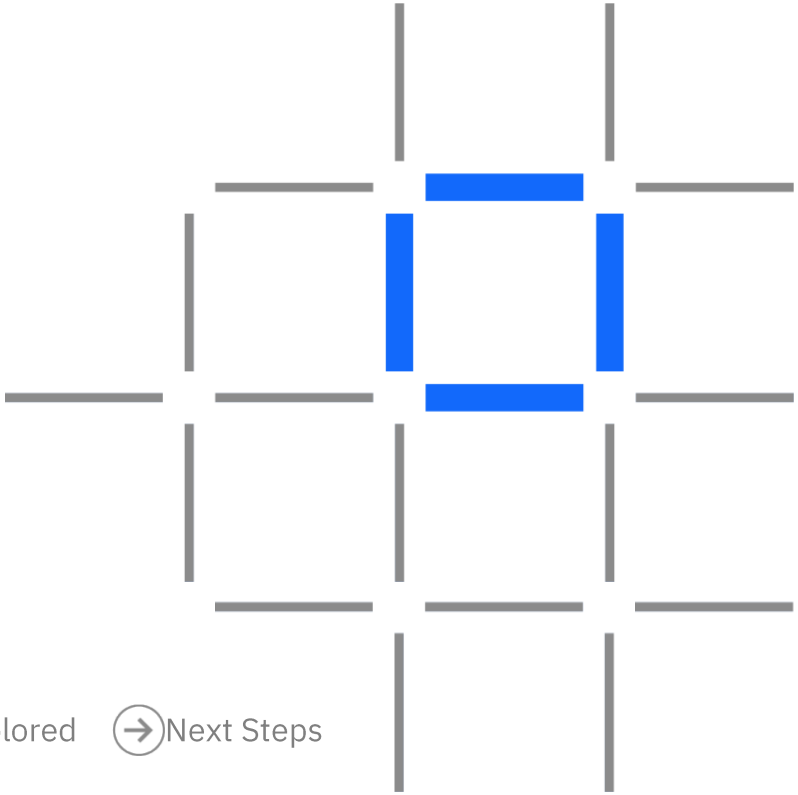
Blockchain Explained

An Introduction to Blockchain for Business

Ronen Siman-Tov
IBM Alpha Zone Accelerator CTO
Certified Thought Leader IT Architect
Jan-30-2018



Blockchain education series

Explained Solutions Composed Architected Explored Next Steps

V5.0, 23 August 2017

What's the Buzz?

Famous Quotes

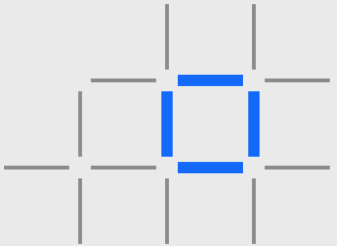
IBM Chief Executive Ginny Rometty.

- "What the internet did for communications, I think Blockchain will do for trusted transactions."

I'm a big believer in the ability of Blockchain technology to effect fundamental change in the infrastructure of the financial service industry."

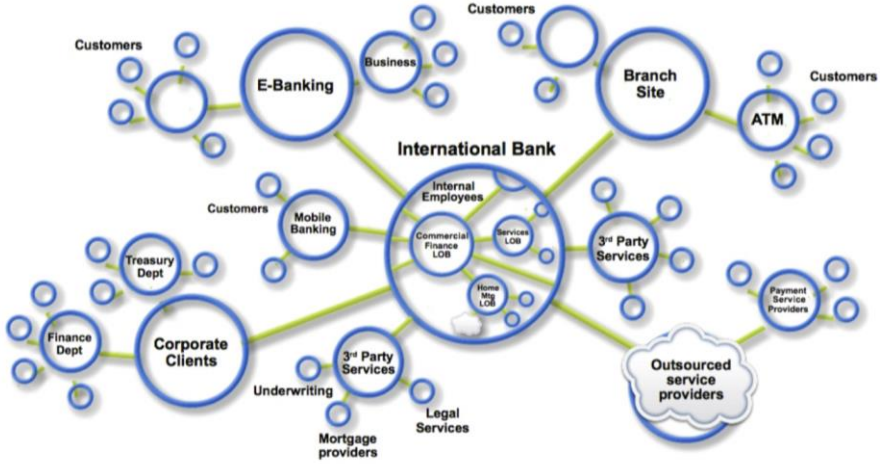
Bob Greifeld, CEO of NASDAQ

Contents



Business networks, wealth and markets

- Business Networks benefit from connectivity
  - Participants are customers, suppliers, banks, partners
  - Cross geography & regulatory boundary
- Wealth is generated by the flow of goods & services across business network in transactions and contracts
- Markets are central to this process:
  - Public (fruit market, car auction), or
  - Private (supply chain financing, bonds)



Transferring assets, building value

Anything that is capable of being owned or controlled to produce value, is an asset

Two fundamental types of asset

- Tangible, e.g. a house
- Intangible, e.g. a mortgage

Intangible assets subdivide

- Financial, e.g. bond
- Intellectual, e.g. patents
- Digital, e.g. music

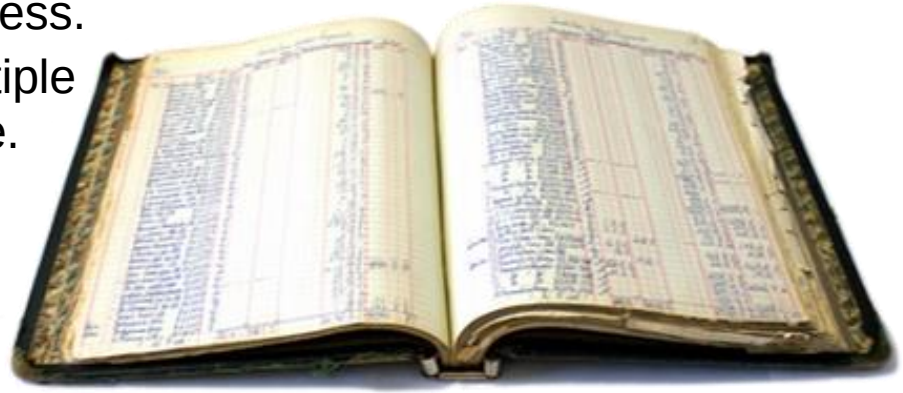
Cash is also an asset

- Has property of anonymity

Ledgers are key

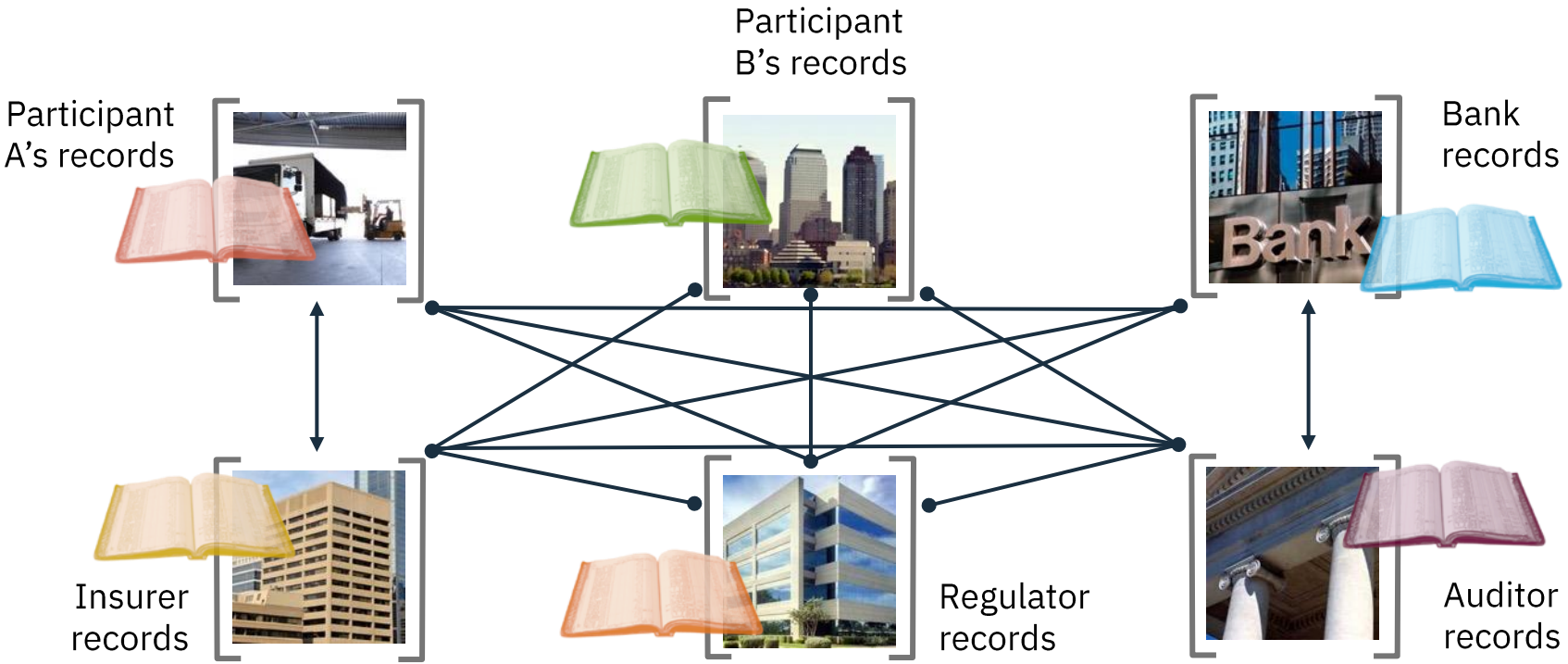
Ledger is THE system of record for a business.

Business will have multiple ledgers for multiple business networks in which they participate.



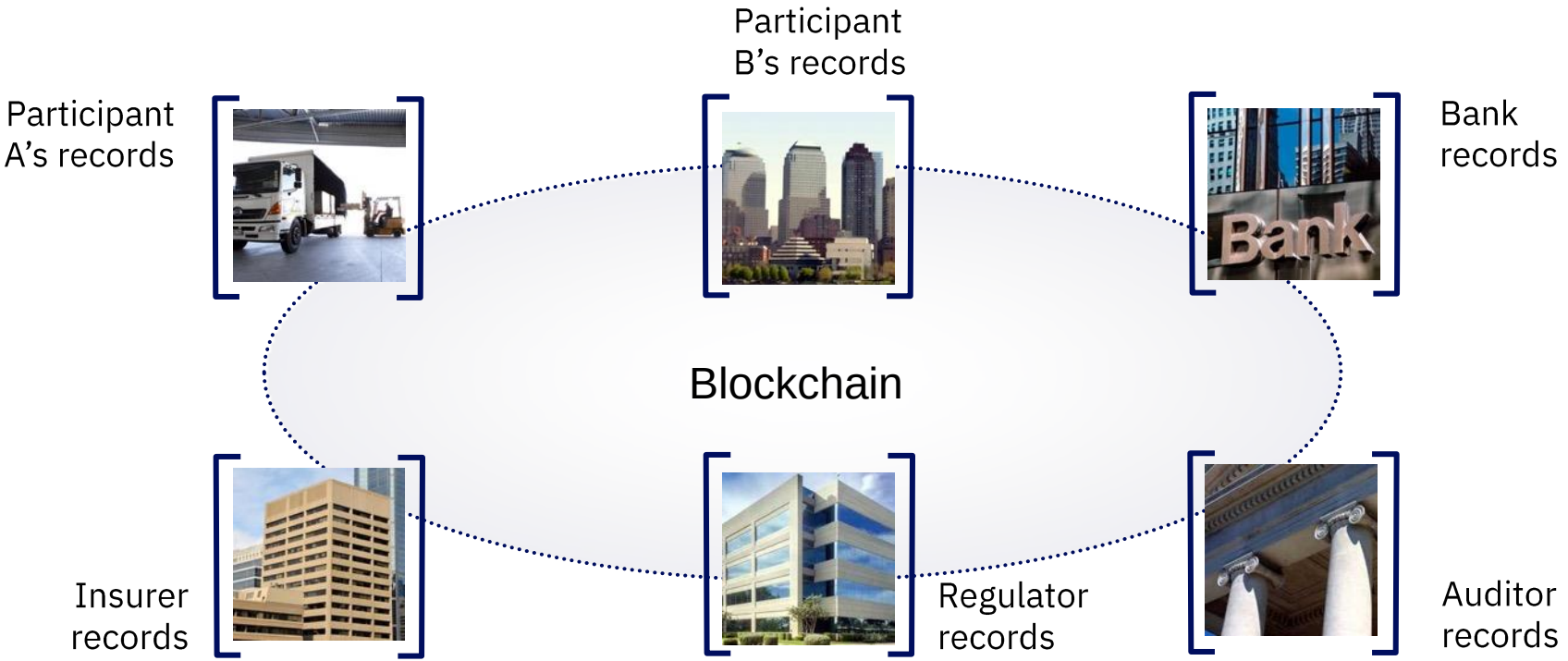
- Transaction – an asset transfer onto or off the ledger
  - John gives a car to Anthony (simple)
- Contract – conditions for transaction to occur
  - If Anthony pays John money, then car passes from John to Anthony (simple)
  - If car won't start, funds do not pass to John (as decided by third party arbitrator) (more complex)

Problem ...



... inefficient, expensive, vulnerable

A shared, replicated, permissioned ledger …



… with consensus, provenance, immutability and finality

Blockchain underpins Bitcoin

bitcoin is:

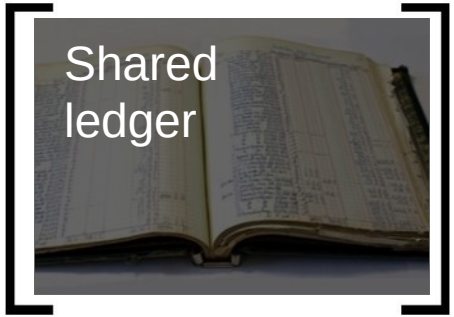
- An unregulated shadow-currency
- The first blockchain application
- Resource intensive

Blockchain for business differs in key areas:

- Identity over anonymity
- Selective endorsement over proof of work
- Assets over cryptocurrency

Requirements of blockchain for business

Append-only distributed system of record shared across business network



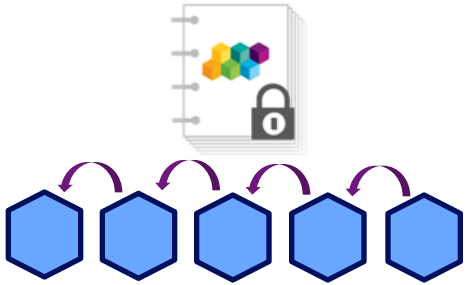
Business terms embedded in transaction database & executed with transactions

Ensuring appropriate visibility; transactions are secure, authenticated & verifiable

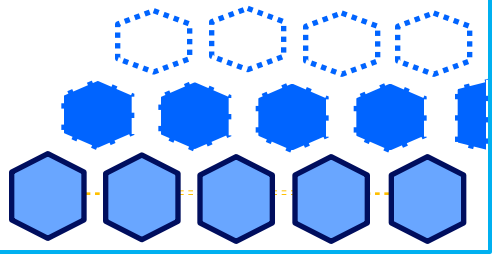
Transactions are endorsed by relevant participants

Essential Properties of a Blockchain

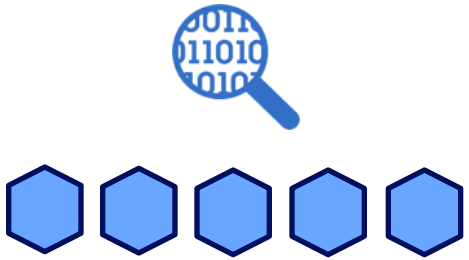
Secure and immutable



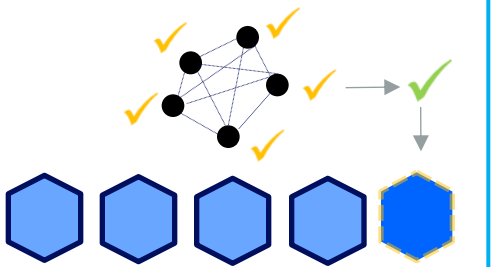
Distributed and Sustainable



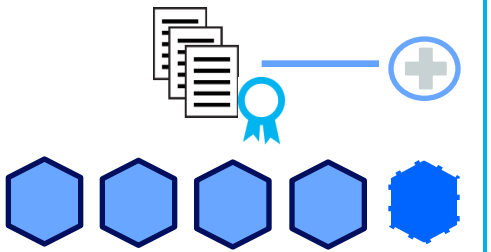
Transparent and Auditable



Consensus based Transactions



Smart Contracts



Blockchain benefits

Saves
time

Transaction time reduced from days to near instantaneous

Removes
cost

Overheads and cost intermediaries

Creates
transparency

Access to data among all participants

Reduces
risk

Tampering, fraud & cyber crime

Contents

What is Blockchain?

Why is it relevant for our business?

How can IBM help us apply blockchain?

