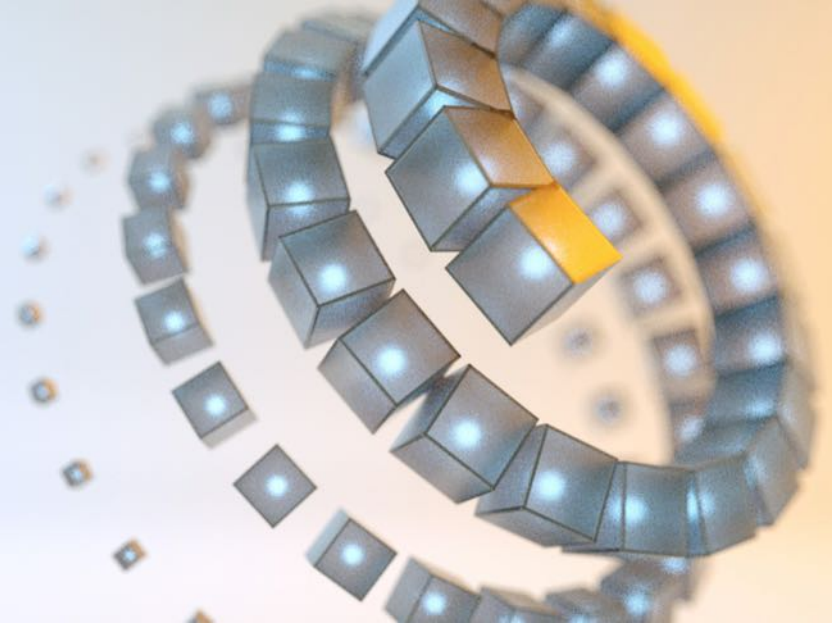# IBM Blockchain is open for business

Learn how blockchain will fundamentally change the way we do business. Then let us help you give it a try.

Get started

GSE
Deutsche Region

Welcome to the cognitive era

outthink your limits

Elke Kunde, Solution Architect
S&D Blockchain Technical Focalpoint IBM DACH
10th European GSE / IBM Technical University for z/VSE, z/VM, KVM and Linux on IBM z Systems,
Oct 26th 2016, Leipzig, Germany

IBM

Contents

What is Blockchain?

Why is it relevant for our business?

How can IBM help us apply Blockchain?
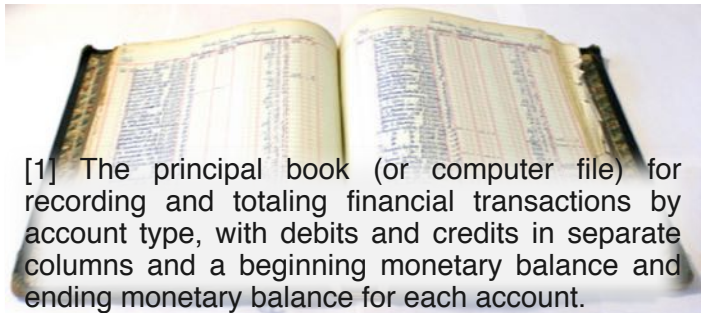
What is the context of Blockchain?

Business Networks, Markets and Wealth

Transferring Assets, building Value

Ledgers [1] are key

[1] The principal book (or computer file) for recording and totaling financial transactions by account type, with debits and credits in separate columns and a beginning monetary balance and ending monetary balance for each account.
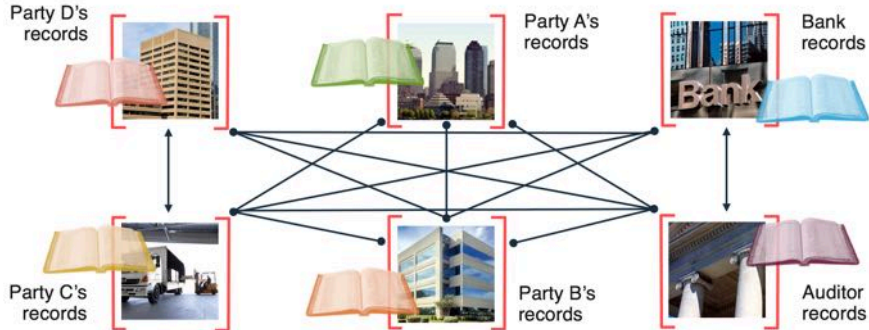
Participants, Transactions and Contracts

outthink your limits

Introducing Blockchain

A shared ledger technology allowing any participant in the business network to see THE system of record (ledger)

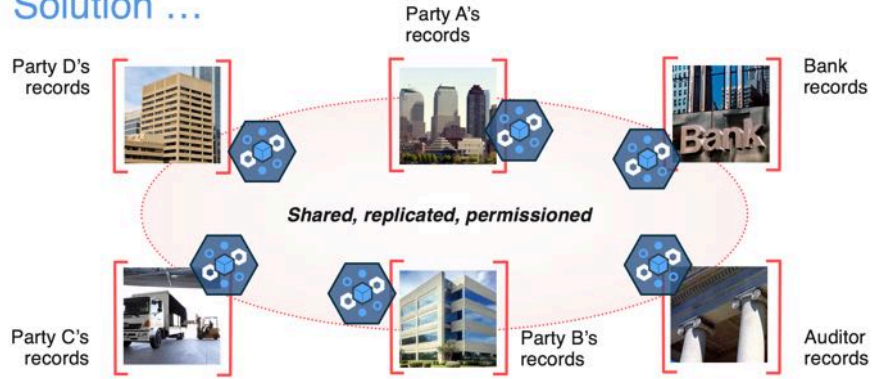# What's the difference with Blockchain?

Blockchain technology has the potential to radically transform multi-party business networks, enabling significant cost and risk reduction and innovative new business models

outthink your limits

Blockchain underpins Bitcoin …

bitcoin

Unregulated, censorship-resistant shadow currency

First Blockchain application
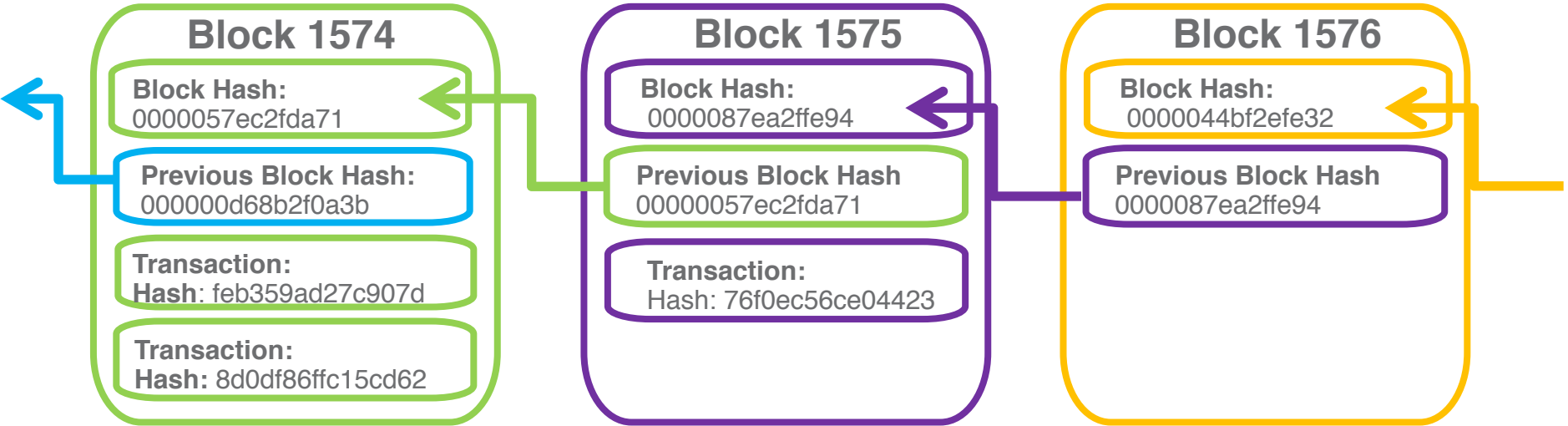
- Pioneer of Blockchain technology

BUT

BLOCKCHAIN is <u>not</u> *bitcoin*

… Digital currencies different from cryptocurrency

outthink your limits

What is a Blockchain ?

