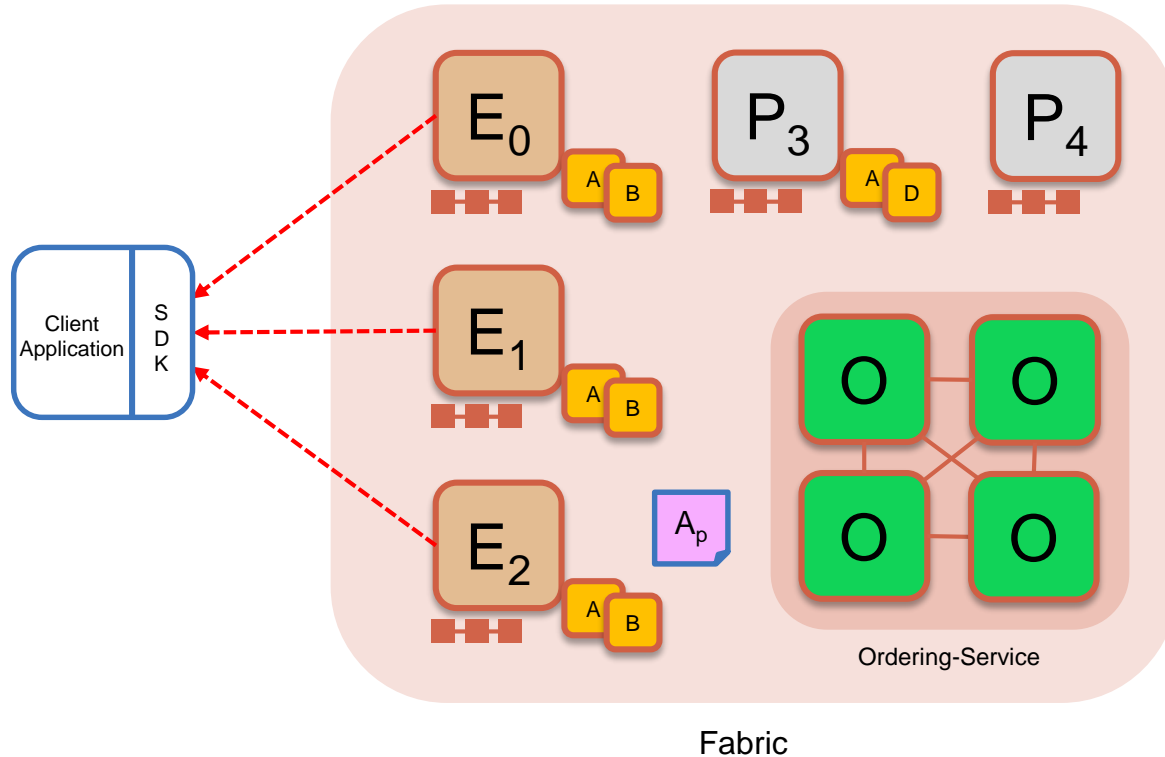
Each execution will capture the set of **R**ead and **W**ritten data, called **RW sets,** which will now flow in the fabric.

Transactions can be signed & encrypted

Key:

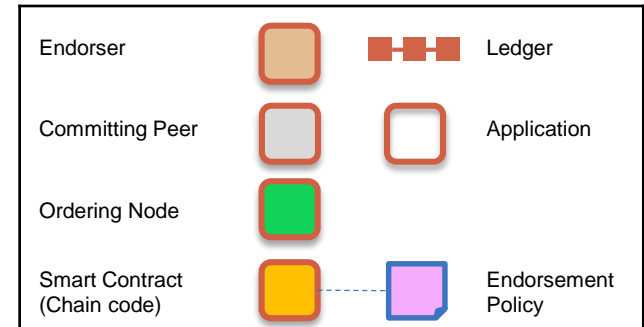|			
Endorser			Ledger
Committing Peer			Application
Ordering Node			
Smart Contract (Chain code)			Endorsement Policy

Sample transaction: Step 3/7 – Proposal Response

Application receives responses

RW sets are asynchronously returned to application

The RW sets are signed by each endorser, and also includes each record version number

(This information will be checked much later in the consensus process)

Key:

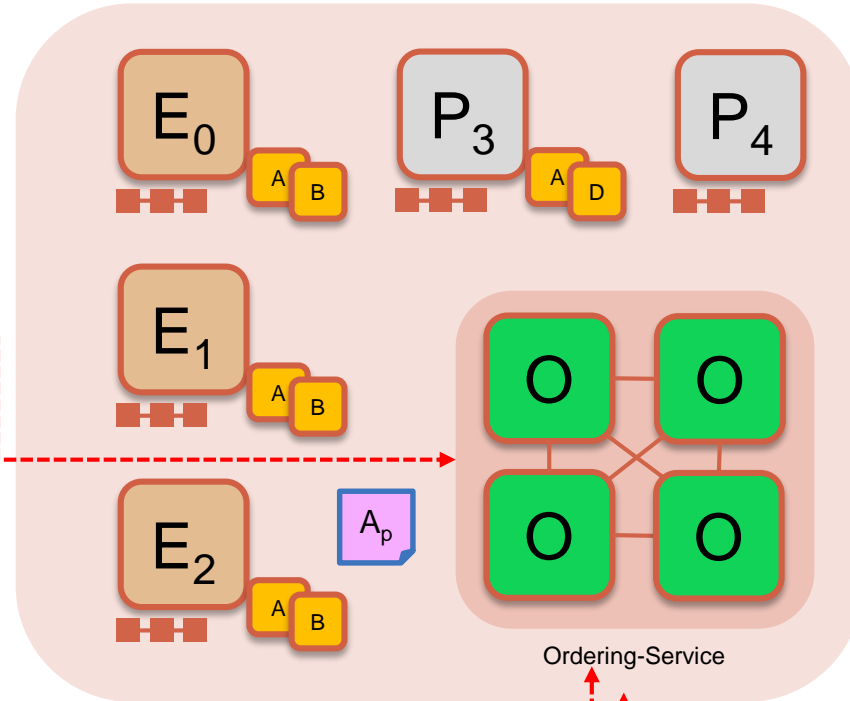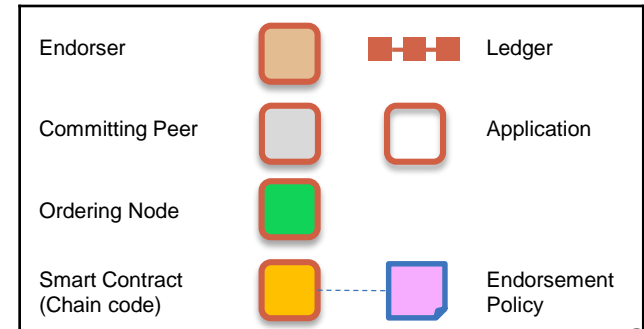|			
Endorser		Ledger	
Committing Peer		Application	
Ordering Node			
Smart Contract (Chain code)		Endorsement Policy	

Fabric

Ordering-Service

Sample transaction: Step 4/7 – Order Transaction

Application submits responses for ordering

Application submits responses as a **transaction** to be ordered.

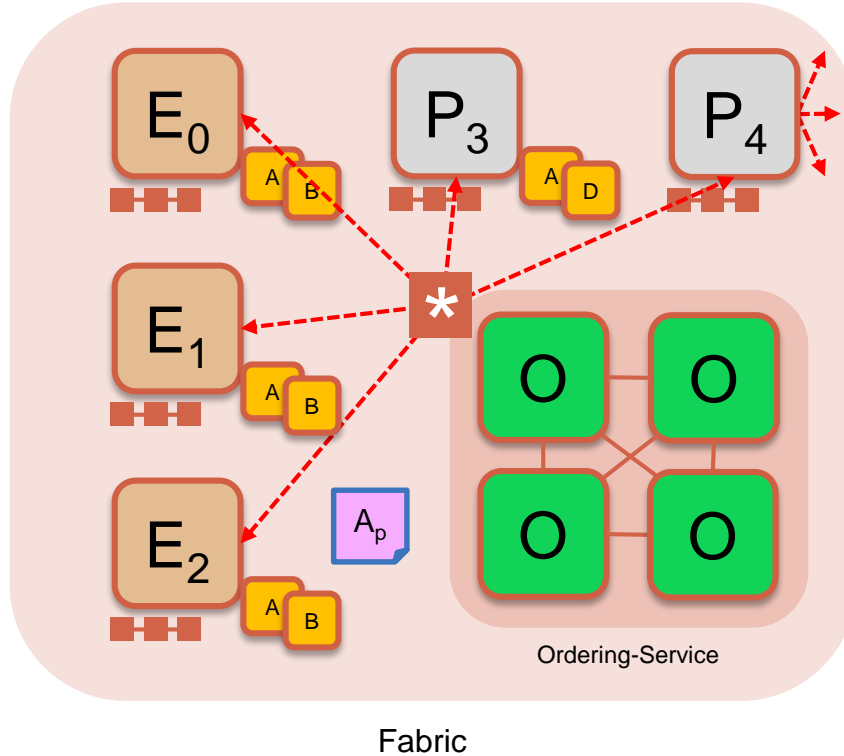Ordering happens across the fabric in parallel with transactions submitted by other applications
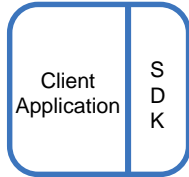
Fabric