Blockchain is creating extraordinary opportunities for businesses to come together in new ways

IBM Blockchain

Create New Value

Exploit new business models and eliminate inefficiencies

Optimize Ecosystems

Streamline business processes and the exchange of value along your ecosystem

Reduce Risk

Replace uncertainty with transparency and a trusted decentralized ledger

Further examples by (selected) industry

Financial

- Trade Finance
- Cross currency payments
- Mortgages

Public Sector

- Asset Registration
- Citizen Identity
- Medical records
- Medicine supply chain

Retail

- Supply chain
- Loyalty programs
- Information sharing (supplier – retailer)

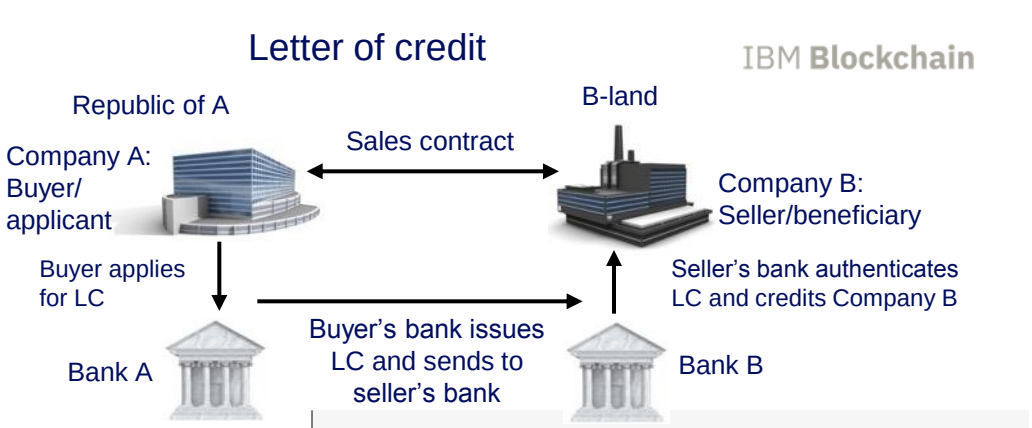
Insurance

- Claims processing
- Risk provenance
- Asset usage history
- Claims file

Manufacturing

- Supply chain
- Product parts
- Maintenance tracking

Example: Letter of credit



What

- Bank handling letters of credit (LOC) wants to offer them to a wider range of clients including startups
- Currently constrained by costs & the time to execute

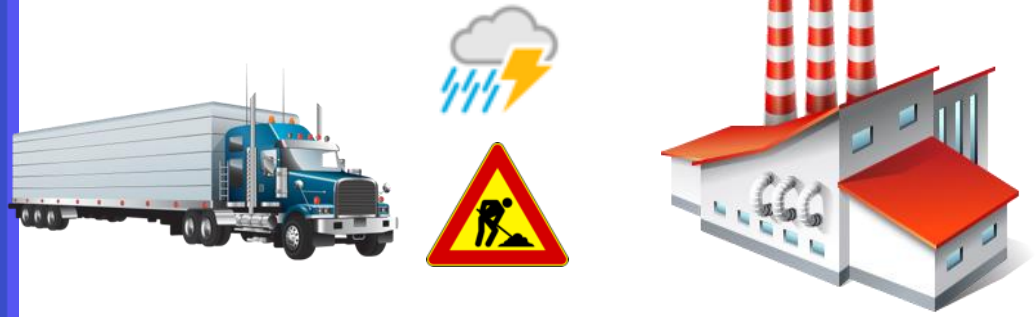
How

- Blockchain provides common ledger for letters of credit
- Allows all counter-parties to have the same validated record of transaction and fulfillment

Benefits

1. Increase speed of execution (less than 1 day)
2. Vastly reduced cost
3. Reduced risk, e.g. currency fluctuations
4. Value added services, e.g. incremental payment

Aerospace Use Case –
Supply Chain



What

- Improve efficiency of inbound logistics to final assembly plant
- Share detailed part info, location and timestamp with suppliers, 3PL logistics providers, transportation companies and assembly plant
- Enable near real-time look up of part location and inventory level for improved production planning

How

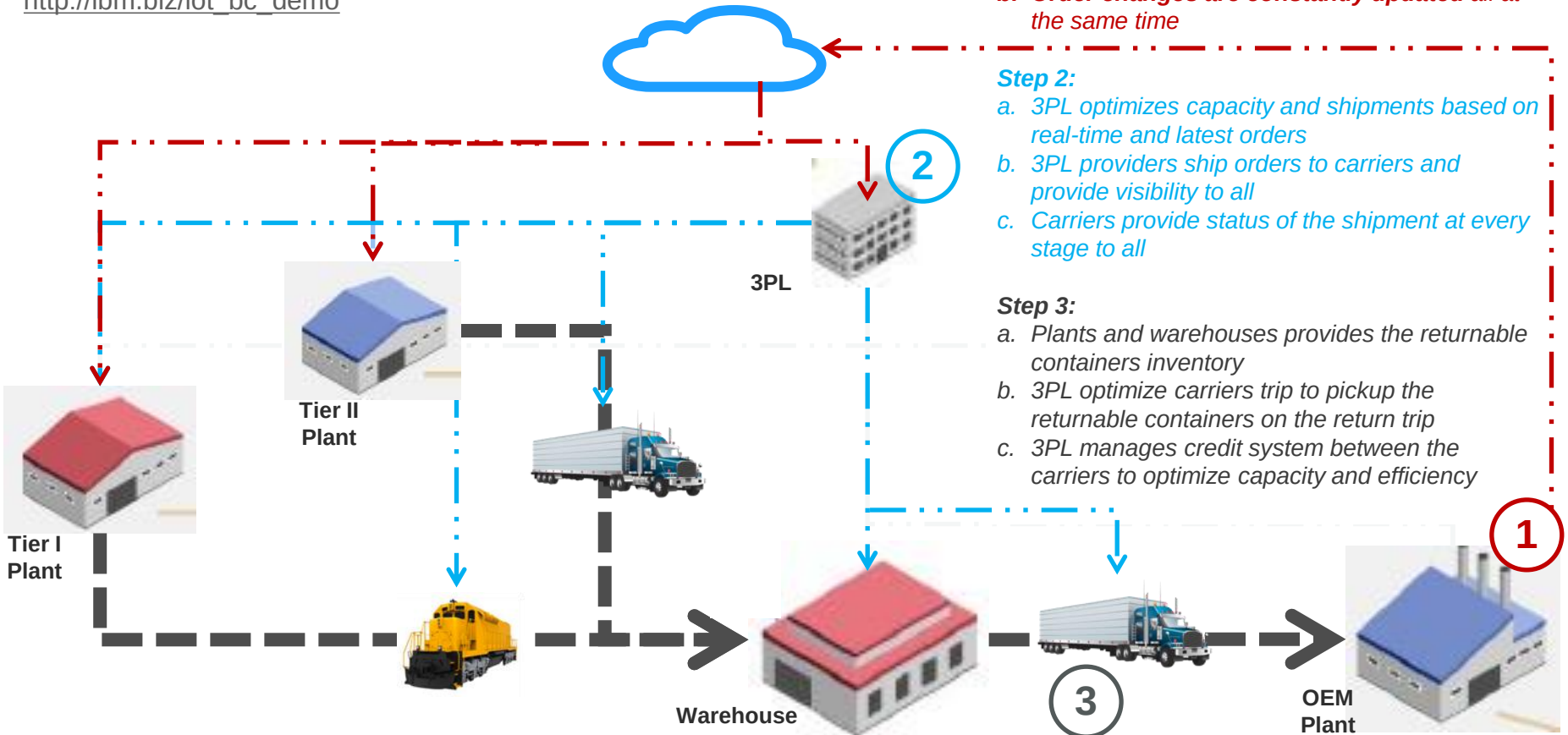
- Send part dispatch and arrival events to shared ledger
- Blockchain holds clear record of transactions and traceable record of responsibility for parts at each stage of shipment process

Benefits

1. Greater transparency between contracting parties
2. Easier production planning at Manufacturer's Plant
3. Reduce inventory and production lead times
4. Reduce number of trips where trucks are travelling empty by offering credit exchange

Inbound Logistics

http://ibm.biz/iot_bc_demo



Aerospace Use Case
Documentation Traceability

What

- Provide easy traceability of aircraft, sub-systems and parts test certifications to customer airlines and regulators
- Blockchain uses encryption and permissioned access so only direct stakeholders have visibility of information

How

- As an aircraft part or sub-system moves through the manufacturing plant, send test certification results to the shared ledger
- Connect shared ledger with IoT devices and document management system for an automated process

Benefits

1. Reduce time to commission a new or repaired aircraft as accurate, detailed certification info is easily accessible
2. Regulator has full visibility
3. Faster turnaround times for aircraft maintenance as documentation flow gets digitized

Aerospace Use Case
Provenance of Parts, Spares

What

- Aircraft are complex systems with multiple parts. Tracing provenance of component parts and spares to back to their real origin is difficult
- In some markets use of counterfeit or end-of-life parts are prevalent

How

- Send details of manufacturer, production date, batch no. and manufacturing machine for each part made to shared ledger
- Blockchain holds transparent record for easy lookup of part origin, certification and expiry date by manufacturer, airlines and regulators

Benefits

1. Reduce usage of counterfeit parts and consequent brand damage
2. Recalls can be "specific" rather than cross fleet
3. Reduced cost of Warranty as parts are easily traceable

Aerospace Use Case

Connected Platform: Software BOM

What

- Manage the Bill of Materials for all software installed on an aircraft
- Create an immutable record of all current and previous software applications and firmware versions installed on the airframe, key sub-systems and parts
- Share with airlines, suppliers, MROs, regulator

How

- Send a record of the software version as it is installed to the shared ledger
- Enable permissioned parties to view and search the shared ledger

Benefits

1. Easy lookup of accurate, historical record of software versions installed accelerates fault diagnosis, test certification and maintenance activities
2. Greater information transparency reduces disputes between airline and manufacturer

Bosch and IBM develop Fake Product Detection POC

Implemented in < 3 months with a small team from both sides in Watson IoT Lab, Munich

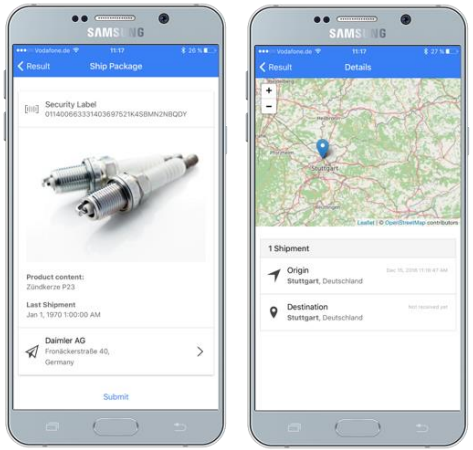
Advantages:

- ✓ Transparency on product logistics
- ✓ Potential cost savings
- ✓ Improved fake detection granularity
- ✓ Identification of gray market imports

Extensible to other business cases like

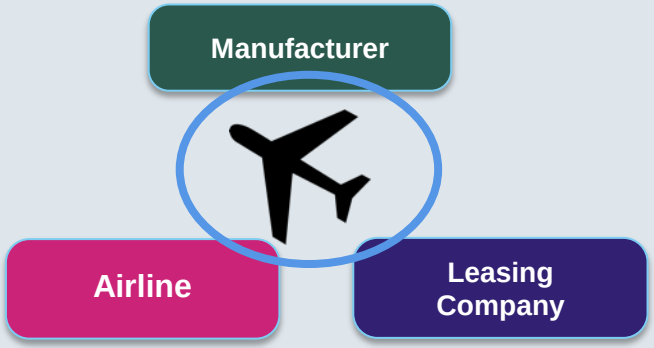
- Logistic chain
- Sharing economy e.g. car/ebike sharing
- Supply chain and parts authentication
- Community-based parking
- Healthcare

Future connection to Watson IoT



https://youtu.be/jY8HFRs6Y4s?t=16m13s

Aerospace Use Case
Aircraft Leasing



What

- Airline sells aircraft to Leasing Co. on a lease-back contract but Leasing Co. finds it difficult to agree a fair buy-back price for aircraft at end of contract
- Airline securely shares aircraft flying and maintenance data with Leasing Co., Insurance Co. and Manufacturer

How

- Capture aircraft usage [take-offs, landings, sensor data] and send threshold event info to shared ledger
- Threshold events and other transactions stored as blocks on the Blockchain and shared with permissioned parties in the network

Benefits

1. Greater transparency
2. Increased trust as all parties get single consistent view
3. Leasing Co. able to pay fair price for aircraft buy-back from Airline as have detailed record of aircraft history
4. Enable new business models

International Business Times

UK | World | Business | Politics | Fintech | Technology | Science | Sport | Entertainment | Opinion | Video

Economy | Companies | Markets | Finance | Regulation

Business | Fintech | Blockchain

Deutsche Bank, HSBC, Societe Generale choose IBM for trade finance blockchain

Digital Trade Chain Consortium also includes KBC, Natixis, Rabobank and Unicredit.

By Ian Allison

June 27, 2017 00:01 BST

HSBC

UniCredit

SOCIETE GENERALE

NATIXIS BEYOND BANKING

KBC

Rabobank

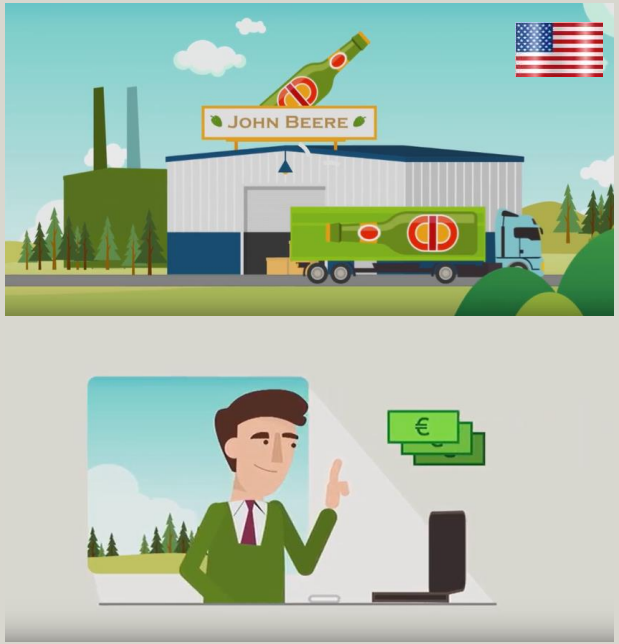
Deutsche Bank

The Challenge of Trade Finance for SMBs

Trust

Time

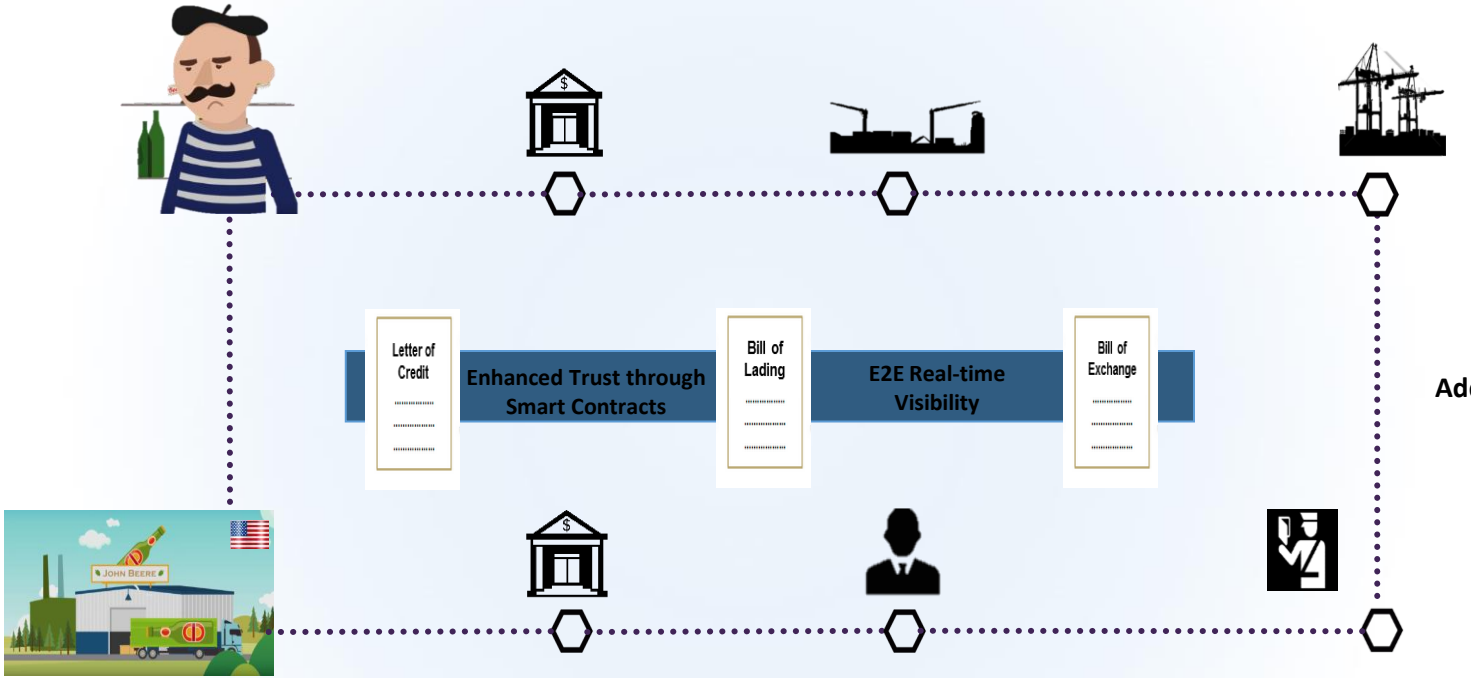
Finance



Today’s International Trade: Inefficiencies and Risks

Risks

Blockchain-Enabled Future State



$14T Finance → $30B Paperless → Weeks → Minutes

IBM and Maersk announce global trade solution based on Blockchain

http://www-03.ibm.com/press/us/en/pressrelease/51712.wss

90% of goods in global trade are carried by the ocean shipping industry each year

MAERSK

Solution to manage and track the paper trail of tens of millions of shipping containers across the world by digitizing the supply chain process

- To be offered to parties operating in the shipping and logistics industry
- To enhance transparency by securely sharing of information among trading partners
- Will show a detailed view a container's progress through the supply supply chain
- Will improve Workflow and Real Time Visibility on the Status of Each Shipment
- Enable view of status of customs documents, bills of lading and other data

When adopted at scale, the solution has the potential to save the industry billions of dollars by reducing fraud and errors and reducing the time products spend in the transit

Food Safety Consortium built on IBM Blockchain Platform

Walmart

Nestlé

Dole

Driscoll's

gsf golden state foods

Tyson

McLane

McCormick

Kroger

Unilever

News Announcements:

22 Aug 2017: **Walmart** and a group of leading companies across the global food supply chain announced a major Blockchain collaboration with IBM

19 Oct 2016 - Walmart opened its new **Walmart Food Safety Collaboration Center** in Beijing. **Walmart and Tsinghua University** announced a collaboration to improve the way food is tracked, transported and sold to consumers across China

- **Business Values:**
  - Food traceability
  - Food quality assurance
  - Food fraud prevention
  - Compliance with food, agriculture and labor regulations
  - Paper-less Operational costs saving
  - Market Potential – Billions of USD
- **IBM Technologies & Services:**
  - Blockchain Garage Services
  - GBS Consulting
  - IBM Blockchain
  - Watson IoT
  - IBM HSBN (Highly Secured Blockchain Network