What

Block 1574

Block Hash:
0000057ec2fda71

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

Made up of a series of blocks added in chronological order

outthink your limits

Blockchain for business …

Append-only distributed system of record shared across business network

Shared ledger

"Smart contract", Chaincode

Business terms embedded in transaction database & executed with transactions

Ensuring appropriate visibility; transactions are secure, authenticated & verifiable

Privacy

Consensus

All parties agree to network verified transaction

… Broader participation, lower cost, increased efficiency

outthink your limits

Shared ledger

Records all transactions across business network

Shared between participants

Participants have own copy through replication

Permissioned, so participants see only appropriate transactions

THE shared system of record

outthink your limits

"Smart contract", Chaincode

Business rules implied by the contract … embedded in the Blockchain and executed with the transaction

Verifiable, signed

Encoded in programming language

Example:

Defines contractual conditions under which corporate Bond transfer occurs

outthink your limits

Privacy

Ledger is shared, but participants require privacy

Participants need:

- Transactions to be private
- Identity not linked to a transaction

Transactions need to be authenticated

Cryptography central to these processes

Government oversight, compliance & audit can be part of the same network.

outthink your limits

Consensus

… the process by which transactions are verified

Anonymous participants

- Bitcoin *cryptographic mining* provides randomized selection among anonymous participants
- Significant compute cost (proof of work)

Known & trusted participants

- Commitment possible at low cost
- Byzantine fault tolerance (BFT)

Multiple alternatives

- Proof of stake, where influence is determined by risk of validators
- Multi-signatures, validation needs consent from 3 out of 5 validators

Industrial Blockchain needs "pluggable" consensus

outthink your limits

Contents

What is Blockchain?

Why is it relevant for our business?

How can IBM help us apply Blockchain?

Blockchain benefits

Saves
time

Transaction time from days to near instantaneous

Removes
cost

Overheads and cost intermediaries

Reduces
risk

Tampering, fraud & cyber crime

Increases
trust

Through shared processes and recordkeeping

outthink your limits

[hype.]

outthink your limits

Blockchain – not for all …

POSITIVE Indicators

1. Reduce cost and complexity

2. Trusted recordkeeping

3. Reduced errors and Resiliency

4. Improve discoverability and auditability

5. Shared trusted and secure process

NEGATIVE Indicators

1. Not suited to high performance (millisecond) transactions

2. Not for just one participant (no business network)

3. Looking for a database replacement, looking for a messaging solution, looking for transaction processing replacement

4. Not suited for low value, high volume transactions

outthink your limits

Consensus use case – Shared routing codes

What
- Competitors/collaborators in a business network need to share reference data, e.g. bank routing codes
- Each member maintains their own codes, and forwards changes to a central authority for collection and distribution
- An information subset can be owned by organizations

How
- Each participant maintains their own codes within a Blockchain network
- Blockchain creates single view of entire dataset

Benefits

1. Consolidated, consistent dataset reduces errors
2. Near-real-time of reference data
3. Naturally supports code editing and routing code transfers between participants

outthink your limits

Provenance use case – Vehicle 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, no authority "owns" provenance

2. Improvement in system utilization

3. Recalls "specific" rather than cross fleet

outthink your limits

Immutability use case – Financial ledger

What
- Financial data in a large organization dispersed throughout many divisions and geographies
- Audit and Compliance needs indelible record of all key transactions over reporting period

How
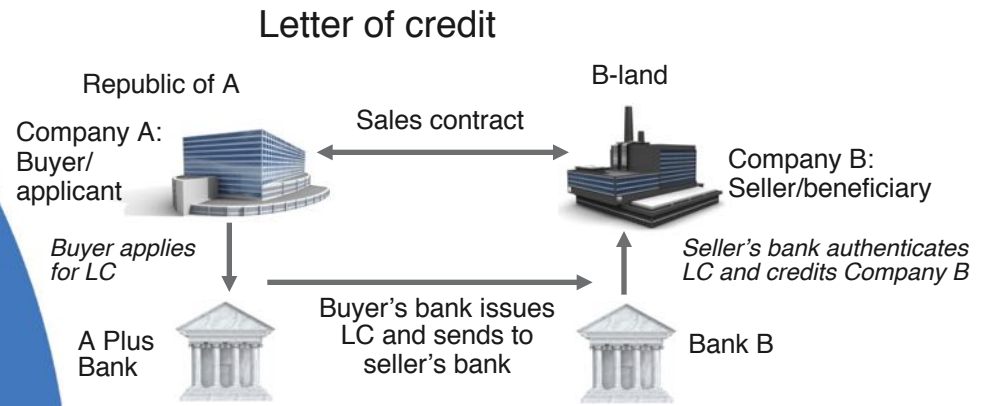- Blockchain collects transaction records from diverse set of financial systems
- Append-only and tamperproof qualities create high confidence financial audit trail
- Privacy features to ensure authorized user access

Benefits

1. Lowers cost of audit and regulatory compliance

2. Provides "seek and find" access to auditors and regulators

3. Changes nature of compliance from passive to active

outthink your limits

Finality use case – Letter of credit

Letter of credit

Republic of A

Company A: Buyer/applicant

Sales contract

B-land

Company B: Seller/beneficiary

Buyer applies for LC

Seller's bank authenticates LC and credits Company B

A Plus Bank

Buyer's bank issues LC and sends to seller's bank

Bank B

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

outthink your limits

Other potential use cases

- Securities
  - Post-trade settlement
  - Derivative contracts

- Trade Finance
  - Bill of Lading
  - Cross-currency payment

- Syndicated Loans

- Supply Chain

- Retail Banking
  - Cross border remittances
  - Mortgage verification

- Public Records
  - Real estate records
  - Vehicle registrations
  - Citizen Identity

- Digital Property Management

outthink your limits

Patterns for customer adoption

HIGH VALUE MARKET

- Transfer of high value financial assets
- Between many participants in a market
- Regulatory timeframes

ASSET EXCHANGE

- Sharing of assets (voting, dividend notification)
- Assets are information, not financial
- Provenance & finality are key

CONSORTIUM SHARED LEDGER

- Created by a small set of participants
- Share key reference data
- Consolidated, consistent real-time view

COMPLIANCE LEDGER

- Real-time view of compliance, audit & risk data
- Provenance, immutability & finality are key
- Transparent access to auditor & regulator

Key players for Blockchain adoption

Regulator

- An organization who enforces the rules of play
- Regulators are keen to support Blockchain based innovations
- Concern is systemic risk – new technology, distributed data, security

Industry Group

- Often funded by members of a business network
- Provide technical advice on industry trends
- Encourages best practice by making recommendations to members

Market Maker

- In financial markets, takes buy-side and sell-side to provide liquidity
- More generally, the organization who innovates
  - Creates a new good or service, and business process (likely)
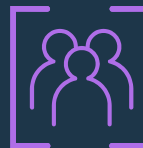 - Creates a new business process for an existing good or service

outthink your limits

Contents

What is Blockchain?

Why is it relevant for our business?

How can IBM help us apply Blockchain?