(other applications)

Key:

Endorser		Ledger	
Committing Peer		Application	
Ordering Node			
Smart Contract (Chain code)		Endorsement Policy	

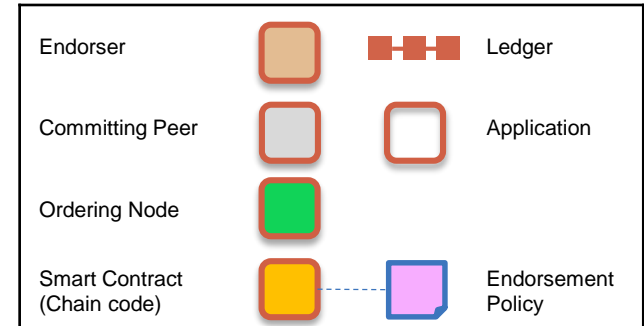# Sample transaction: Step 5/7 – Deliver Transaction

Fabric

Orderer delivers to all committing peers

Ordering service collects transactions into proposed blocks for distribution to committing peers. Peers can deliver to other peers in a hierarchy (not shown)

Different ordering algorithms available:
- SOLO (Single node, development)
- Kafka (Crash fault tolerance)
- SBFT (Byzantine fault tolerance)

Key:

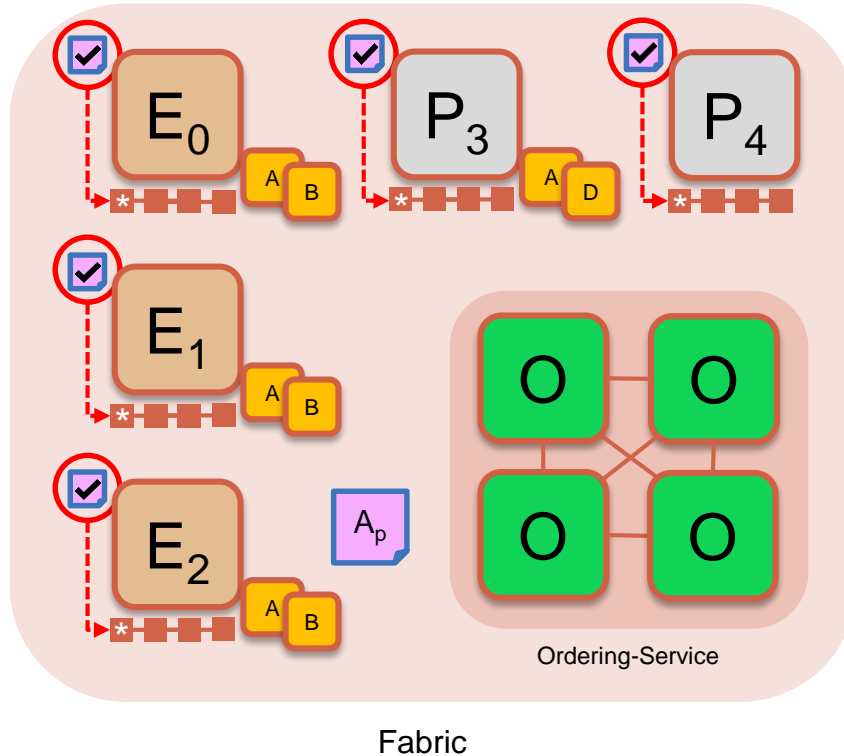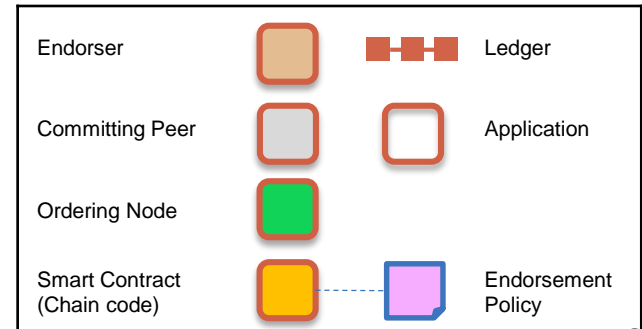|		
Endorser	▨	▬▬▬ Ledger
Committing Peer	▨	▢ Application
Ordering Node	🟩	
Smart Contract (Chain code)	🟧	🟪 Endorsement Policy