Blockchain in Healthcare

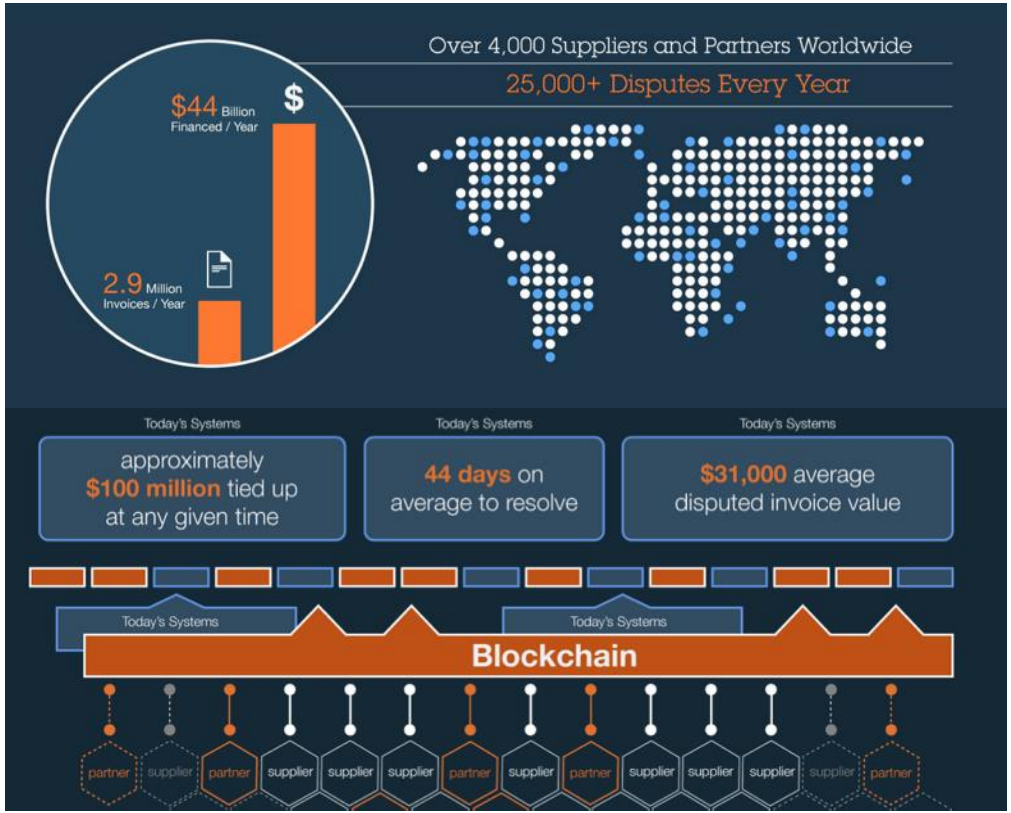
Blockchain is good for your health, and your business

EMR: Supporting the entire lifecycle of a patient's EMR
Counterfeit drug prevention and detection: anti-tampering capabilities.
Clinical trial results: Accountability and transparency to the clinical trial reporting process.
Internet of Things: Patient's IoT data and EMR integration

IBM Watson Health has partnered with US Food and Drug Administration to explore the use of health data transfers from wearables and other IoT devices using blockchain.

IBM Global Financing using Blockchain to address Dispute Resolution

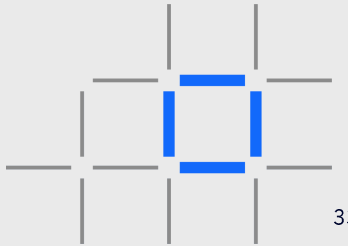
https://youtu.be/0DSNdLDOZ5w



Blockchain utilized to significantly improve resolution time for common disputes

- Utilized data available from suppliers to deliver enhanced information to both Suppliers and Business Partners
- Accomplished with no code changes to our core Commercial Financing system using shadow ledge approach
- Integrated blockchain into existing user interface
- Enhanced data includes key information regarding shipments status which minimizes proof of delivery disputes
- Established a 'platform' for competitive advantage
- Continuing to work with our Suppliers and Business Partners to further expand Blockchain capabilities

Contents



Hyperledger: A Linux Foundation project

- A collaborative effort created to advance cross-industry blockchain technologies for business
- Announced December 2015, now around 150 members
- Open source, open standards, open governance
- Five frameworks and three tools projects
- IBM is a premier member of Hyperledger

Brian Behlendorf
Executive Director

Blythe Masters
Board Chair

Chris Ferris
TSC Chair

www.hyperledger.org

Hyperledger members

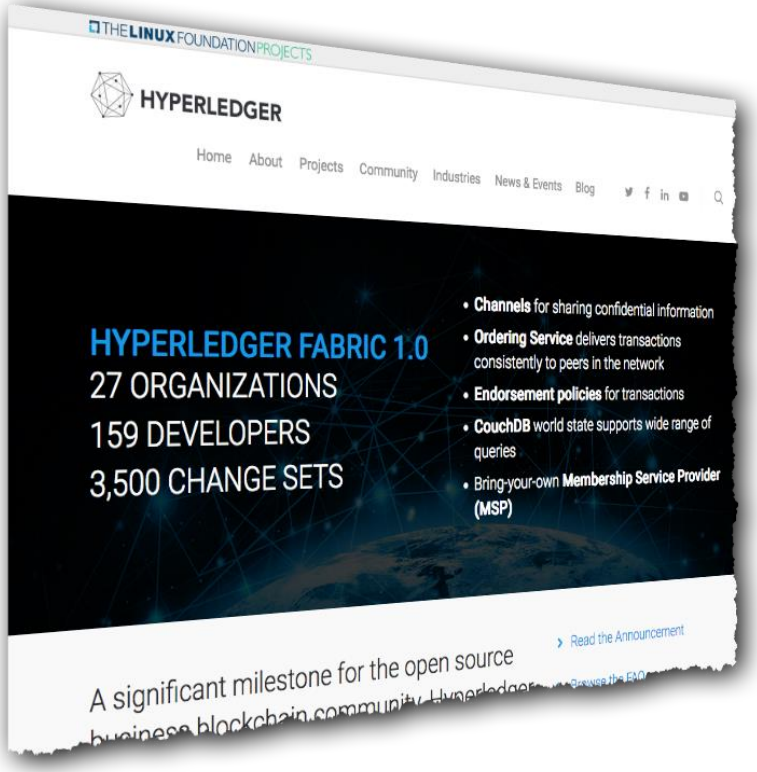
Premier

General

Associate

Source: https://www.hyperledger.org/about/members
Updated 21 August 2017

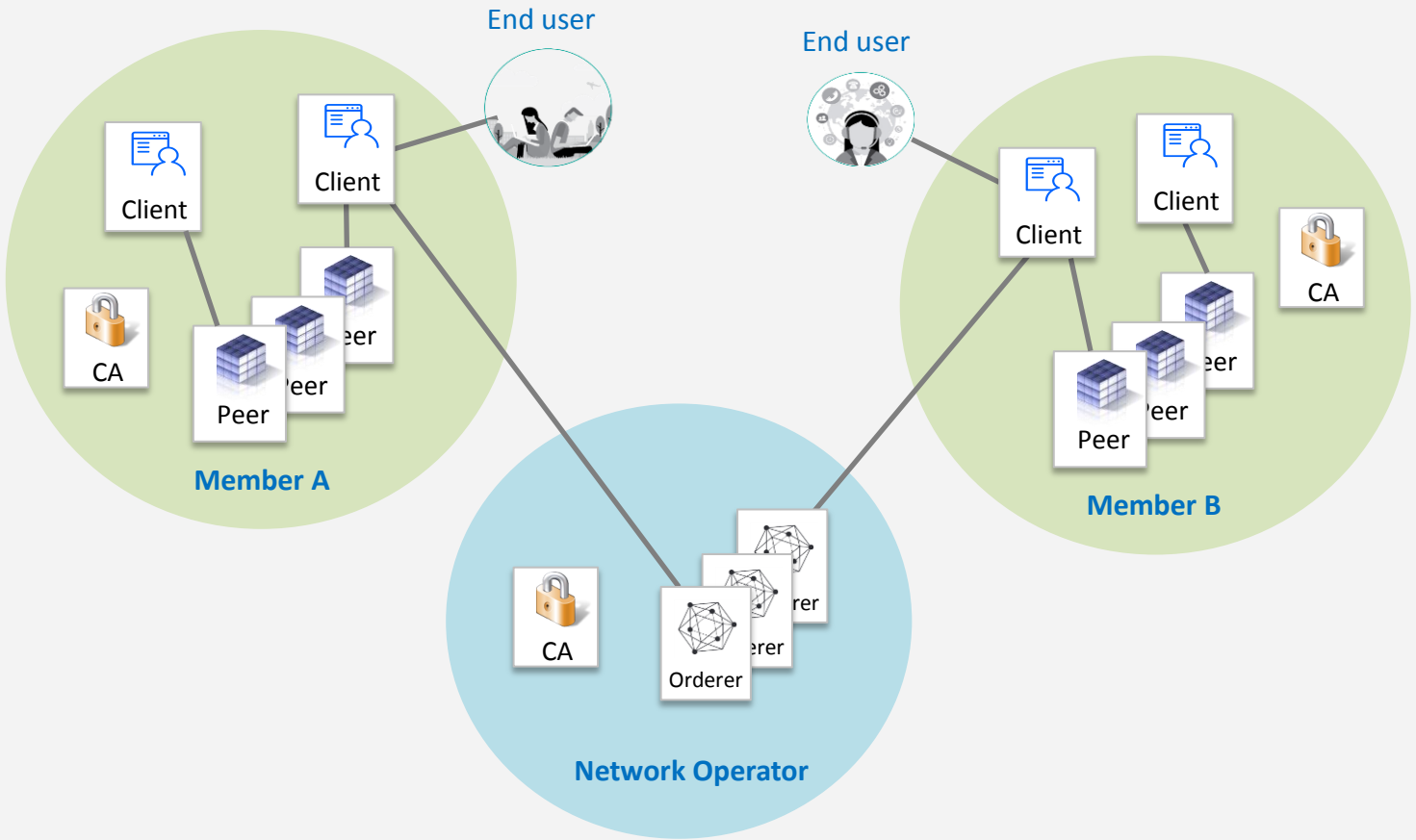
Hyperledger Fabric: Distributed ledger platform



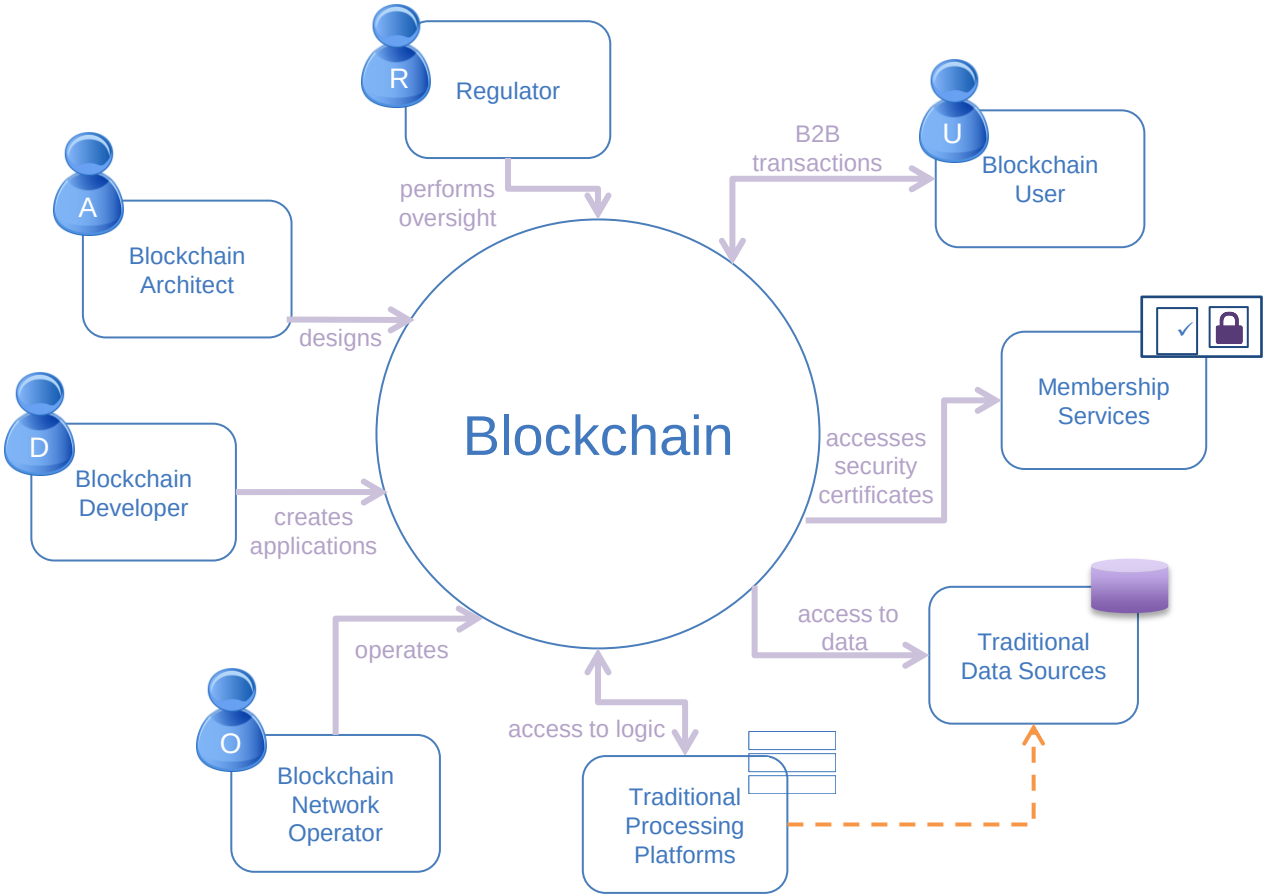
- An implementation of blockchain technology that is a foundation for developing blockchain applications
- Emphasis on ledger, smart contracts, consensus, confidentiality, resiliency and scalability.
- V1.0 released July 2017
  - 159 developers from 27 organizations
  - IBM is one contributor of code, IP and development effort to Hyperledger Fabric

http://hyperledger-fabric.readthedocs.io/

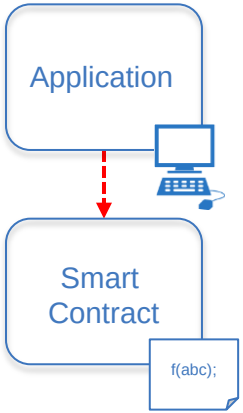
Business Network Example

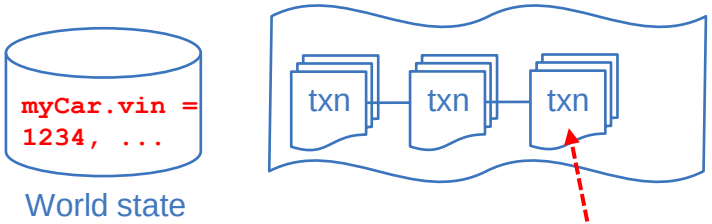


Actors in a blockchain solution



Working with the ledger: Example of a change of ownership transaction





Transaction input - sent from application

```
invoke(myContract, setOwner,
       myCar, Matt)
...
```

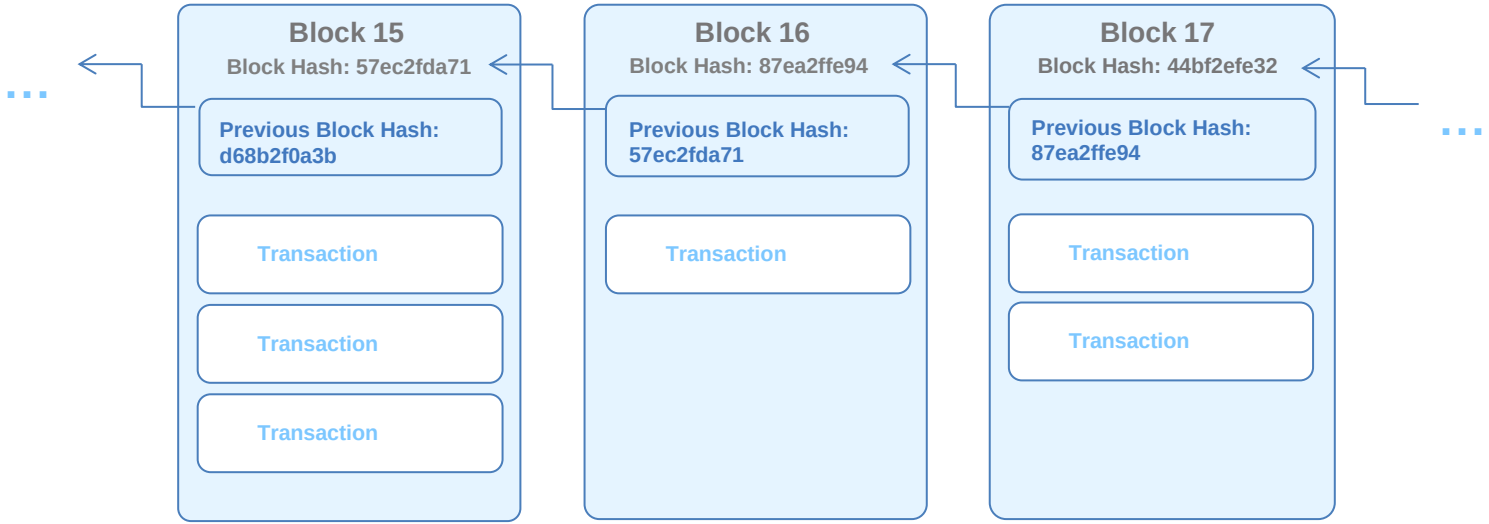
Smart contract implementation

```
setOwner(Car, newOwner) {
   set Car.owner = newOwner
}
```