Blockchain for Business – Our Point of View

Community + Code

Linux Hyperledger Project

Open Source Code: Blockchain for business;

**Consensus | Provenance
Immutability | Finality**

Open Governance – 40 member cross industry board

Cloud

IBM Blockchain

Blockchain managed service on IBM Cloud and z Systems

**Identity | Consensus | System Integration |
Hardware-assist for Performance & Security**

IBM Blockchain on Bluemix

Clients

Blockchain Solutions
Blockchain Garage
Blockchain Competence Center

Making Blockchain real for business

Blockchain Garage;
**New York | London | Singapore | Tokyo
Boeblingen, Paris/Lille, Groningen**

Blockchain Services Practice

outthink your limits

IBM Garage - Offerings

Proof of Technology	IBM Design Thinking Workshop	Sprint zero	First Project sprints	Blockchain hackathon	Port your experiment
1 day	2 days	3 days	10 days / sprint	3 days	1 week or T&M
Structured classroom based hands on exploration of the code behind the car leasing demo. Technical and business audience	Structured exploration of client use case. Business and technical audience. On-ramp to a sprint.	Set up the sizing and environment for the first project sprints. Gain commitment from client technical and business sponsors.	Engage our team with 2 to 4 developers from the customer in pair programming scenarios to create a minimum viable product	Offer Bluemix platform and garage expertise to run an innovation hackathon around blockchain	Re-platform your previous experiment onto Hyperledger – our fabric – and node infrastructure of your choice

outthink your limits

Linux Foundation's Hyperledger Project

– Linux Foundation project announced December 17, 2015 with **17** founders, now **over 85** members

– The Hyperledger Project is a collaborative effort to advance Blockchain technology by identifying and addressing important features for a cross-industry open standard for distributed ledgers that can transform the way business transactions are conducted globally

– Open source and open standards-based

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

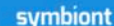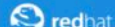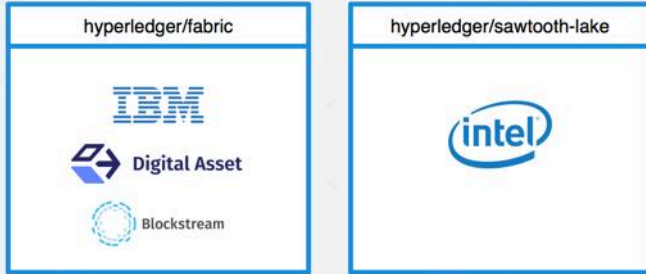| QUICK FACTS	
Chairman	Blythe Masters/DAH
Executive Director	Brian Behlendorf
Technical Chair	Chris Ferris/IBM
Contribution	44,000 lines of code in February 2016
Sprint to one codebase with unified thinking	Staged releases

www.Hyperledger.org

outthink your limits

PREMIER

accenture — High performance. Delivered. | AIRBUS | CME Group | DEUTSCHE BÖRSE GROUP | Digital Asset | DTCC

FUJITSU | HITACHI Inspire the Next | IBM | intel | J.P.Morgan | R

GENERAL

ABN·AMRO | ANZ | JM | belink | bitse | BLOCKCHAIN

Blockstream | bloq | BNP PARIBAS | BNY MELLON | Broadridge | bubi.cn

Calastone | CISCO | cloudsoft | CLS Fundamental to FX | coinplug | colu.

consensys | CREDITS | Cuscal The complete payments partner | ENERGY BLOCKCHAIN LABS | | eVUE digital labs

Gem | PeerSafe | guardtime | intellect | intuit | INVeSHARE

IROOTECH | itBit | KSD Korea Securities Depository | Libra | Milligan Partners | MIRACL

MonetaGo | ML | MOSCOW EXCHANGE | Orchestrating a brighter world NEC | NETKI | norbloc

NTT DaTa | onchain | 橙色魔方 | redhat | Ribbit.me | SAMSUNG SDS

SANY | Skry | SORAMITSU | STATE STREET | | symbiont

| tequa creek | THOMSON REUTERS | TMX | UMP | vmware

WELLS FARGO | 梧桐树 wutongtree.com | 云象 YUNPHANT |

As of 2nd September 2016

Hyperledger Project proposed contributions as of July 2016
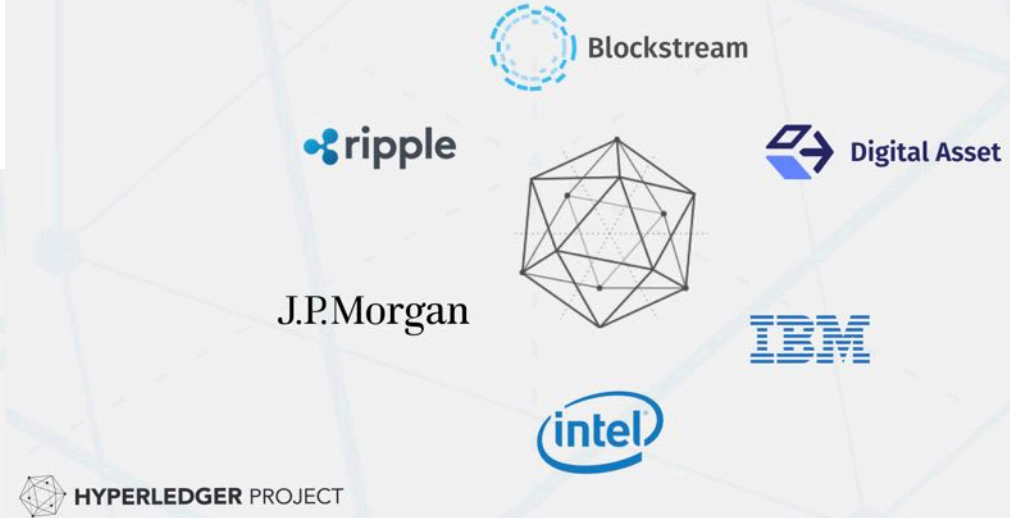
IBM Blockchain Platform | Hyperledger project context How
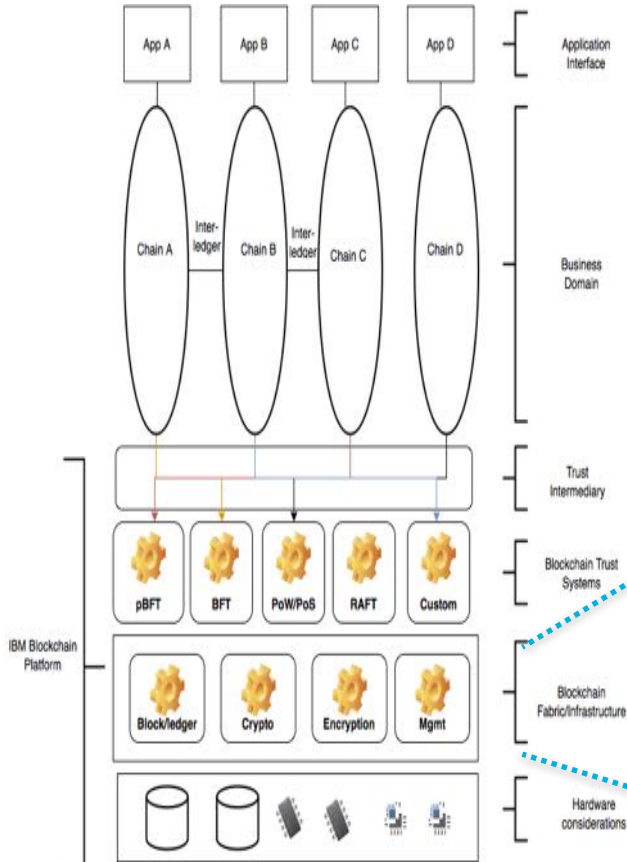
Custom built applications for specific use cases

Application development facilities specialized extensions, specialized validation algorithms integration gateway, operations dashboard