Sample transaction: Step 6/7 – Validate Transaction

Committing peers validate transactions

Every committing peer validates against the endorsement policy. Also check RW sets are still valid for current world state

Validated transactions are applied to the world state and retained on the ledger

Invalid transactions are also retained on the ledger but do not update world state
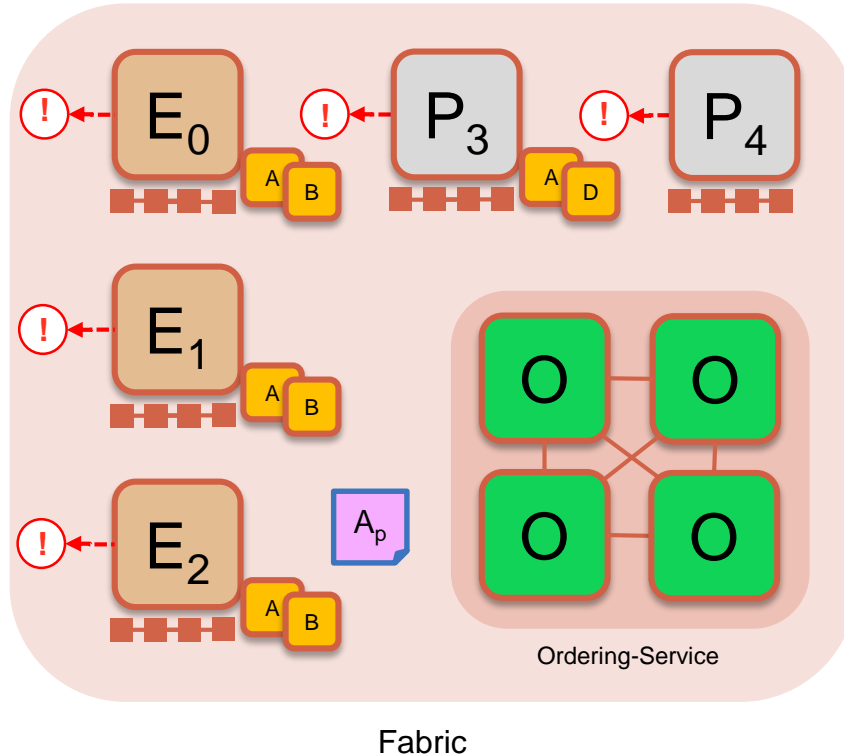
Key:

Endorser		Ledger	
Committing Peer		Application	
Ordering Node			
Smart Contract (Chain code)		Endorsement Policy	

Fabric

Ordering-Service

Sample transaction: Step 7/7 – Notify Transaction

Fabric

Committing peers notify applications

Applications can register to be notified when transactions succeed or fail, and when blocks are added to the ledger

Applications will be notified by each peer to which they are connected

Key:

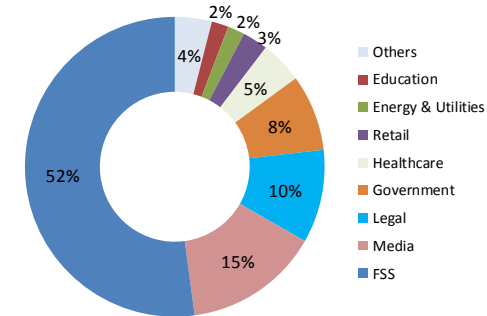|			
Endorser		Ledger	
Committing Peer		Application	
Ordering Node			
Smart Contract (Chain code)		Endorsement Policy	

Use Case Discussion

Blockchain Use Case Characterization & Viability Study

Assessment of use cases across multiple industry segments to build a framework for characterization & use case viability as well as how use cases are being explored in practice

- Financial Services Sector
    - Post- trade clearing & settlement
    - Banking / Market place lending