World state: new contents

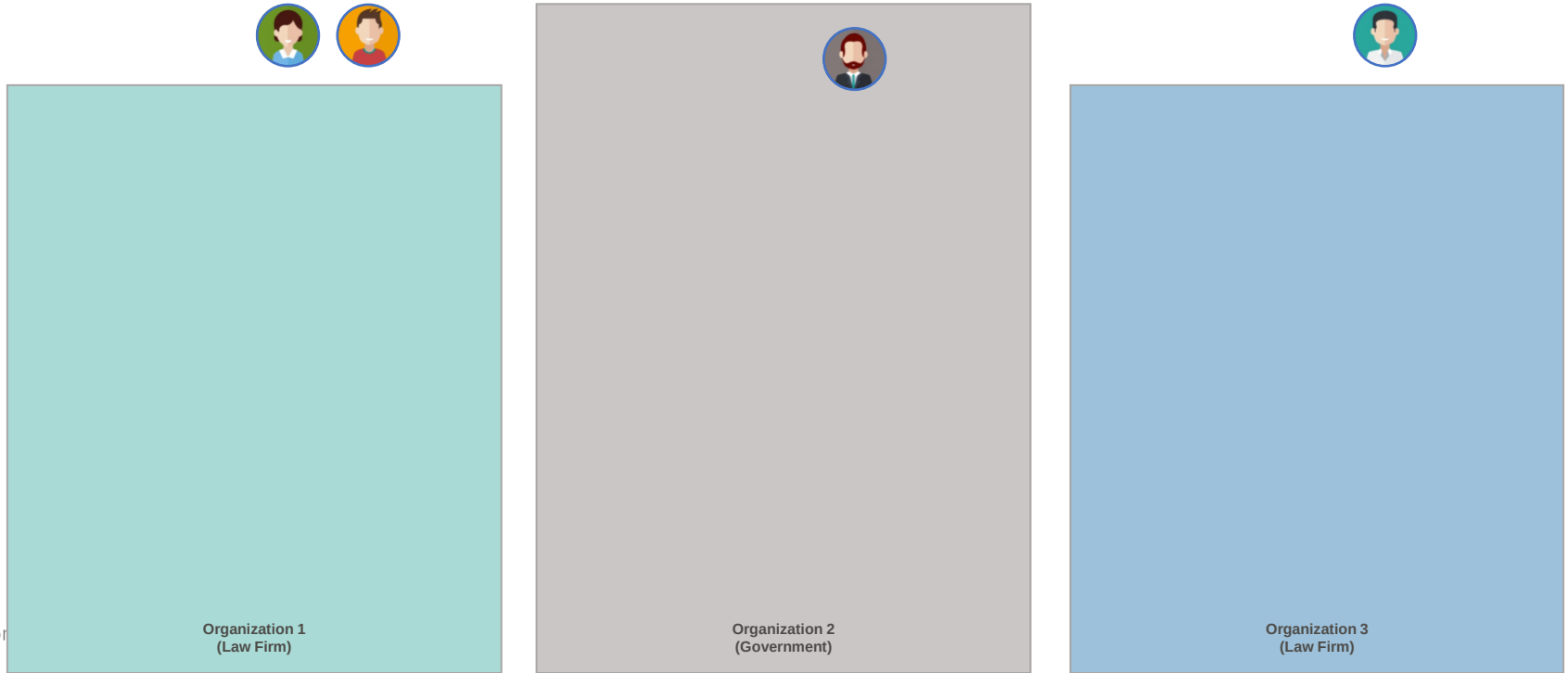
```
myCar.vin = 1234
myCar.owner = Matt
myCar.make = Audi
...
```

Block detail

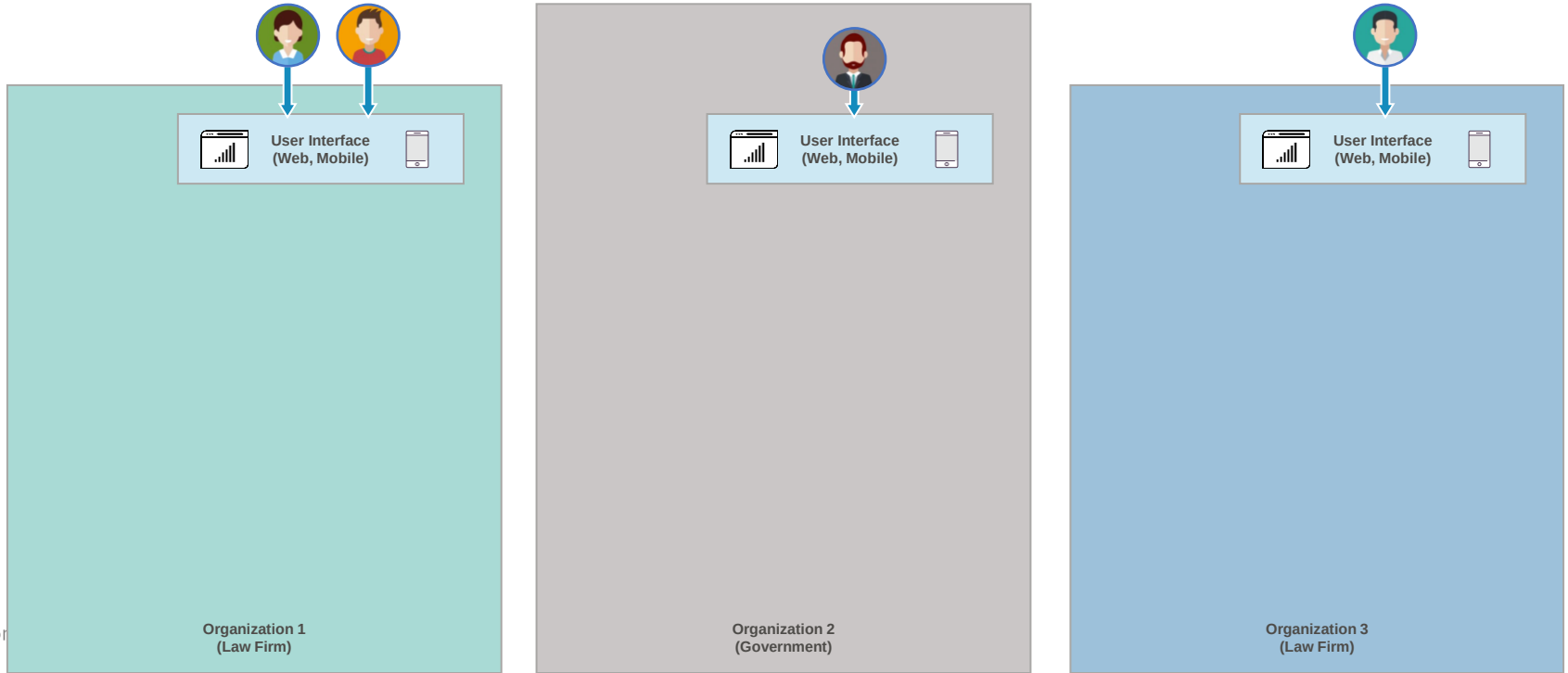


- A blockchain is made up of a series of blocks with new blocks always added to the end
- Each block contains zero or more transactions and some additional metadata
- Blocks achieve immutability by including the result of a hash function of the previous block
- The first block is known as the “genesis” block

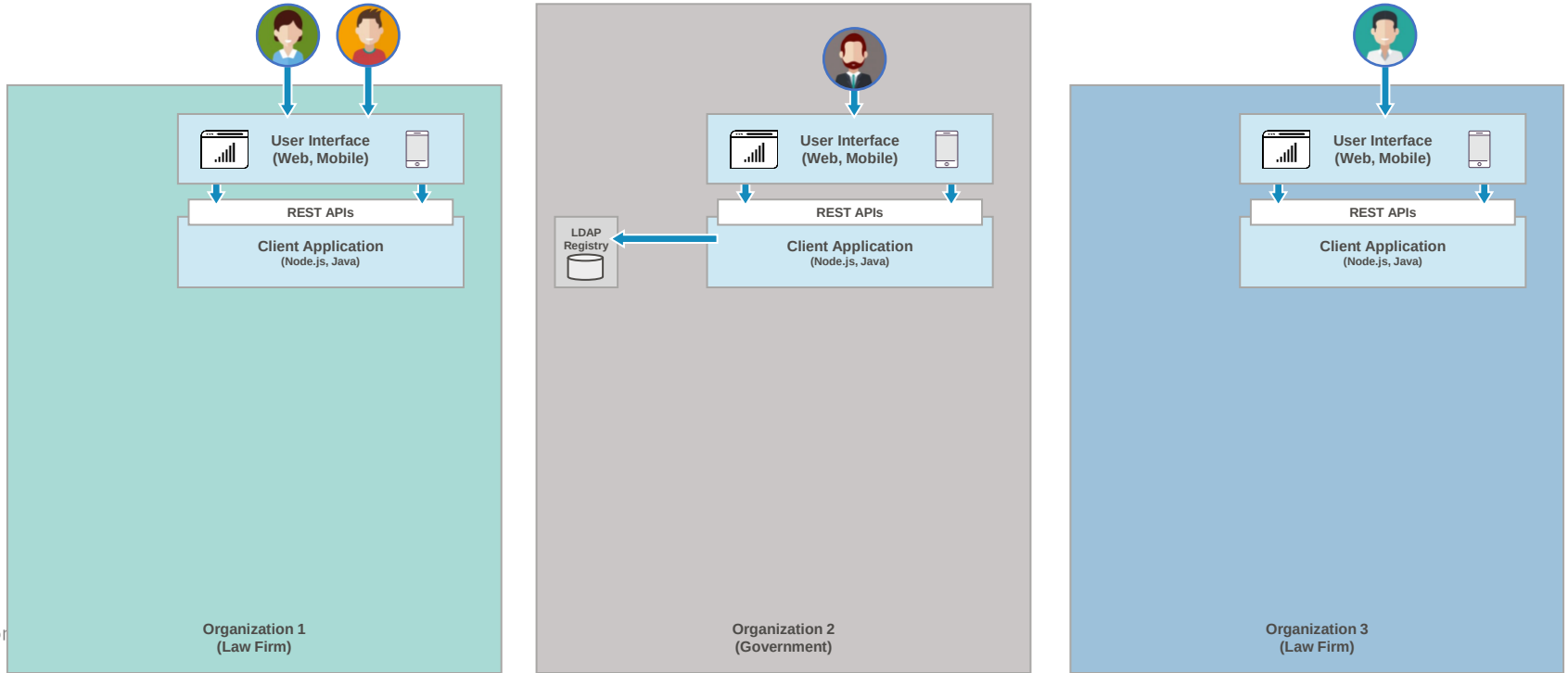
Blockchain is a team sport, so it's important to begin with the perspective of multiple organizations that want to work together, and the individuals who will be interacting with the blockchain-based solution via those organizations. This is a **business network**.



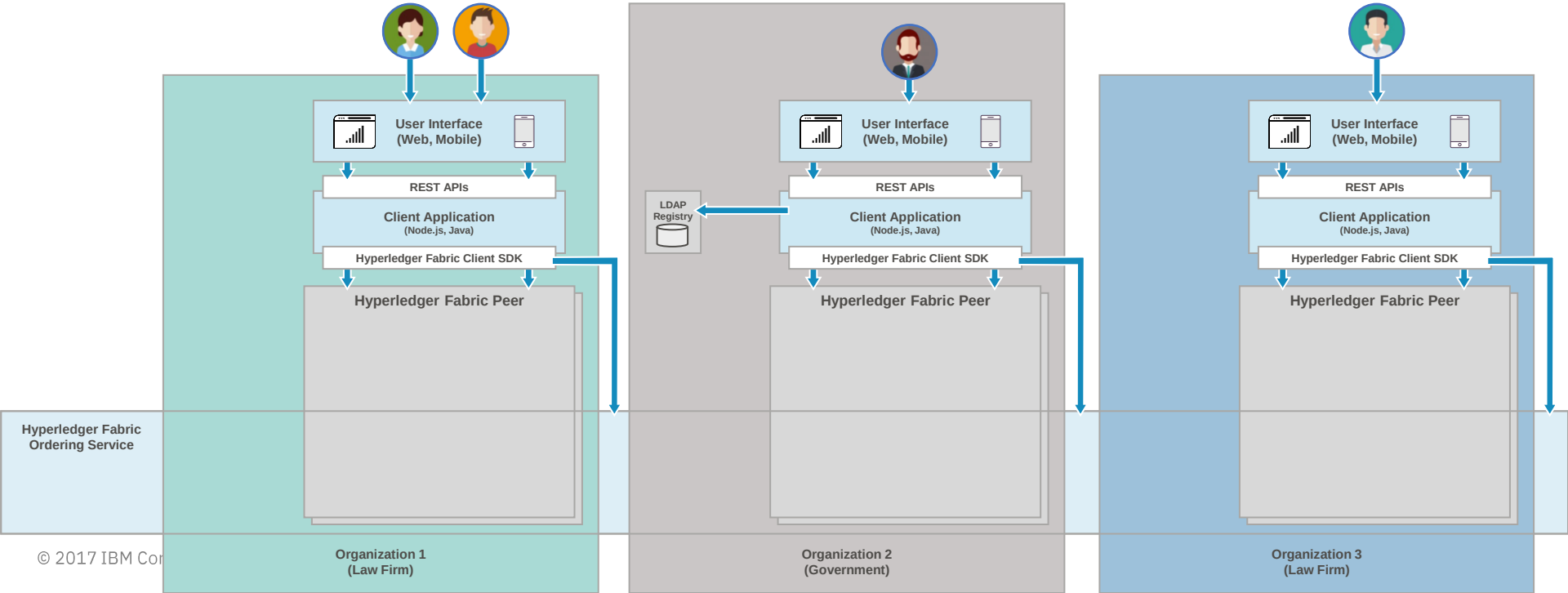
Individuals interact with public-facing and organization-internal applications, through a variety of user interfaces (mobile, web, etc.)



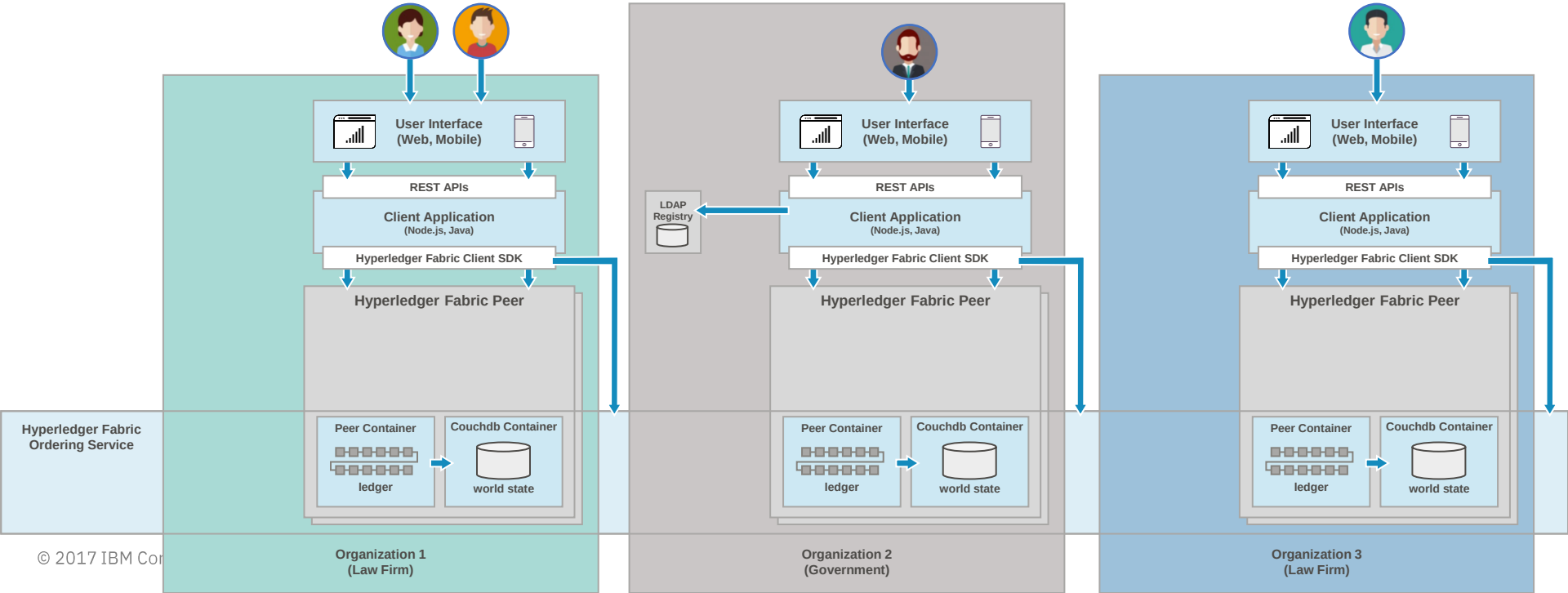
User interfaces typically communicate with backend applications through REST APIs which expose functionality to the UI layer according to the business domain of the application. Applications have various ways of authenticating users (e.g. LDAP, SSO, OAUTH, etc.)