Out of scope

Smart contract execution environment, ledger data structures, Membership services, modular validation framework, modular identity services, network peer services
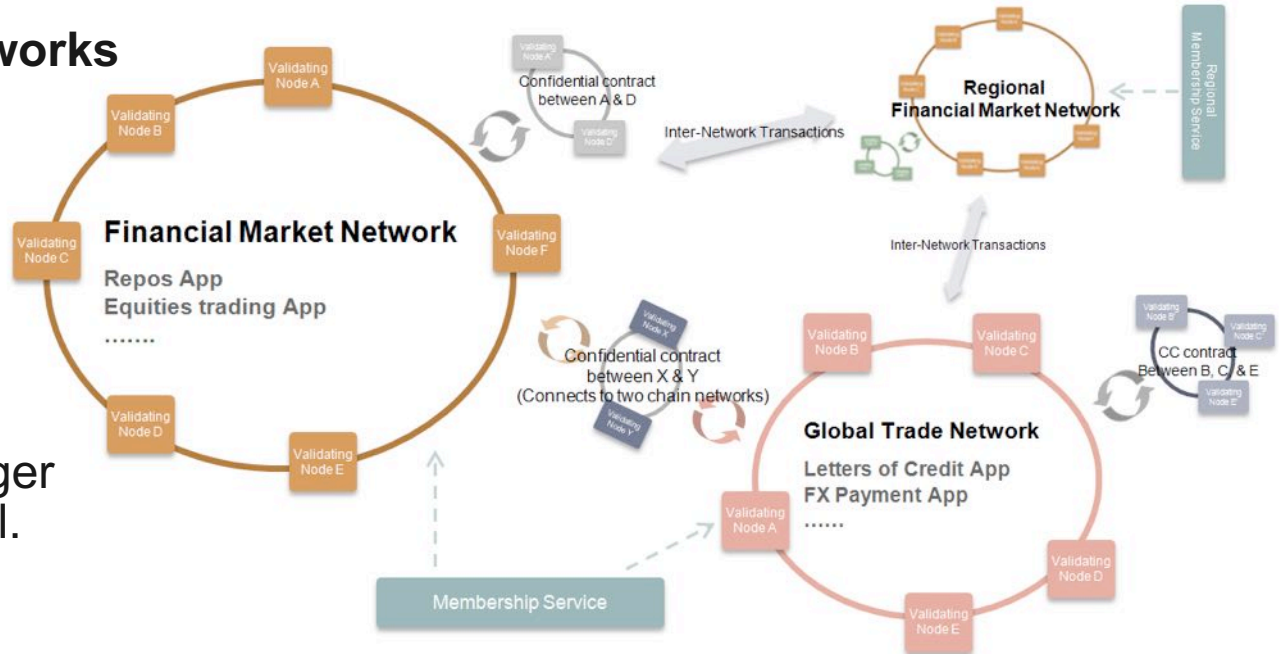
In-scope

outthink your limits

Hyperledger whitepaper summary

Hyperledger whitepaper Draft 2.0 as of August 3rd 2016

A world of many networks

Hyperledger is based on the expectation that there will be many blockchain networks, with each network ledger serving a different goal.

outthink your limits

Hyperledger – Architecture

Identity services manages identities of entities, participants and ledger objects such as assets and smart-contracts.

Policy services manages access control, privacy, consortium rules, consensus rules, etc.

Blockchain services manage the distributed ledger through a peer-to-peer communication protocol.

Different consensus algorithms guaranteeing strong consistency may be plugged in and configured per deployment.

Smart-contract services are a secured and lightweight way to sandbox the smart-contract execution on validating nodes. The environment is a "locked down" and secured container with a set of signed base images.
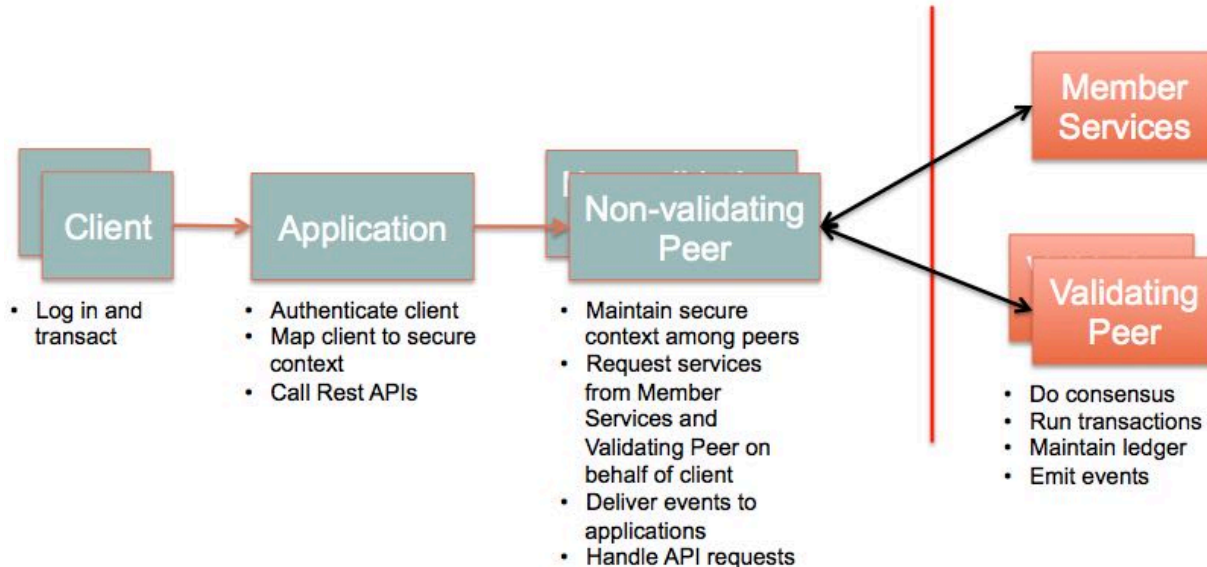
outthink your limits
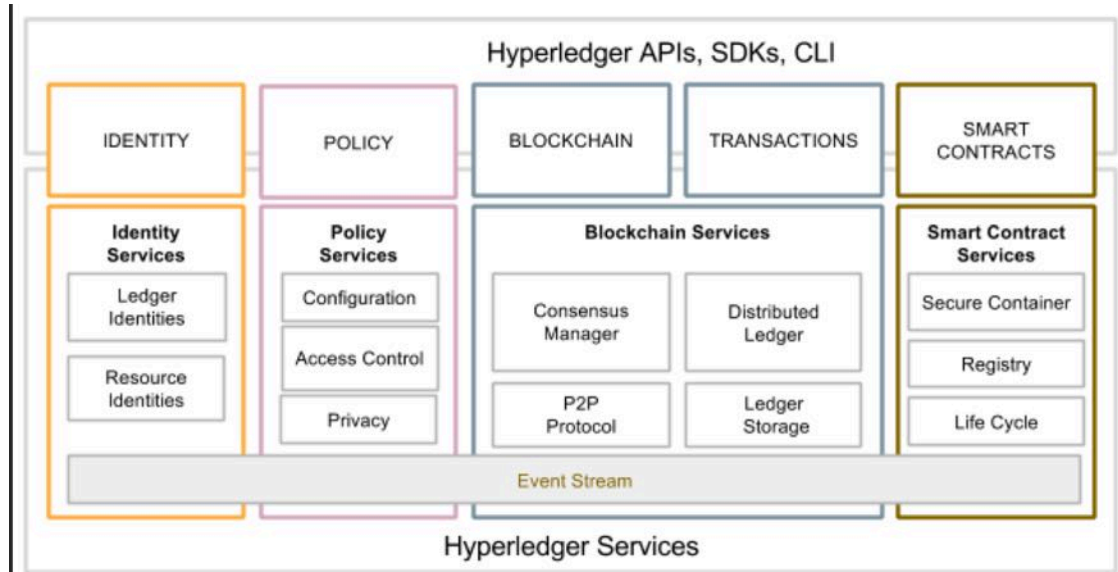
Hyperledger Fabric –
Identity services – Topology 1/2

VALIDATORS

A deployment of Open Blockchain may consist of a membership service, many validating peers, non-validating peers, and 1 or more applications. All of these components make up a chain.

Client
- Log in and transact

Application
- Authenticate client
- Map client to secure context
- Call Rest APIs

Non-validating Peer
- Maintain secure context among peers
- Request services from Member Services and Validating Peer on behalf of client
- Deliver events to applications
- Handle API requests

Member Services

Validating Peer
- Do consensus
- Run transactions
- Maintain ledger
- Emit events

IDENTITY

Identity Services
- Ledger Identities
- Resource Identities

outthink your limits

Byzantine Generals Problem – Agreement in presence of faults

The abstract problem:
Byzantine generals lay siege to a city.
Each division is directed by its own General/Lieutenant.
Each division is camped outside the city, observing the enemy.
They communicate with each other by messengers.
Some of the Generals/Lieutenants are/could be traitors and send malicious messages.
A consensus is needed whether to attack or retreat.