- Healthcare
    - Patient profile
    - Validation & Payment of claims

- Insurance
    - Claims Processing & Settlement

- Supply chain management
    - Automotive – regulatory tracking

- Media
    - Digital rights for consumer products

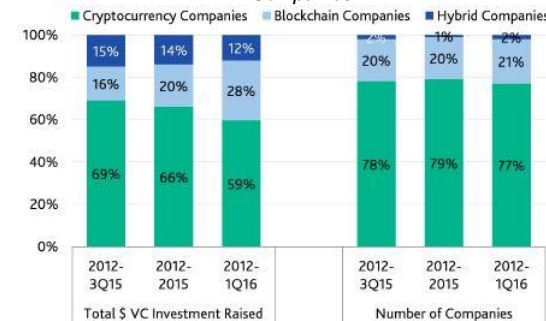- Government
    - Voting
    - Record management

Use Cases by Industry

Broad appeal however Financial Services Sector is 52% of the use cases

Legend:
- Others
- Education
- Energy & Utilities
- Retail
- Healthcare
- Government
- Legal
- Media
- FSS

Values: 4%, 2%, 2%, 3%, 5%, 8%, 10%, 15%, 52%

Source – World Economic Forum | 2016

Pure Play Blockchain Companies Taking away Venture Capital Share from Cyrptocurrency Companies

Legend: Cryptocurrency Companies, Blockchain Companies, Hybrid Companies

	Total $ VC Investment Raised			Number of Companies		
	2012-3Q15	2012-2015	2012-1Q16	2012-3Q15	2012-2015	2012-1Q16
Hybrid	15%	14%	12%		1%	2%
Blockchain	16%	20%	28%	20%	20%	21%
Cryptocurrency	69%	66%	59%	78%	79%	77%

Source – Coindesk, Moody's Investor Service 2016

Framework Created for Use Case Characterization & Viability

1) Is the use case Blockchain Aligned

- Assess if use business case holds characteristics of high-potential Blockchain use cases
    - ❖ Shared repository
    - ❖ Multiple writers
    - ❖ Minimal trust
    - ❖ Intermediaries
    - ❖ Transaction dependencies

- Consider the attributes of Blockchain are important to the use case
    - ❖ Consensus
    - ❖ Provenance
    - ❖ Immutability
    - ❖ Finality

Framework Created for Use Case Characterization & Viability (cont.)

2) Consider the Business Case

– How do they make money or provide service

– How does the process work today

– Who are their partners today – how do they trade assets and information

3) Consider the transactional effects

• What is the asset being ledgered

• What is the longevity of that asset

• What is the requirement for that asset and are there dependencies on other parties to meet that requirement

• What is the rate of these processes

• Is this a short or long term process

31

Framework Created for Use Case Characterization & Viability (cont.)

4) Consider the network effects - there has to be a network

– Who are the core players/users to support this use case

– How do the benefits change as more users are added - is this when a majority of the benefit achieve

– Is this a regulated assets and who is the reporting authority

– If regulated, is there value to starting with just a shadow chain

– What is the level of trust in the network - why is this so

– Is this network reliant on other networks

5) Who is the Anchor Client(s)

– Who has the most to benefit from this network

– Who is the controlling entity/entities for this network

– Who is disrupted by this network and how may they respond

– Does the Business Case justify the investment

32

Use Case – Aircraft Maintenance

What?

- Provenance of each component part in complex system hard to track

- Manufacturer, production date, batch and even the manufacturing machine program.

How?

- Blockchain holds complete provenance details of each component part

- Accessible by each manufacturer in the production process, the aircraft owners, maintainers and government regulators.

Benefits

1. trust increased b/c no authority "owns" provenance

2. improvement in system utilization

3. recalls "specific" rather than cross fleet
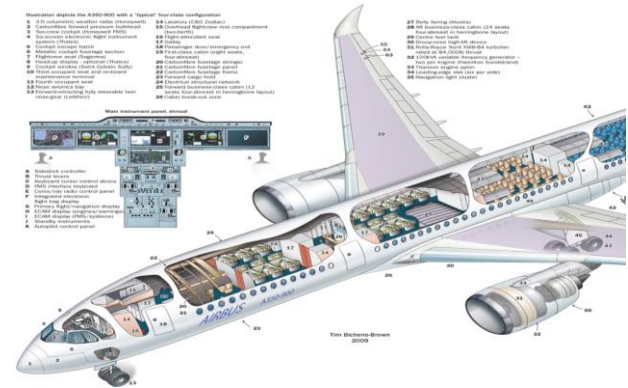
Food supply chain use case

Walmart and IBM Are Partnering to Put Chinese Pork on a Blockchain

A decade ago in the United States, a deadly strain of E. coli in tainted spinach ripped through 26 states, killing three people and sickening more than 200. The outbreak represents what can happen when sourcing food—and tracing contaminations—goes horribly wrong.