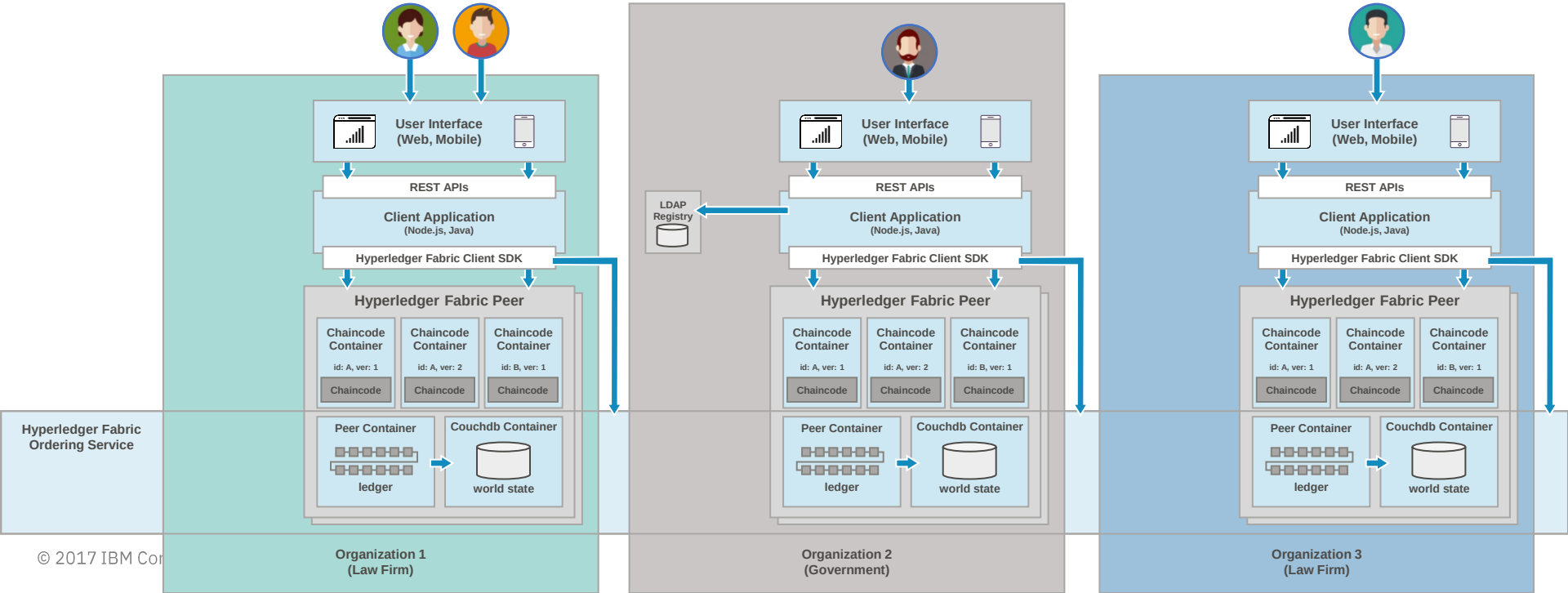
In a Hyperledger Fabric application, the application layer acts as a **blockchain client**, in that it connects to the Fabric components (using the Hyperledger Fabric Client SDK) on behalf of the user in order to query the ledger and execute transactions.



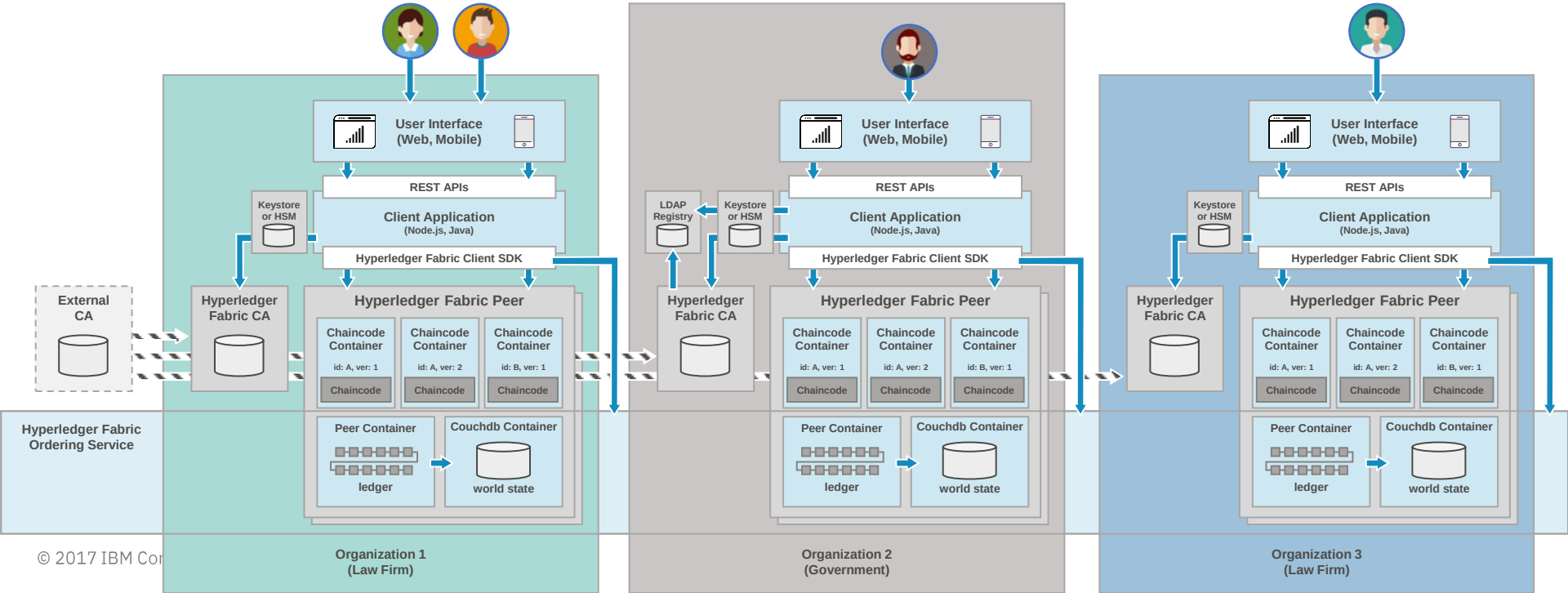
Peers are a primary concept in Hyperledger Fabric. A peer is a Fabric application component that runs in a Docker container and is responsible for maintaining a copy of the ledger, and providing programmatic access to the information on the ledger via the world state DB. An organization will typically have more than one peer, primarily for high availability.



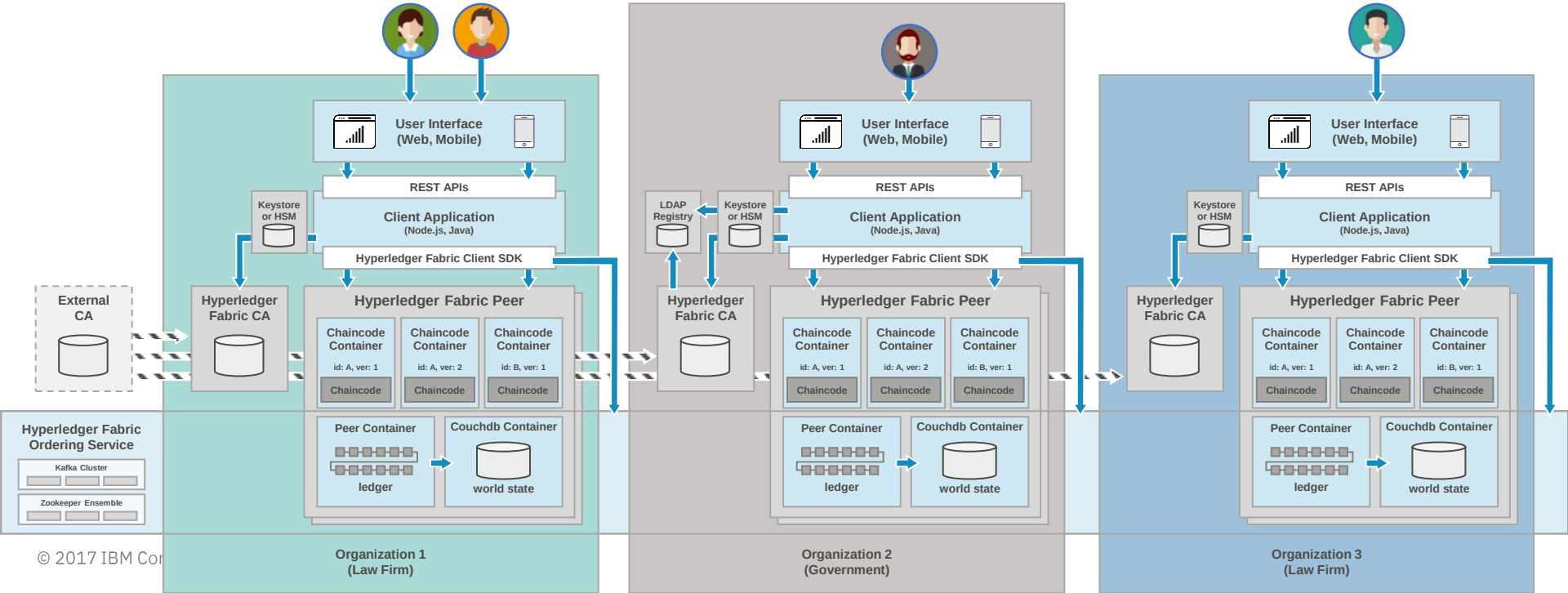
Peers perform application-specific function by executing smart contracts, or more technically, chaincode. Chaincode is managed application code with a well-defined lifecycle that runs within a peer. Chaincode uses Hyperledger Fabric APIs to interact with the world state.



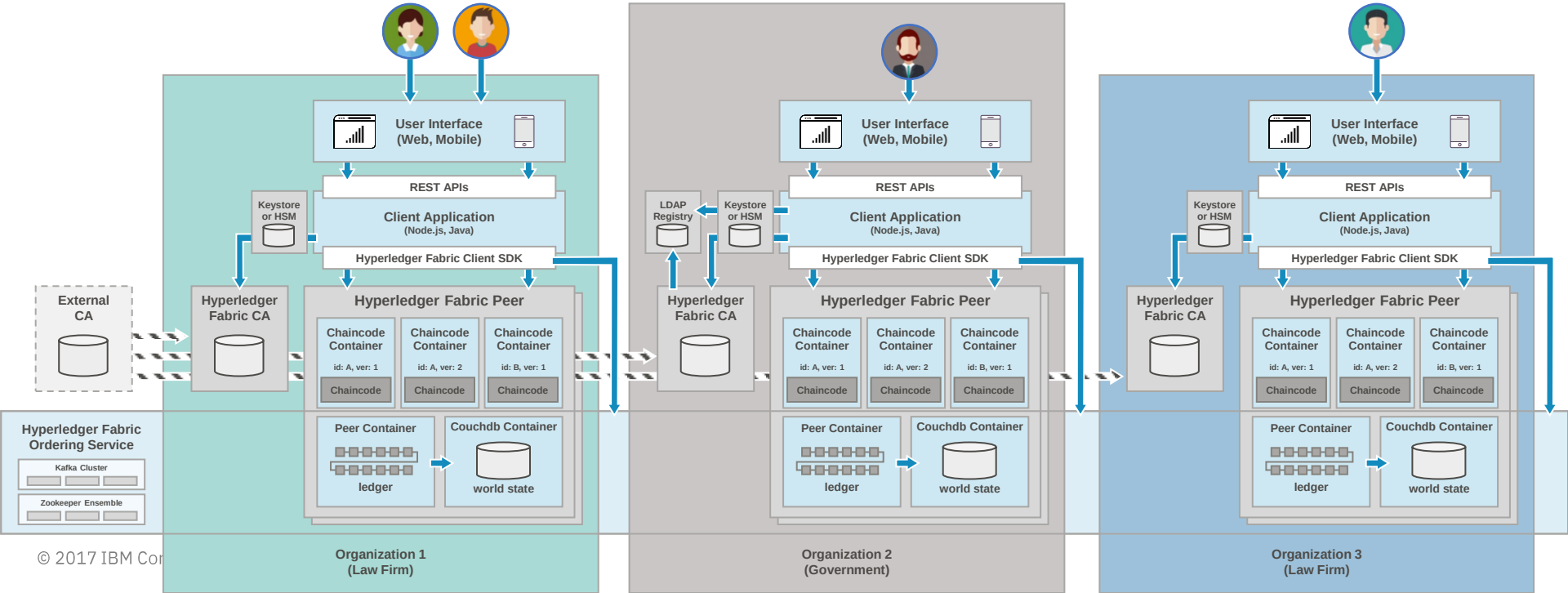
Because Hyperledger Fabric is a private, permissioned blockchain, identity plays a critical role. Identity of individuals as well as Fabric Components such as peers and orderers are defined by certificates, issued by a **certificate authority**. Any certificate authority can be (and often is) used, but Fabric also includes one in the box, called the Hyperledger Fabric CA.



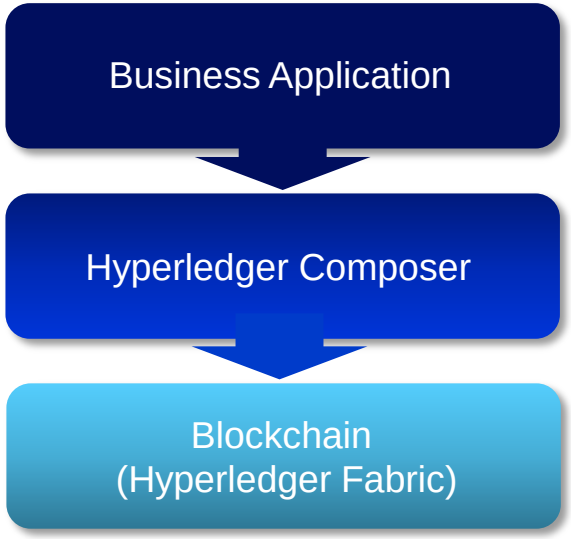
The Ordering Service is the network-level service responsible for determining the order in which transactions coming from any participant in the business network should be committed to the ledger. For high availability and throughput, a Kafka cluster backed by a Zookeeper ensemble is used to distribute blocks to peers (i.e. perform **consensus**).



This makes up our final conceptual architecture diagram for a Hyperledger Fabric application

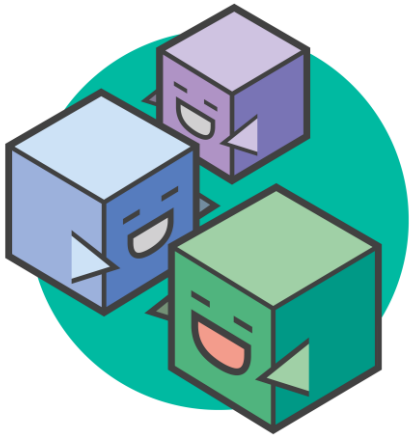


Hyperledger Composer: Accelerating Time to Value



https://hyperledger.github.io/composer/

- A suite of high level application abstractions for business networks
- Emphasis on **business-centric vocabulary** for quick solution creation
- Reduce risk, and increase understanding and flexibility

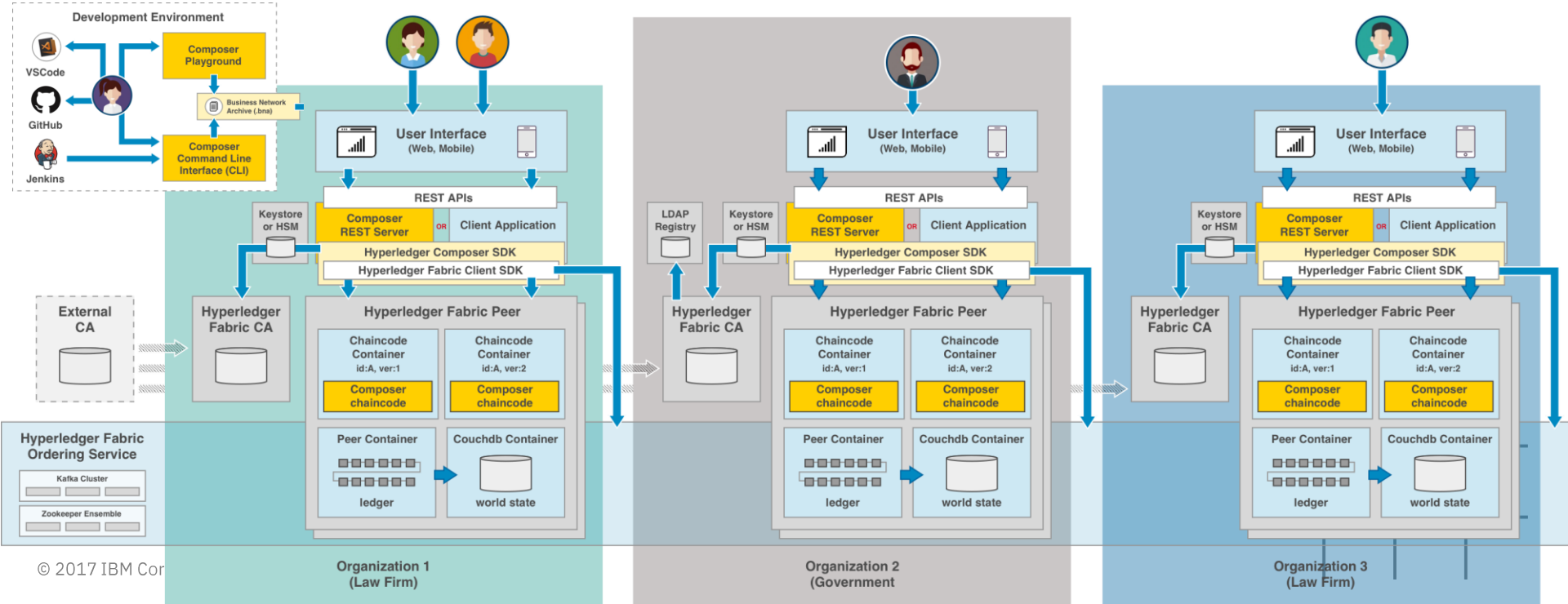


- Features
  - Model your business networks, test and expose via APIs
  - Applications invoke transactions to interact with business network
  - Integrate existing systems of record
- Fully open and part of Linux Foundation Hyperledger
- Try it in your web browser now: http://composer-playground.mybluemix.net/

Hyperledger Fabric + Composer

IBM Blockchain

Hyperledger Composer adds a number of components that leverage the underlying Fabric concepts and infrastructure, simplifying the programming model

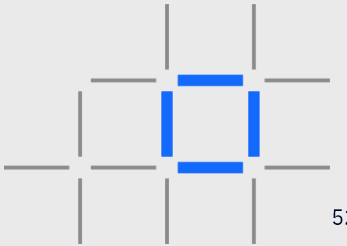


Contents

Understanding
Hyperledger Fabric

Transaction Flow in
Hyperledger Fabric

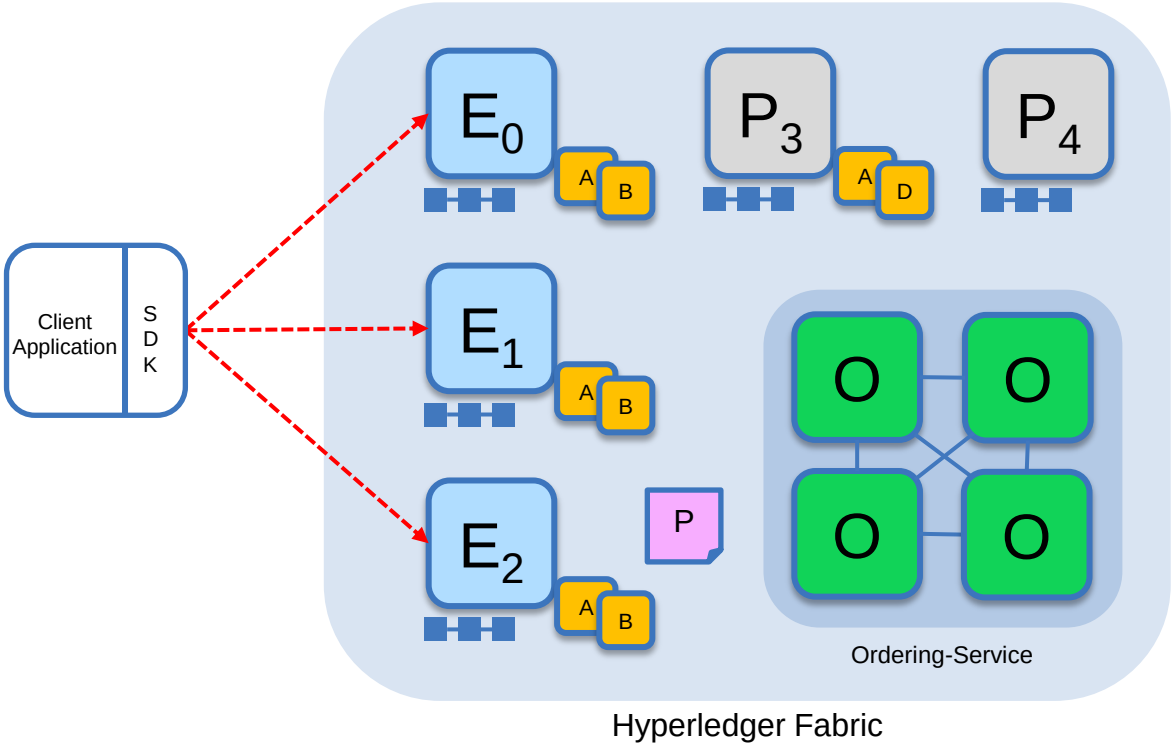
Who is involved in a
Hyperledger Fabric project?