- Decide on same plan of action: Do they all attack or retreat?
- They have to do the same option or will be beaten by the City's forces.
- Do they trust the messengers?
- What to do if they get conflicting orders by the messengers?
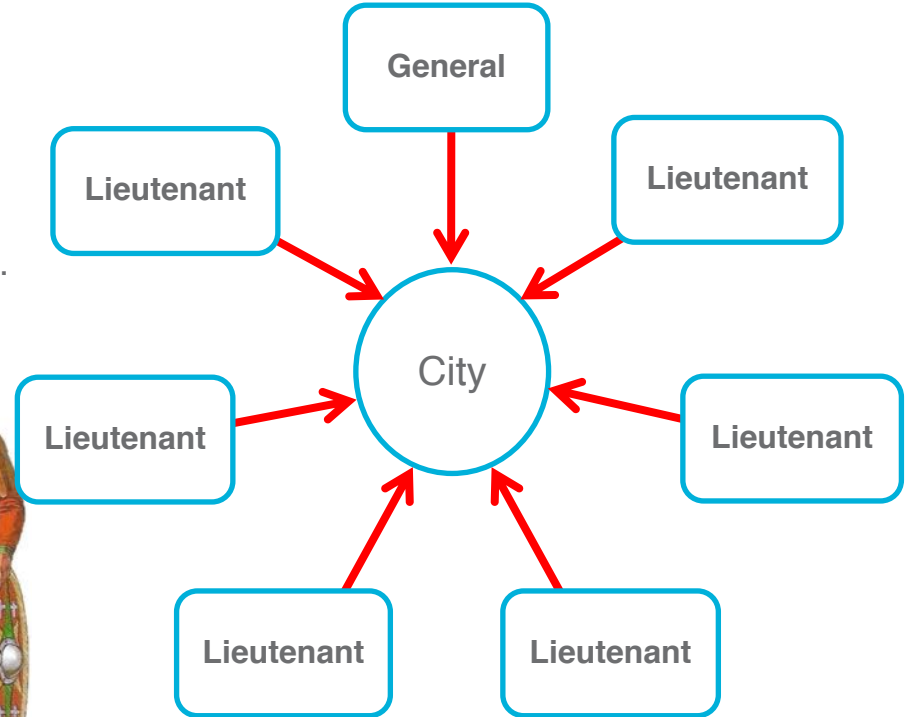
Practical Byzantine Fault Tolerance
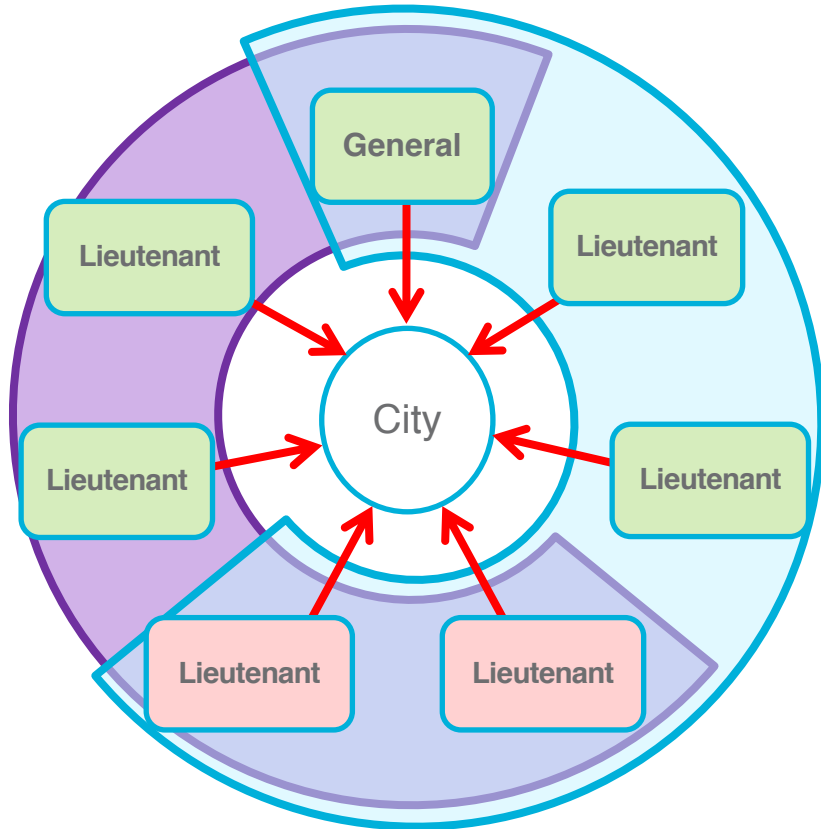
- The implementation of the seminal PBFT consensus protocol provides consensus among validators despite a threshold of validators acting as Byzantine, i.e., being malicious or failing in an unpredictable manner.
  In the default configuration, PBFT tolerates up to t<n/3 Byzantine validators.

- n = number of nodes
  f = assumed number of faulty nodes
  Assume n >= 3f + 1

- In this example, consensus can be achieved with up to 2 nodes assumed Byzantine, i.e., being malicious or failing in an unpredictable manner.

outthink your limits

New from IBM: Sieve consensus protocol

- Basically the idea behind Sieve is to provide a fabric-level protection from non-deterministic transactions, which PBFT and similar existing protocols do not offer.

- In a nutshell, Sieve requires replicas to **deterministically agree on the output of the execution** of a request.
  If the request was deterministic in the first place, all correct replicas will have obtained the same output, and they can agree on this very result.
  However, if a request happens to produce divergent outputs at correct replicas, Sieve may detect this divergent condition, and the replicas will agree to discard the result of the request, thereby retaining determinism.

- Notice that, as discussed further below, Sieve allows false negatives, i.e., execution of non-deterministic requests that execute with the same result at a sufficient number of replicas. However, Sieve allows no false positives and any discarded request is certainly non-deterministic.
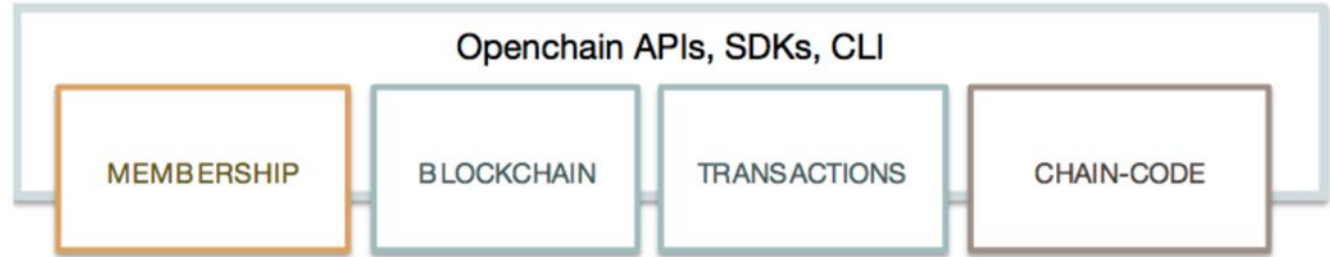
- http://www.zurich.ibm.com/~cca/papers/sieve.pdf

outthink your limits

Hyperledger – Application Programming Interfaces

APPLICATION

PROGRAMMING

INTERFACES

Hyperledger

Openchain APIs, SDKs, CLI

MEMBERSHIP | BLOCKCHAIN | TRANSACTIONS | CHAIN-CODE

includes the REST and JSON RPC APIs, events, and an SDK for applications to communicate with the network. SDK will be available in **Golang, JavaScript, and Java**; additional programming languages can be added as necessary. The API spans the following categories:

- **Identity** - Enrollment to get certificates or revoke a certificate
- **Address** - Target and source of a transaction
- **Transaction** - Unit of execution on the ledger
- **Chaincode** - Program running on the ledger
- **Blockchain** - Content of the ledger
- **Network** - Information about the blockchain network
- **Storage** - External store for files or documents
- **Event** - Sub/pub events on blockchain

outthink your limits

Hyperledger Fabric – Protocol Specification

PROTOCOL SPECIFICATION

https://github.com/hyperledger/fabric/blob/master/docs/protocol-spec.md

The very fine print ☺
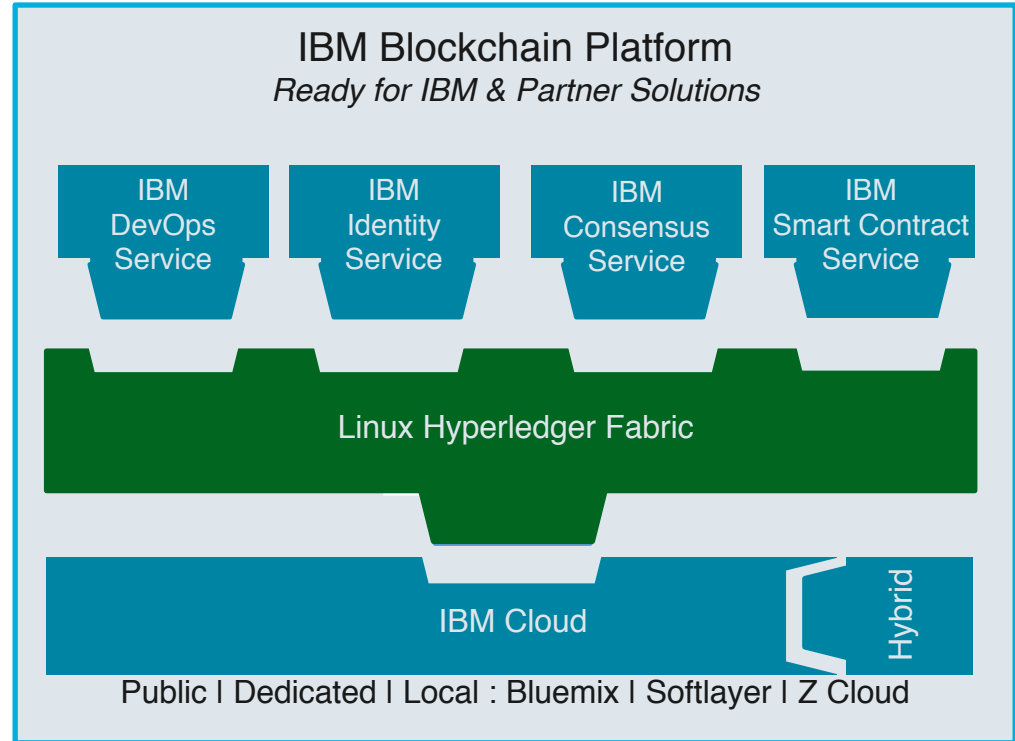
outthink your limits

IBM Blockchain Platform – Powering Always-On Business Networks

Capabilities

- Complete DevOps Lifecycle via Bluemix

- Smart contract language and API standards

- Enterprise-grade identity, security and privacy

- Seamless hybrid integration with legacy systems

- Market leading performance and scalability

IBM Blockchain Platform
Ready for IBM & Partner Solutions

| IBM DevOps Service | IBM Identity Service | IBM Consensus Service | IBM Smart Contract Service |

Linux Hyperledger Fabric

IBM Cloud

Hybrid

Public | Dedicated | Local : Bluemix | Softlayer | Z Cloud

outthink your limits

Blockchain on IBM Bluemix

IBM Blockchain API

Interact with the enterprise blockchain through IBM Blockchain API

Block Show/Hide | List Operations | Expand Operations

GET /chain/blocks/{Block} Individual block information

Blockchain Show/Hide | List Operations | Expand Operations

GET /chain Blockchain information

Chaincode Show/Hide | List Operations | Expand Operations

POST /chaincode Service endpoint for Chaincode operations

Network Show/Hide | List Operations | Expand Operations

GET /network/peers List of network peers

Registrar Show/Hide | List Operations | Expand Operations

POST /registrar Register a user with the certificate authority

DELETE /registrar/{enrollmentID} Delete user login tokens from local storage

GET /registrar/{enrollmentID} Confirm the user has registered with the certificate authority

GET /registrar/{enrollmentID}/ecert Retrieve user enrollment certificate

GET /registrar/{enrollmentID}/tcert Retrieve user transaction certificates

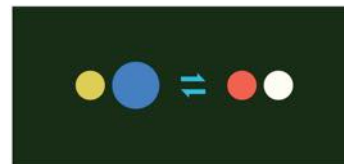**Transactions** Show/Hide | List Operations | Expand Operations

GET /transactions/{UUID} Individual transaction contents

[BASE URL: , API VERSION: 1.0.0]

DevOps Services on Bluemix!

IBM Blockchain services will help developers create and manage a blockchain network that can be used to manage transactions. Developers can create private and secure digital assets in test applications that can be traded quickly and securely over permissioned networks.

DevOps Service

Car Lease Demo

This more advanced app shows a sample supply chain process between multiple parties.

▶ View Demo (03:01)

Marbles App

This starter app shows how to make a simple asset transaction with a blockchain network.

↪ Single click deploy to IBM Bluemix

↪ View sample code on Github

Commercial Paper Demo
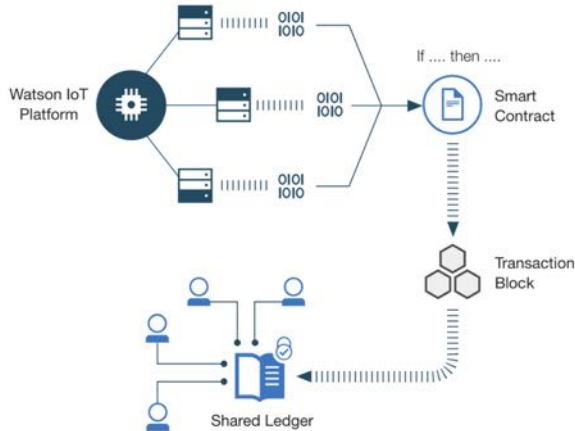
This app shows how a commercial paper trading network might be implemented with a blockchain network.

↪ Github Code   ↪ Deploy to Bluemix

http://www.ibm.com/blockchain/for_developers.html

outthink your limits

IBM Watson IoT with Blockchain on Bluemix

Integrate Watson IoT Platform with Blockchain

The Watson IoT Platform has a built-in capability that lets you add selected IoT data to a private blockchain. The protected data is shared among only the business partners involved with the transaction.
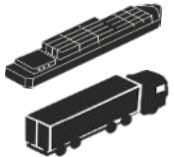
- IBM Blockchain provides the private blockchain infrastructure of distributed peers that replicates the device data and validates the transaction through secure contracts.

- Watson IoT Platform translates existing device data, from one or more device types, into the format needed by the blockchain contract APIs. The blockchain contract doesn't need to know the specifics of your device data.

- Watson IoT Platform filters device events and sends only the required data to the contract.

Freight Transportation

Move freight with multiple transport companies, ensuring transparency and timely delivery.

Component tracking and compliance

Store provenance records for the original and replacement parts of your fleet of vehicles.

Log operational maintenance data

Store operational and maintenance records in the indelible blockchain ledger for sharing among business partners or for regulatory purposes.

http://discover-iot-blockchain.eu-gb.mybluemix.net/iot-blockchain.html

outthink your limits

Example Blockchain IoT use cases

How

Industry	Use Case	IoT Data
Logistics	Track, monitor, and report on container status and location Optimize packing and transfer of shipments	• Location • Temperature • Handling • Carrier
Electronics	Track, monitor, report on meter readings Building management systems Water heater management	• Electricity usage • Building state • Water heater usage
Finance	Enable pay-per-use models where connected devices contribute sensor reading to indicate/log usage that triggers payment	• Items consumed • Location visited • Usage of device
Manufacturing	Communicate and agree on shared information across vendors in manufacturing equipment and supply according to Digital Business Ecosystem (DBE) Core data model	• DBE Core documents • Device state • Location
Electronics	Edge computing in devices Agreements for peer-to-peer appliance, home, vehicle interactions and decisions driven by contracts on a shared ledger	• Location • Temperature • Inventory • Appliance state
Automotive	Warranty and service logging for vehicles, proof of service work performed, and logging of parts installed into vehicles	• Parts inventory • Service performed

© 2016 IBM Corporation   Page 43

outthink your limits
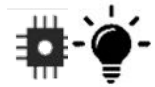
IBM Blockchain on Bluemix – test network

Get started with a test network on IBM Blockchain — complimentary during beta release

Easily develop applications while testing security, availability, and performance of a permissioned blockchain network.

http://www.ibm.com/blockchain/bluemix.html

We recently announced several security features in its blockchain offering powered by IBM LinuxONE™, the industry's most secure Linux server. IBM Blockchain networks are built on the notion of decentralized control, but some cloud environments leave back doors open to vulnerabilities. Working with teams of security experts, cryptographers, hardware experts and researchers, IBM has created essential new cloud services for tamper-resistant, trusted blockchain networks.