"Consumers, in general, stopped eating spinach. Restaurants pulled it off the menu," says Frank Yiannas, vice president of food safety at Walmart (wmt). "If you could track and pinpoint where that came from faster, you could alleviate all that and ensure consumer confidence continues."

This is the impetus behind the retailer's latest unlikely project intended to overhaul the supply chain. Walmart is teaming up with IBM (ibm) and Tsinghua University in Beijing to digitally track the movement of pork in China on a blockchain, also known as a distributed ledger.

Such a system could help prevent disaster scenarios like the fatal, nationwide outbreak described above, Yiannas says.

Walmart plans to use technology developed by the Hyperledger Project, an open source software project that builds blockchain tools and is based out of the Linux Foundation, a non-profit organization that maintains the code for a popular eponymous operating system. The blockchain in question, a private database co-developed by IBM, is designed to provide the retailer with a way to indelibly record a list of transactions indicating how meat has flowed through a commercial network, from producers to processors to distributors to grocers—and finally, to consumers.

"Consumers today want more transparency about where and how a product came to be," Yiannas tells *Fortune* on a call from Beijing. "If you shine a light on the food system, that leads to transparency."

(Courtesy of Walmart)

Paul Chang, a global supply chain lead at IBM, says that the trial represents a substantial improvement over earlier projects that solely used barcodes and radio ID tags. "The missing piece was a shared forum where companies could begin to see each others' transactions and develop trust," he said. "That missing piece is something like the blockchain."

Everledger Rolls Out Blockchain Technology to Digitally Certify Kimberley Diamonds

By **Richard Kastelein** - September 20, 2016

👍 Like 9   🐦 Tweet

37

REUTERS

Business   Markets   World   Politics   Tech   Commentary   Breakingviews   Money   Life

TECHNOLOGY NEWS | Mon Mar 6, 2017 | 12:55pm EST

IBM, Maersk in blockchain tie-up for shipping industry

FILE PHOTO – A woman passes by the IBM offices in New York City, U.S. on October 17, 2016. REUTERS/Brendan McDermid/File Photo

By **Gertrude Chavez-Dreyfuss** | NEW YORK

IBM and Danish transport company Maersk said they were working together to digitize, manage, and track shipping transactions using blockchain technology.

The technology, which powers the digital currency bitcoin, enables data sharing across a network of individual computers. It has gained worldwide popularity due to its usefulness in recording and keeping track of assets or transactions across all industries.

DTCC Partners With IBM, Startups For Blockchain-Based Credit Default Swaps Solution

Laura Shin, ◎ CONTRIBUTOR

I cover Bitcoin, blockchain, fintech, personal finance and career **FULL BIO** ∨

Opinions expressed by Forbes Contributors are their own.

Michael Bodson, president and chief executive officer of the Depository Trust and Clearing Corporation (DTCC) (Andrew Harrer/Bloomberg)

In a step toward turning blockchain from hype to reality, the Depository Trust and Clearing Corporation (DTCC), the central bookkeeper for Wall Street's securities trades, announces it has selected IBM and two blockchain startups, Axoni and R3, to develop distributed ledger software for its post-trade processing.

The new solution will build on the current Trade Information Warehouse service, which manages recording keeping and payments for $11 trillion of credit derivatives and is used by 2,500 buyside firms such as mutual funds and pension funds in more than 70 countries.

CoinDesk IBM, China Unio... × +

www.coindesk.com/ibm-china-unionpay-blockchain-loyalty-exchange/

Search

Most Visited   Bookmarks Toolbar   blockchain   cognitive   IBM Blockchain for Tra...   IBM Blockchain Soluti...

IBM, China UnionPay Develop Blockchain Loyalty Points Exchange

Michael del Castillo (@DelRayMan) | Published on September 23, 2016 at 02:00 GMT

NEWS

374   f   g+   in 52   1

IBM is working with a Chinese credit card company to to create a blockchain-based system for trading loyalty points.

In a proof-of-concept revealed today, IBM and China UnionPay have developed a platform that allows customers to trade points earned through purchases and other incentivized behavior with one another. It's a concept that can be applied to the