Transaction Flow in Hyperledger Fabric

	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
	Orderer Node (part of the Ordering 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.

Sample transaction: Step 1/7 – Propose transaction



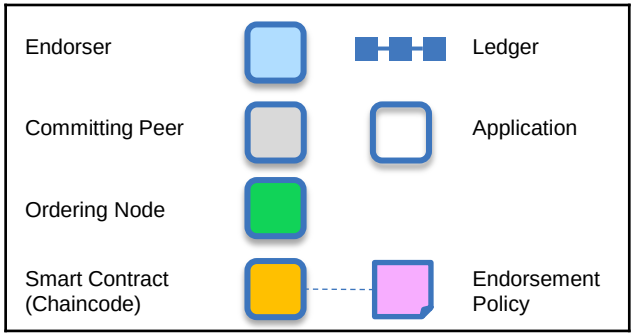
Hyperledger Fabric

Application proposes transaction

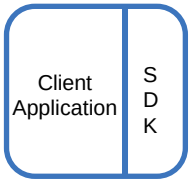
Endorsement policy:
- "E_0, E_1 and E_2 must sign"
- (P_3, P_4 are not part of the policy)

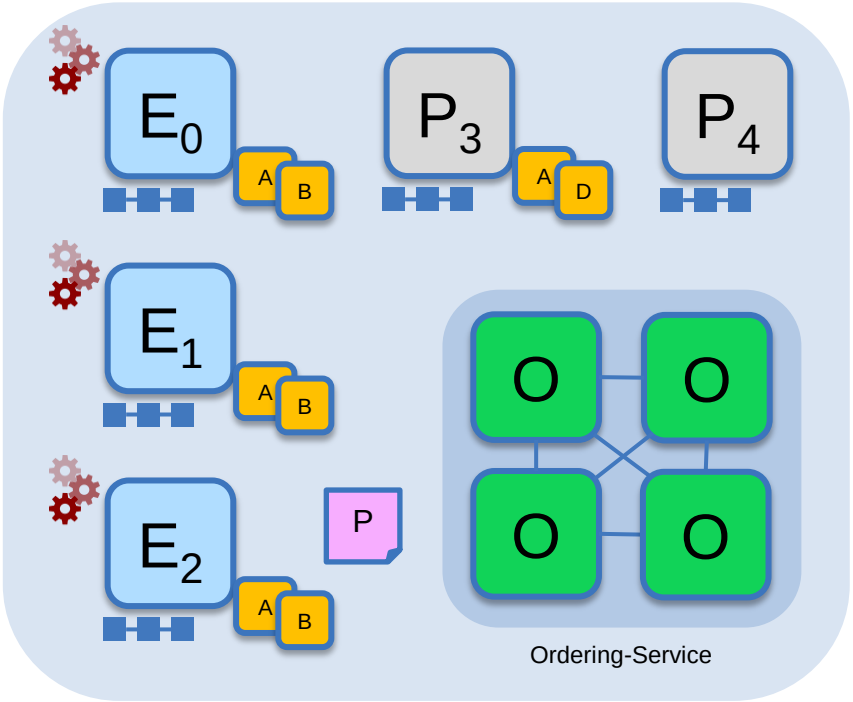
Client application submits a transaction proposal for Smart Contract A. It must target the required peers {E_0, E_1, E_2}

Key:



Sample transaction: Step 2/7 – Execute proposal





Hyperledger Fabric

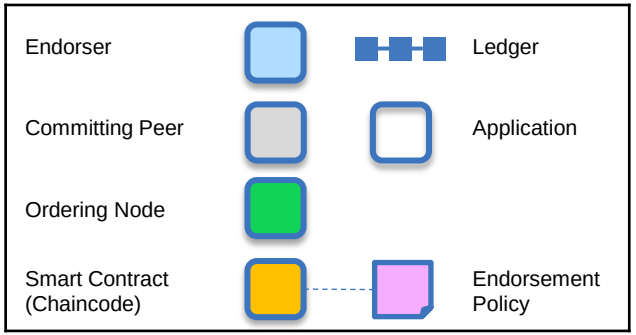
Endorsers Execute Proposals

E_0, E_1 & E_2 will each execute the proposed transaction. None of these executions will update the ledger

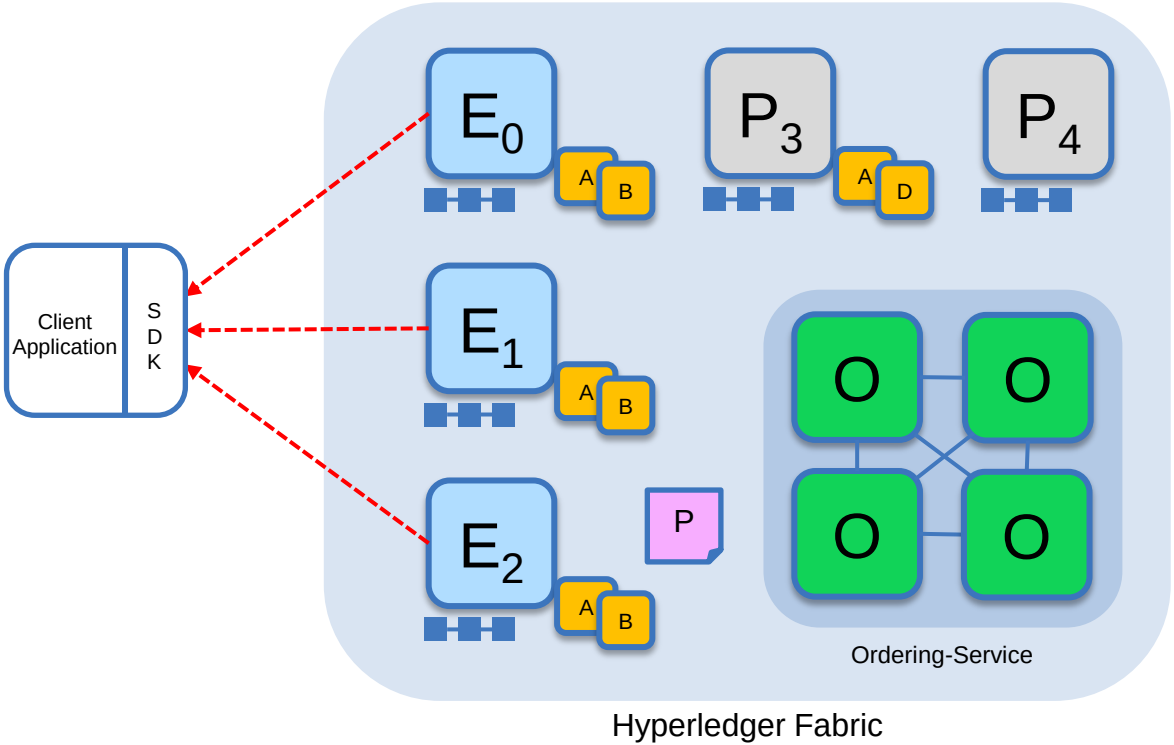
Each execution will capture the set of Read and Written data, called RW sets, which will now flow in the fabric.

Transactions can be signed & encrypted

Key:



Sample transaction: Step 3/7 – Proposal Response



Hyperledger Fabric

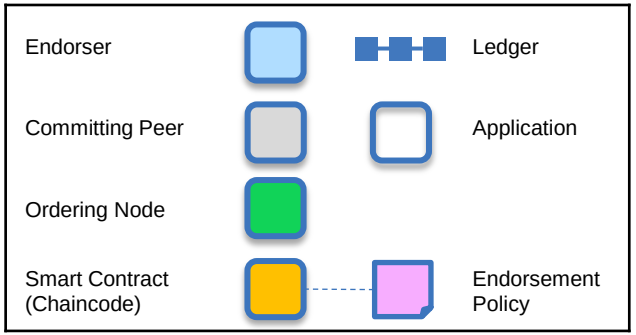
Application receives responses

RW sets are asynchronously returned to application

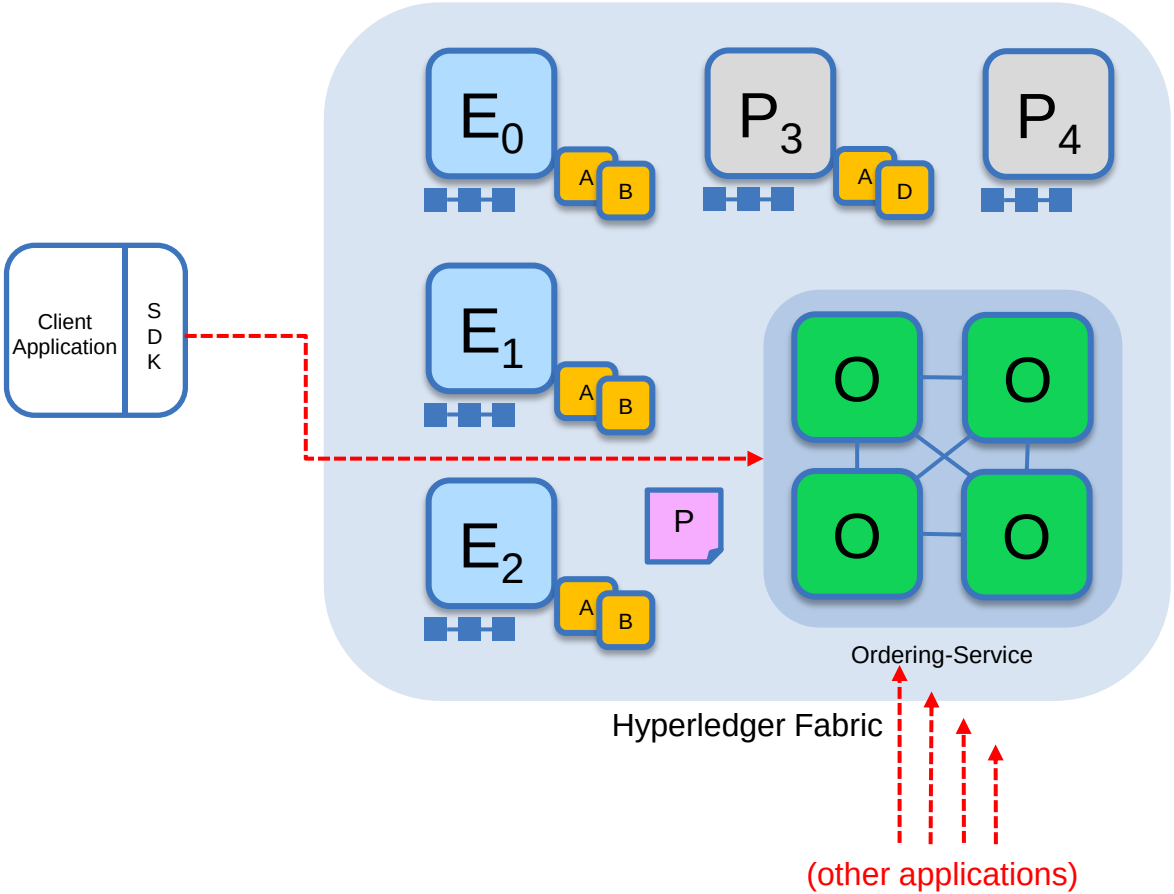
The RW sets are signed by each endorser, and also includes each record version number

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

Key:



Sample transaction: Step 4/7 – Order Transaction

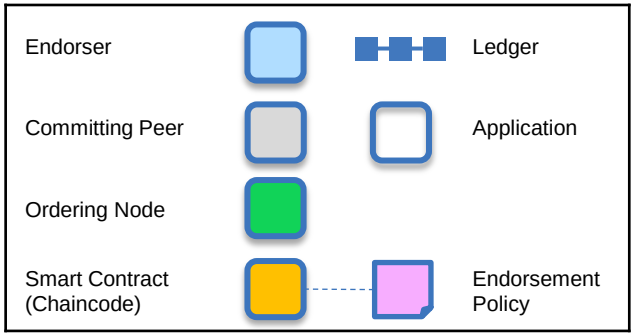


Application submits responses for ordering

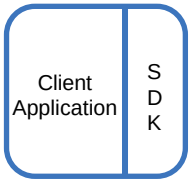
Application submits responses as a transaction to be ordered.

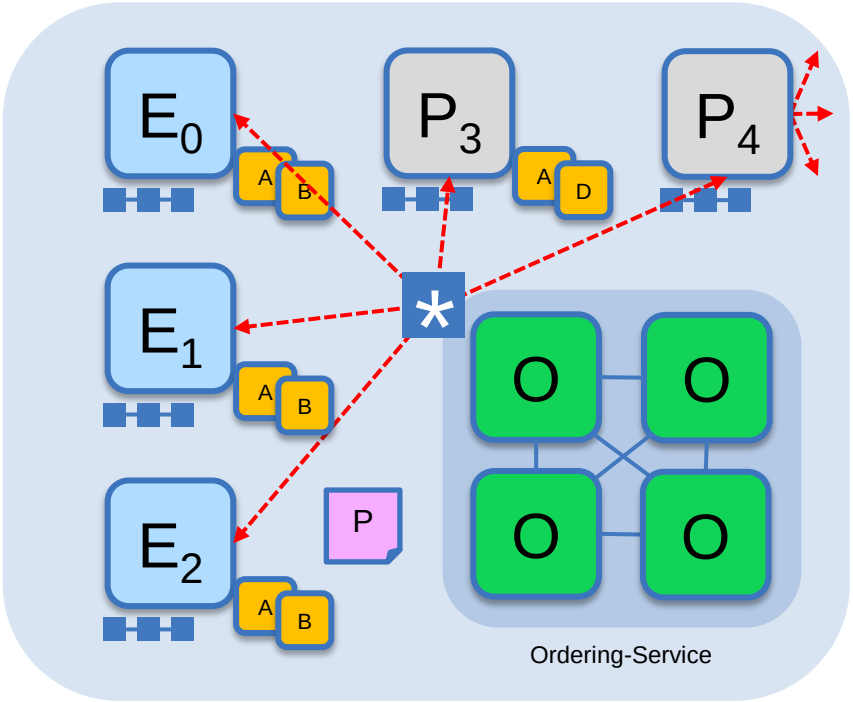
Ordering happens across the fabric in parallel with transactions submitted by other applications

Key:



Sample transaction: Step 5/7 – Deliver Transaction





Hyperledger Fabric

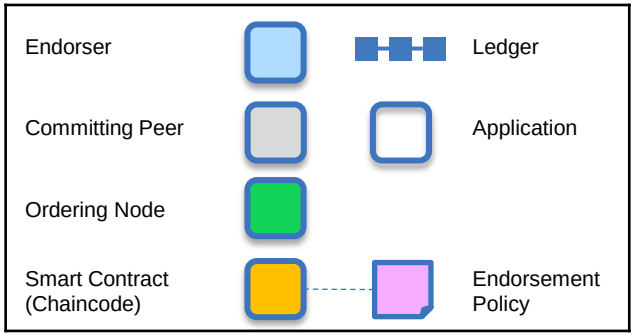
Orderer delivers to all committing peers

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

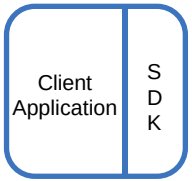
Different ordering algorithms available:

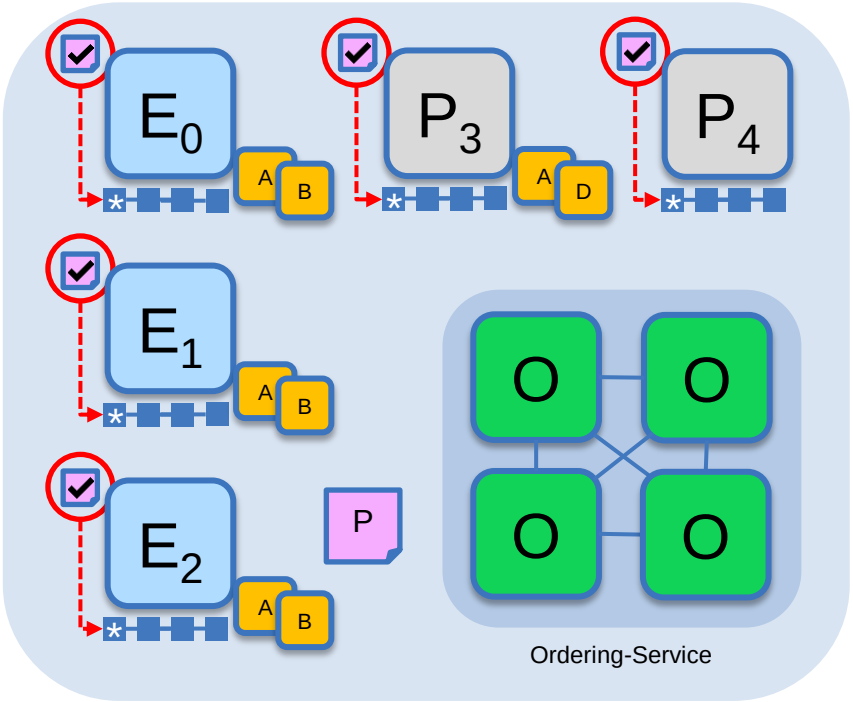
- SOLO (Single node, development)
- Kafka (Crash fault tolerance)

Key:



Sample transaction: Step 6/7 – Validate Transaction





Hyperledger Fabric

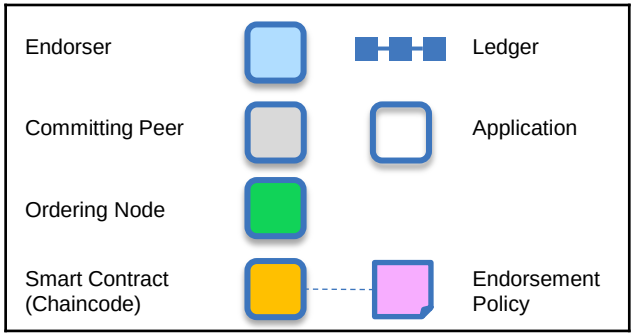
Committing peers validate transactions

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

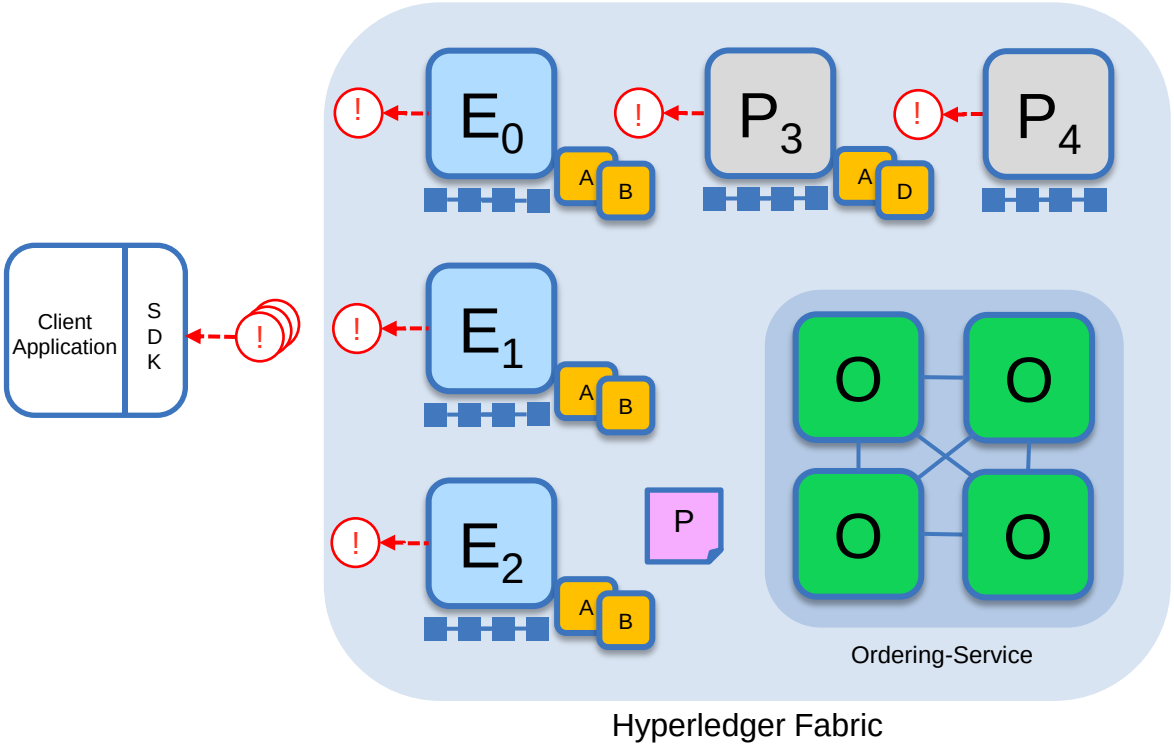
Validated transactions are applied to the world state and retained on the ledger

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

Key:



Sample transaction: Step 7/7 – Notify Transaction

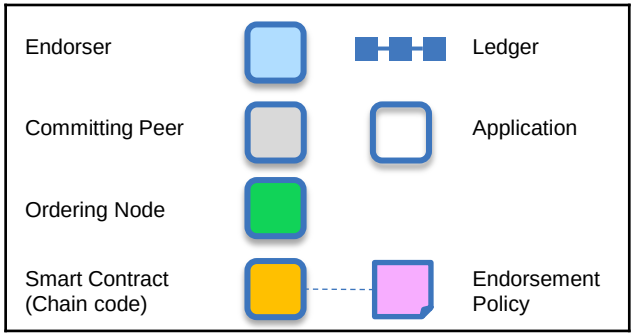


Committing peers notify applications

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

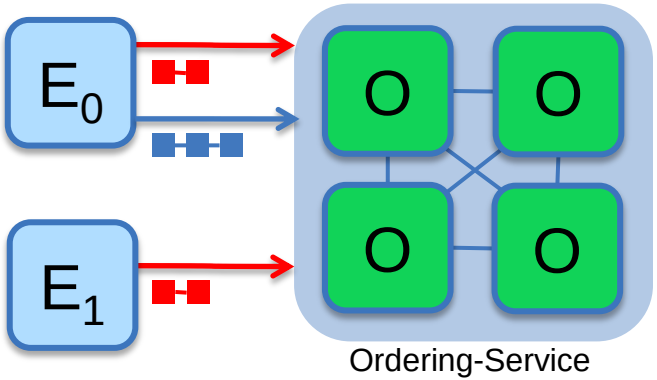
Applications will be notified by each peer to which they are connected

Key:



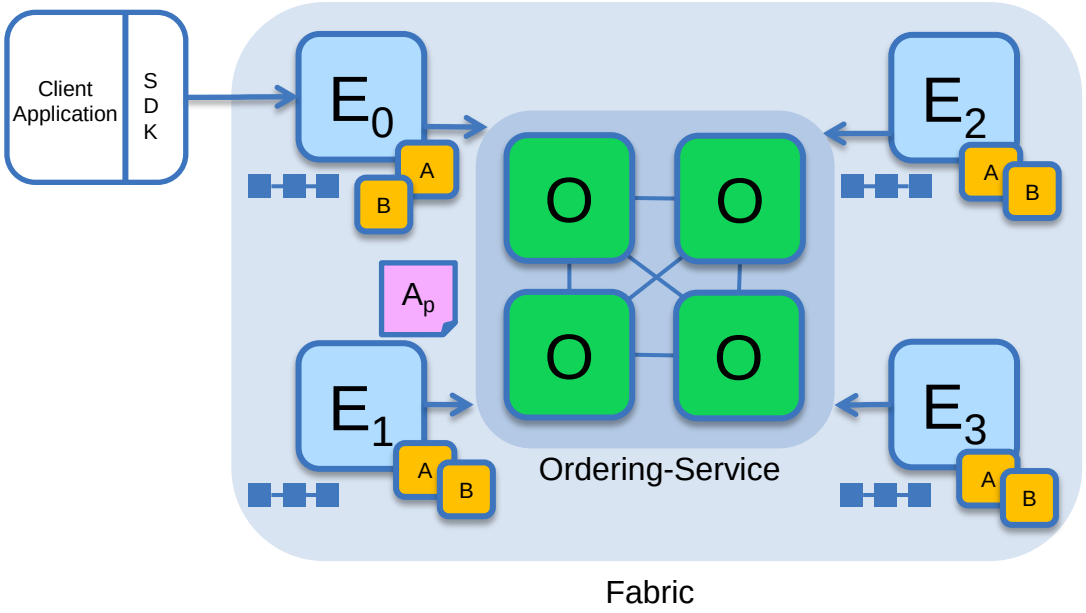
Channels

Channels are used to enforce data and business logic separation within a single Hyperledger Fabric business network



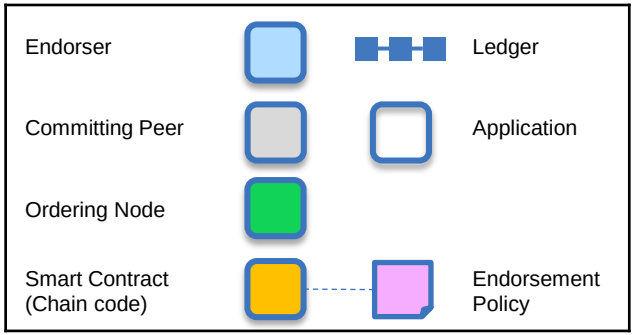
- Chaincode is installed on peers that need to access the worldstate
- Chaincode is instantiated on specific channels for specific peers
- Ledgers exist in the scope of a channel
  - Ledgers can be shared across an entire network of peers
  - Ledgers can be included only on a specific set of participants
- Peers can participate in multiple channels
- Concurrent execution for performance and scalability

Single Channel Endorsement

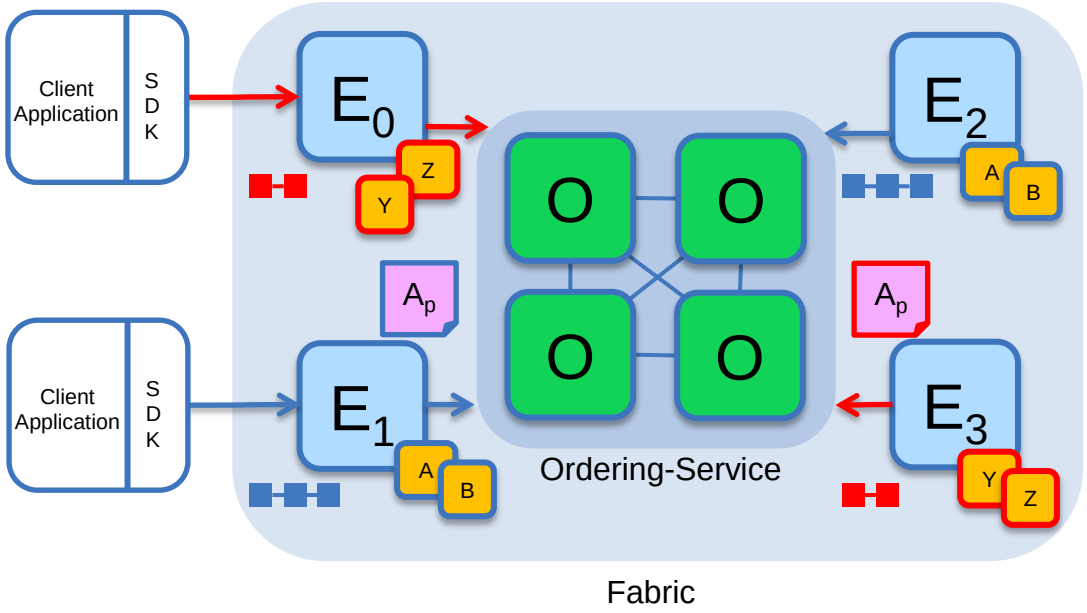


- All peers connect to the same channel (blue).
- All peers consider the same chaincodes for execution and maintain the same ledger
- Endorsement by peers E_0, E_1, E_2 and E_3

Key:

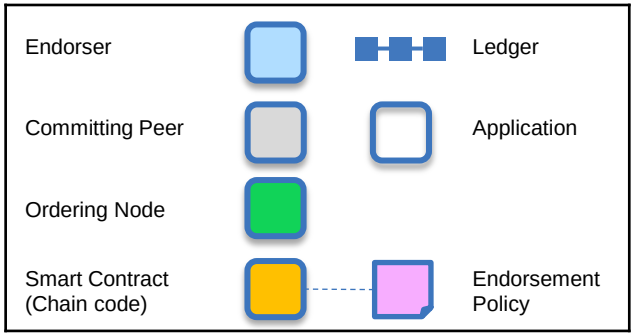


Multi Channel & Chaincode Endorsement



- Peers E_0 and E_3 connect to the red channel for chaincodes **Y** and **Z**
- Peers E_1 and E_2 connect to the blue channel for chaincodes **A** and **B**

Key:

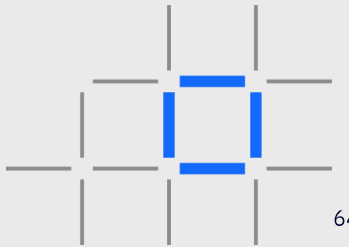


Contents

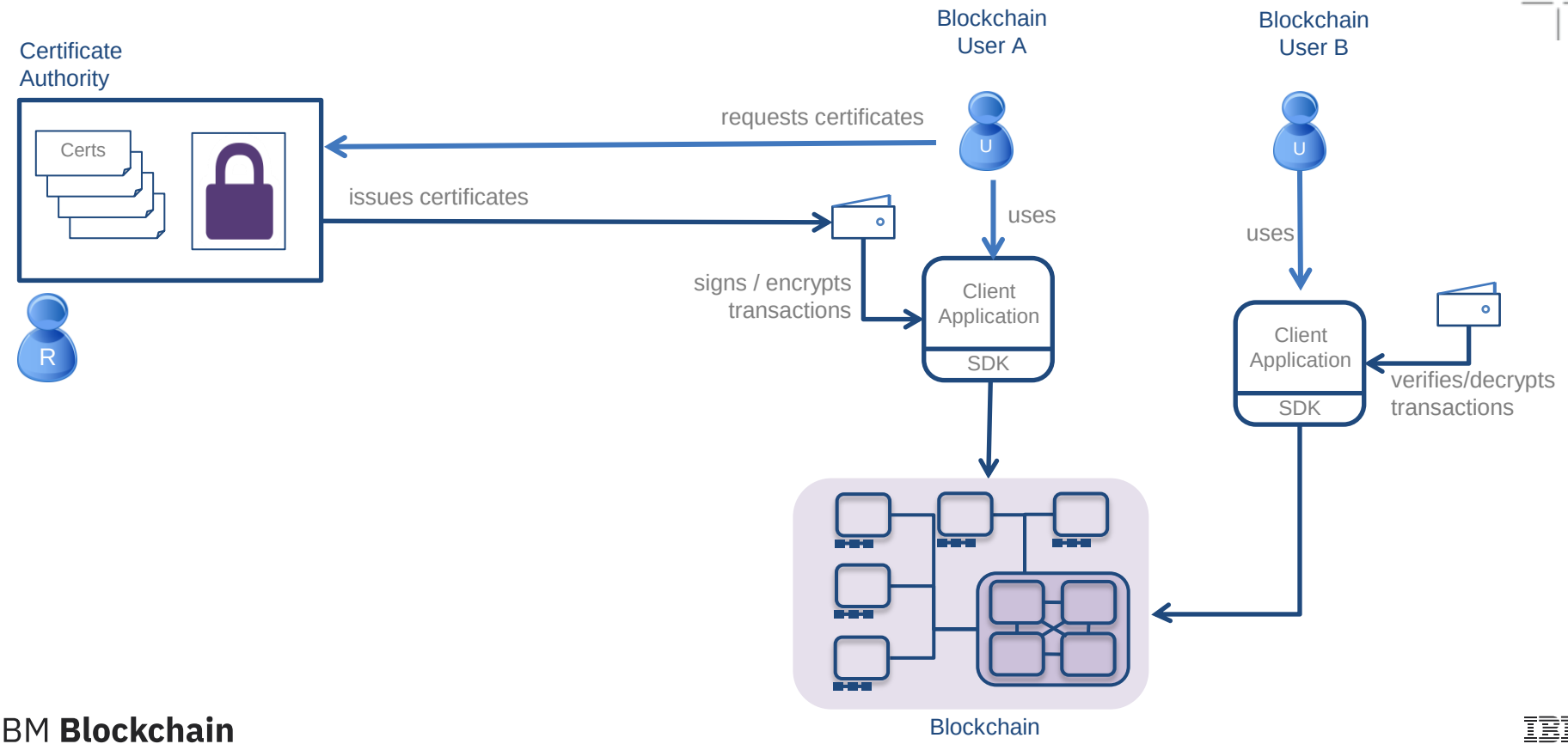
Understanding
Hyperledger Fabric

Transaction Flow in
Hyperledger Fabric

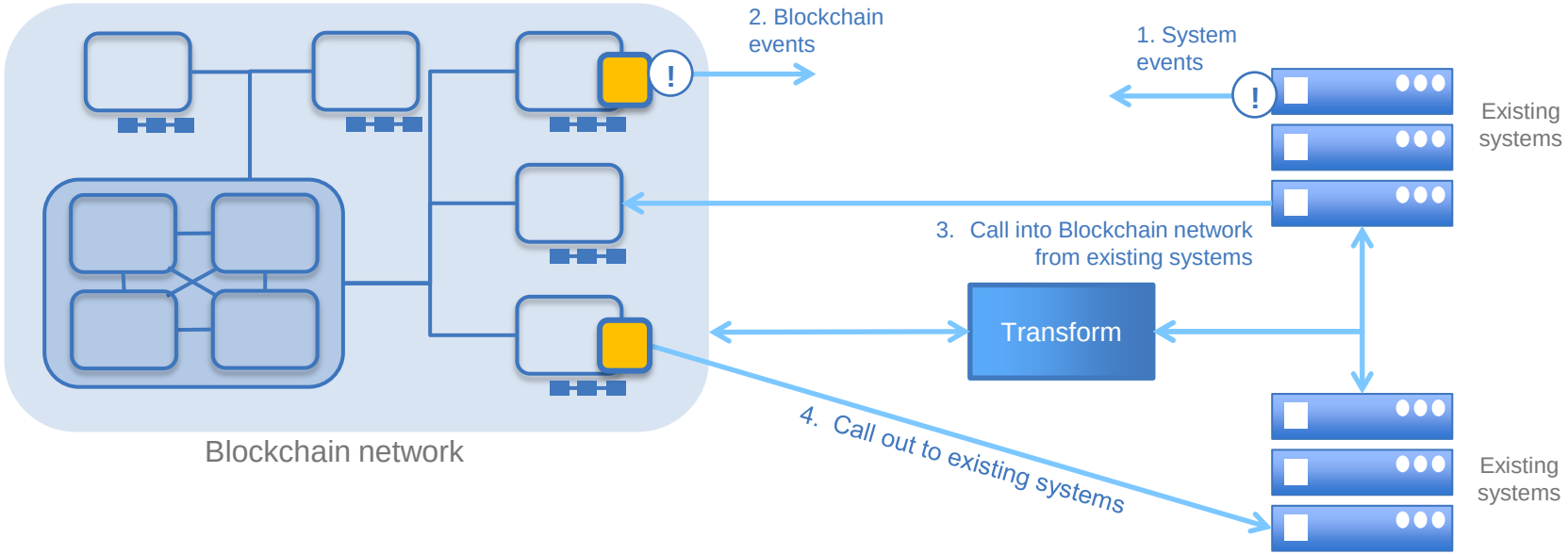
Who is involved in a
Hyperledger Fabric project?