We offer two plans to quickly spin up your blockchain network on the cloud:

	SoftLayer	IBM LinuxONE™
Platform	SoftLayer	IBM LinuxONE™
Purpose	Development	Simulate a business network
Environment	Shared multi-tenant	Isolated single tenant
Secure services container	No	Yes
Nodes	4 nodes + Certificate Authority	4 nodes + Certificate Authority
Confidential transactions	Yes	Yes
Dashboard Monitor	Yes	Yes

outthink your limits

IBM System z support for IBM Blockchain

Blockchain z acceleration

App 1, App 2, App 3, ...

API Layer — Integrate, Connect existing Business Processes - CICS, IMS, TPF, DB2, VSAM

Smart Contracts — Elliptical Curve Digital Signatures

Cryptographic Protocols — Crypto Accelerators, In Memory (10TB)

Shared Replicated Ledger — Hashing

Consensus Algorithm — Global Security Compliance - Enterprise PKCS11, FIPS 140-2

Optimized Network between Blockchain Nodes — Up to 7X more throughput, 82% faster response time

Smart contract integration with SoR on z

IMS, CICS, TPF, DB2z

Port Authority Chain code, Customs Authority Chain code, Trucking Service Chain code, Import Bank Chain Code

IBM Blockchain Applications

5 key differentiators

1. **Secure key management** — protects transaction keys and ensures peers on the Blockchain are not at risk of being compromised.

2. **High Evaluation Assurance Level protection between environments** — enables Blockchain peers to run in protected environments isolated from other peers and other parties.

3. **Highly auditable operating environment** — allows complete auditing for all transaction logs to support forensics and compliance.

4. **Crypto optimization** — supports an environment that moves hashing and the creation of digital signatures to optimized accelerators

5. **Protection from system administrators and root users**— Blockchain operating environments protected from access by system administrators and root users.

Overview: High security business network

Service Plan on Bluemix

- Isolated and highly secured environment, distinguishing it from other cloud-hosted offerings

- Operating system, fabric, and nodes all exist in an **IBM Secure Service Container**, providing your enterprise with a high level of security

- IBM Secure Service Container also delivers **performance optimization** for peer-to-peer communication, availability, scalability, hardware encryption, & securely encrypted VMs

- Keys secured in HSM

Sign up:
https://www.ibm.com/blockchain/bluemix.html

Product documentation:
https://new-console.ng.bluemix.net/docs/services/blockchain/etn_hsn.html

IBM Cloud Service Plans
HYPERLEDGER PROJECT

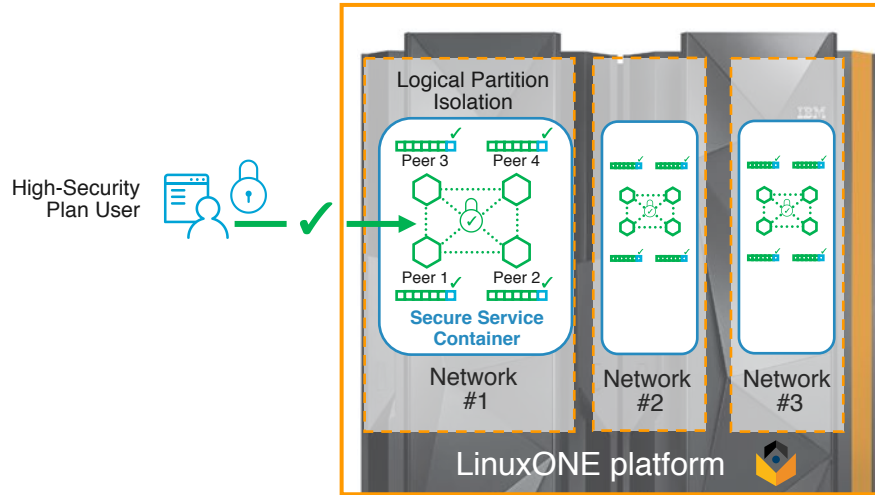|	Starter Plan	High Security Plan
Purpose	Development	Simulate a business network
4 nodes + Certificate Authority		
Dashboard for registration, monitoring, provisioning & documentation provided through Bluemix	✓	✓
Network Connections through SoftLayer	✓	✓
Cloud Provisioning & Self Service Enablement	✓	✓
Service Management and Billing through Bluemix	✓	✓
Customer Support through Bluemix	✓	✓
Environment	Shared, multi-tenant	Isolated, single tenant
Secure Service Container		✓
Highest levels of isolation in industry		✓
Compliance for highly regulated industries (Keys secured in HSM)		✓ *
Accelerated performance		✓

* Available in GA version

outthink your limits

Architecture
High Security Business Network

Logical Partition
Isolation

Peer 3   Peer 4

High-Security
Plan User

Peer 1   Peer 2

**Secure Service
Container**

Network
#1

Network
#2

Network
#3

LinuxONE platform

Overview: https://console.ng.bluemix.net/docs/services/blockchain/etn_ssc.html

The **high security business network** is deployed as an **appliance** into a **Secure Service Container**, which provides the base infrastructure for hosting Blockchain services.

The appliance combines operating systems, Docker, middleware, and software components that work autonomously to provide core services and infrastructure with optimized security.

outthink your limits

Secure Service Container
High Security Business Network

Secure Service Container (SSC) ensures …

Appliance Content (i.e., Blockchain)

SSC Software Runtime Environment

SSC

Secure Execution Context

Mainframe & LinuxONE platform

Secure Service Container
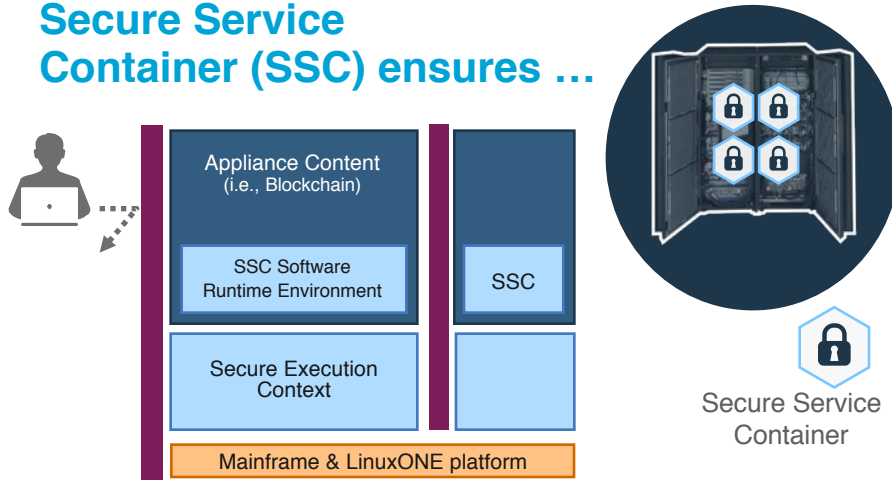
No system admin access, ever

- Once the appliance image is built, OS access (ssh) is not possible
- Only Remote APIs available
- Memory access disabled
- Encrypted disk
- Debug data (dumps) encrypted

How the Secure Service Container boot sequence works …

Protected Memory (SSC PAR)