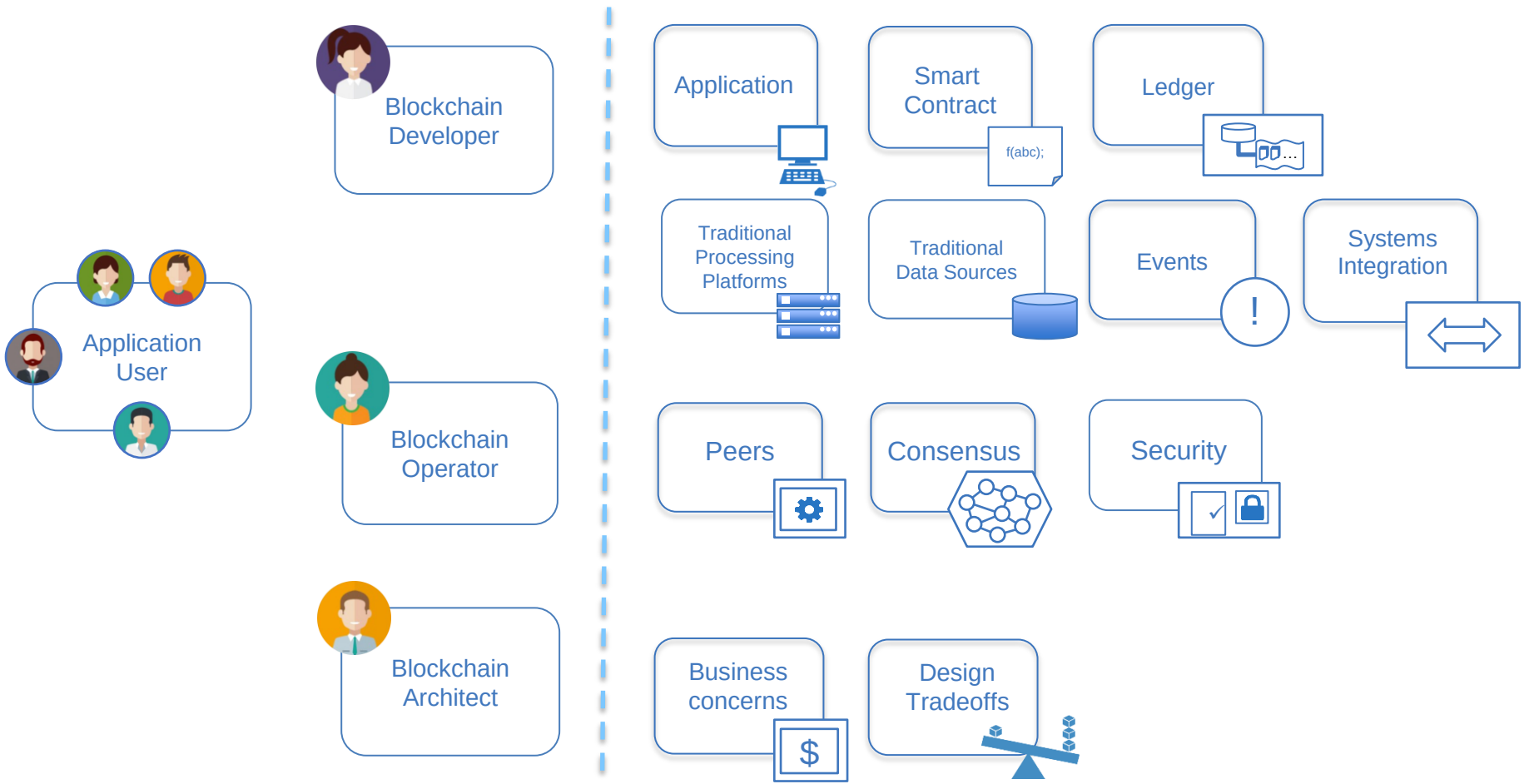
Certificate Authorities and Blockchain



Integrating with existing systems – possibilities



Summary of key concepts



Contents

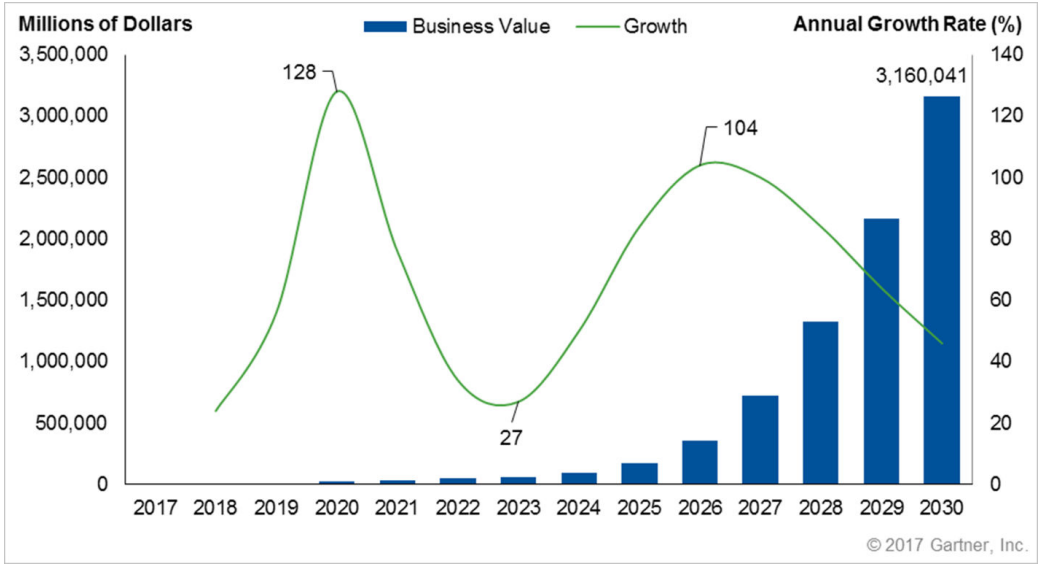
What is Blockchain?

Why is it relevant for our business?

How can IBM help us apply blockchain?

Practical Blockchain: A Gartner Trend Insight Report

Published: 3 March 2017 **ID:** G00325933



- Blockchain is evolving from a digital currency infrastructure into a platform for digital transformation.
- Forecasts operational risks in many Blockchain projects over the **next five to seven years**.

By 2025, five Blockchain / distributed ledger platforms will be "mainstream" commerce platform enablers.

400+

IBM Blockchain

DISRUPTION

Chemicals

Government

Finance

Transportation

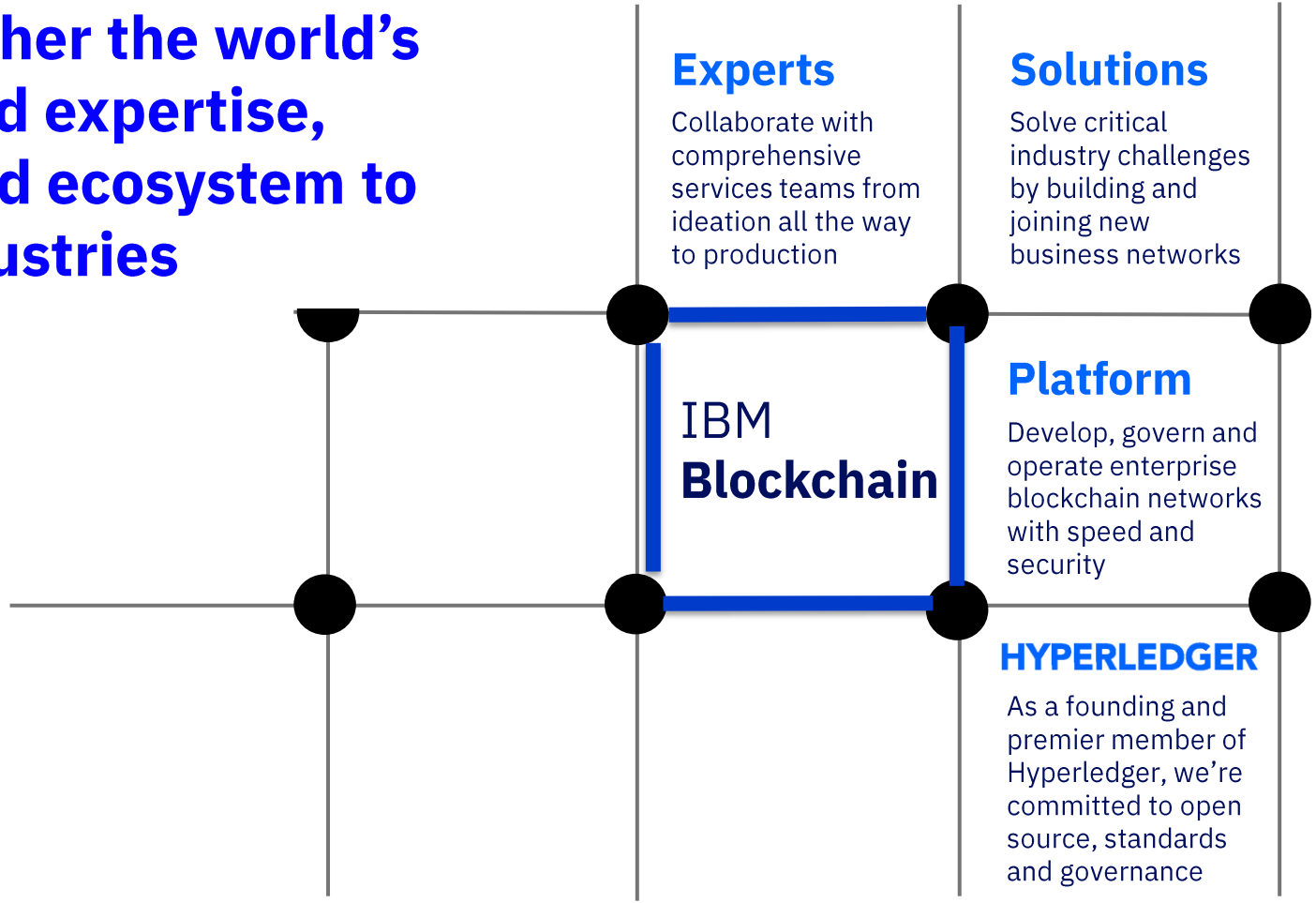
Supply Chain

Energy & Utilities

Media

Healthcare

Bringing together the world's most advanced expertise, technology and ecosystem to transform industries



Introducing the IBM Blockchain Platform

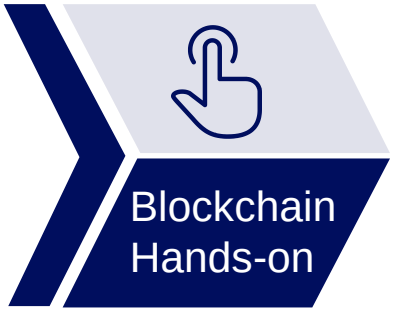
The only fully integrated enterprise-ready blockchain platform designed to accelerate the development, governance, and operation of a multi-institution business network

- Based on Hyperledger Fabric V1 runtime optimized for enterprise requirements
- Specialized compute for security, performance and resilience
- Delivered via the IBM Cloud on a global footprint with 24x7 Integrated Support
- Full lifecycle tooling to speed activation and management of your network

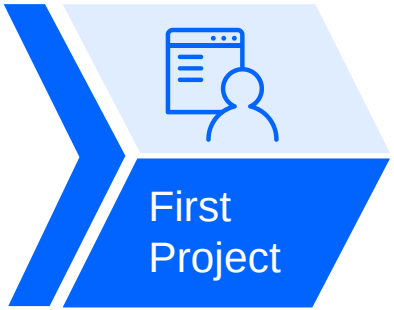
[http://ibm.biz/Platform_Demo]

IBM Engagement Model overview

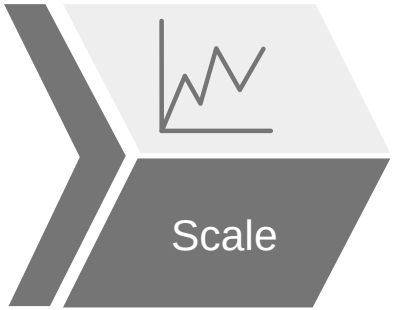
1. Discuss Blockchain technology
2. Explore customer business model
3. Show Blockchain Application demo



1. Understand Blockchain concepts & elements
2. Hands on with Blockchain on Bluemix
3. Standard demo customization



1. Design Thinking workshop to define business challenge
2. Agile iterations incrementally build project functionality
3. Enterprise integration



1. Scale up pilot or Scale out to new projects
2. Business Process Re-engineering
3. Systems Integration

Remote	Digital	Face to face	Face to face

Key Links for IBM Blockchain

- IBM Blockchain Community
  http://ibm.biz/blockchain
- Introduction to Blockchain slides
  https://ibm.box.com/v/BlockchainExplained
- Blockchain training materials
  http://ibm.biz/BlockC101
- Blockchain use cases
  http://ibm.biz/BlockUseCases
- Blockchain demos (incl. Car Leasing)
  http://ibm.biz/BlockDemos
- Blockchain for A,A&D sub-community
  http://ibm.biz/BlockAAD
- Blockchain and Watson IoT
  https://ibm.biz/Bd4jKZ
- Public References
  http://ibm.biz/BlockPubRef
- IBM Newsroom
  http://www-03.ibm.com/press/us/en/presskit/50610.wss
- IBM public webpage on Blockchain
  https://www.ibm.com/blockchain/
- IBM developerWorks
  https://developer.ibm.com/blockchain/

Thank you

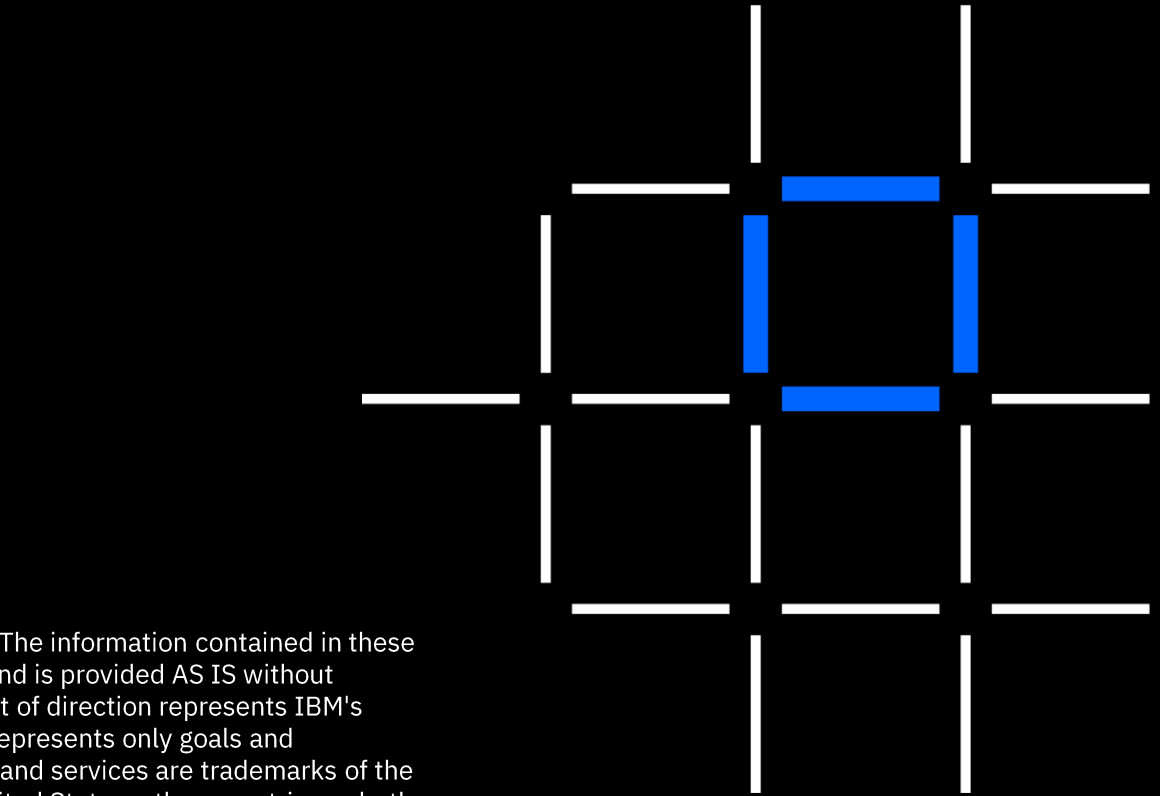
Ronen Siman-Tov

IBM **Blockchain**

www.ibm.com/blockchain

developer.ibm.com/blockchain

www.hyperledger.org



IBM