Firmware Bootloader
- signature check
- **decryption**

check

decrypt

Software Bootloader
- Disc Encryption Key

open

LUKS

Software Image & Data
- Disc Encryption
- LVM

SE

Encrypted Software
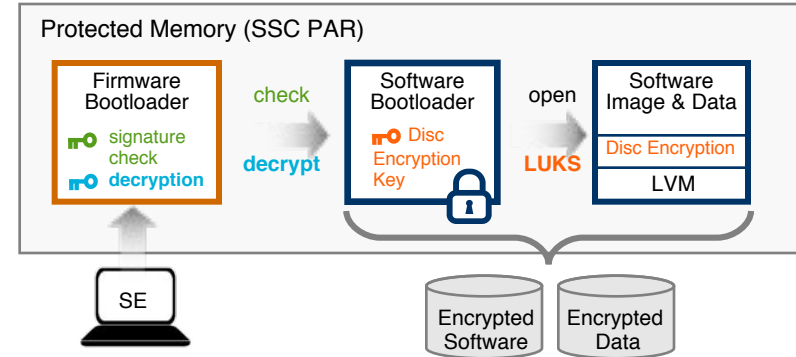
Encrypted Data

1. Firmware bootloader is loaded in memory
2. Firmware loads the software bootloader from disk
   i. Check integrity of software bootloader
   ii. Decrypt software bootloader
3. Software bootloader activate encrypted disks
   i. Key stored in software bootloader (encrypted)
   ii. Encryption/decryption done on the flight when accessing appliance code and data

outthink your limits

IBM Blockchain Offerings

Hyperledger fabric
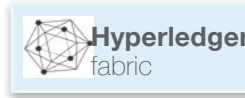
IBM managed on IBM cloud

self managed

Starter

- Start writing chaincode in seconds
- Integrated dashboard, logs and tools
- Community samples, tutorials, and quickstarts

High Security Business Network

- High performance and reserved capacity
- Best in Industry security, isolation and spec support
- Proven Audit environment for compliance and forensics

Docker

any Docker environment

IBM offers technical support for x86, Power and System z

IBM Blockchain Starter for **Developers**	**IBM Blockchain** for High Security Business Network
Public Beta	**Generally Available**
provision now on IBM Bluemix!	**Available on IBM Bluemix!**

Support for Hyperledger Fabric

Generally Available

https://hub.docker.com/r/ibmblockchain/fabric/

G A

outthink your limits

Key clients we've been working with using HSBN

Client	Industry	Solution (why blockchain)
IBM Global Finance	Global Finance	Dispute Resolution Manage disputes between business partners and suppliers
Global Trade Company	Europe Global Trade	Reduce Inefficiencies in Global Trade Replace paper bills of lading (describe goods)
Major Retailer	USA Retail Supply	Reduce efficiencies in Retail Supply Chain (joint with major goods supplier and major transportation company)
Everledger	UK, High value assets	Address Provenance, fraud: tracking high value assets with initial focus on the diamond industry.
Wells Fargo	USA Banking	Global Banking: Inter-bank Banking payment reconciliation and settlement

outthink your limits

IBM and Hyperledger in Action

HSBC, Bank of America, IDA	Trade Finance - Letter of Credit
ABN AMRO	Financial Restructuring & Recovery
Crédit Mutuel Arkéa	Consortium Shared Ledger
Japan Exchange Group (JPX)	Post Trade
Kouvola Innovation	Supply Chain Logistics
London Stock Exchange	Market Innovation
Mizuho	Digital Currency
IBM Global Finance	Shadow Chain for Dispute Resolution

outthink your limits

New Hyperledger pilot announcements:

How

http://www-03.ibm.com/press/us/en/pressrelease/50615.wss

CLS to develop netting service:
CLS Group (CLS), a leading provider of risk management and operational services for the global foreign exchange (FX) market recently announced that it has secured 14 institutions to join its new payment netting service on the Hyperledger blockchain for buy-side and sell-side institutions.

http://www-03.ibm.com/press/us/en/pressrelease/50816.wss

Walmart, IBM and Tsinghua University Explore the Use of Blockchain to Help Bring Safer Food to Dinner Tables Across China

http://www-03.ibm.com/press/us/en/pressrelease/50861.wss

SBI SECURITIES Works with IBM to Test Blockchain Technology for Bond Trading Platform

outthink your limits

Blockchain Solution for IBM Global Financing (IGF)

How

Our Commercial Financing business provides working capital to IT suppliers, distributors and partners through financing of inventory and accounts receivables

What?

Improve the efficiency of our commercial financing business by sharing data in a secure and transparent manner on Blockchain
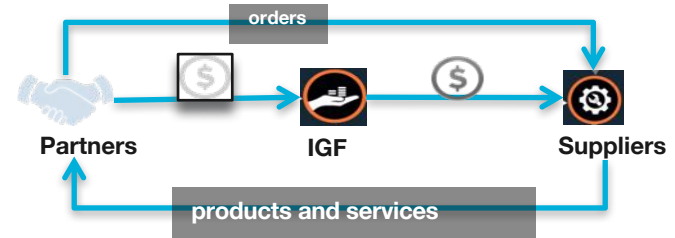
How?

- Blockchain enables Comprehensive View of key operational data:

Purchase Order > Transaction Approval > Shipments > Invoices > Remittances

Benefits:

- Fewer disputes & faster settlement

- Reduction in dispute resolution time: 40+ days to under 10 days

- Improved capital efficiency; freer flow of capital

orders

Partners — **IGF** — **Suppliers**

products and services

IGF world-wide statistics		
4000+ Partners and Suppliers	**2.9M** Invoices / year	**$44B** Financed / Year
$100M Capital tied up any time!	**25,000** Disputes / year	**$31K** Avg. disputed invoice value / **44 days** Avg. time to resolve a dispute

outthink your limits

■ Information Available in the Current System   □ No Information Available in the Current System

Order Placed	Transaction Approval Request	Approved / Rejected	Shipment Sent	Invoice to IGF	IGF Remittance to Supplier Initiated	Proof of Delivery	Payment Due to IGF from Partner	Partner Remittance to IGF Initiated
							⚠️	

Partner 945
Business Partner

Dispute: Proof of Delivery / Not Received

Dispute ID:	279283
Invoice / Loan:	11679040
Amount:	$ 1088.36

outthink your limits

Summary

Blockchain …

– is a shared, replicated, permissioned ledger technology

– can open up business networks by taking out cost, improving efficiencies and increase accessibility

– addresses an exciting and topical set of business challenges, which cross every industry

IBM …

– supports the Linux Foundation Hyperledger open standard, open source, open governance Blockchain

– has an easy to access, proven and incremental engagement model giving customers the confidence to get started NOW

outthink your limits

Engagement model overview

How

Let's Talk	Blockchain Hands-on	First Project	Scale
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 or face to face	*Remote or face to face*	*Face to face*	*Face to face*
Free of charge	*Free of charge*	*For fee*	*For fee*

outthink your limits
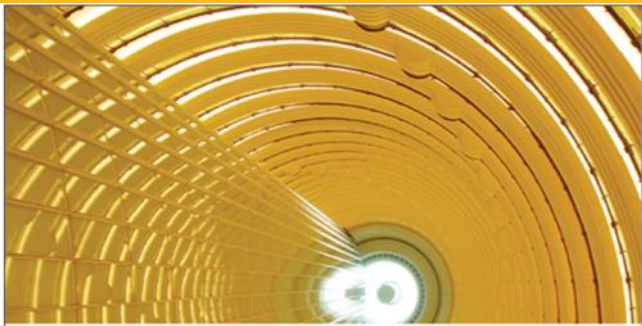
Fast forward
Rethinking enterprises, ecosystems and economies with blockchains
IBM Institute for Business Value

BANKING ON BLOCKCHAIN:
CHARTING THE PROGRESS OF
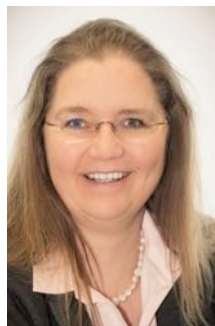DISTRIBUTED LEDGER TECHNOLOGY
IN FINANCIAL SERVICES

Finextra

Empowering the edge
Practical insights on a decentralized Internet of Things
IBM Institute for Business Value

Device democracy
Saving the future of the Internet of Things
IBM Institute for Business Value

IBM®

IBM

Elke Kunde
Solution Architect

Industries & Business Development
Technical Sales
Banking & Financial Markets
Blockchain Technical Focalpoint

IBM Deutschland GmbH
Am Weiher 24
65451 Kelsterbach

Mobile: +49 170 5626563
Phone: +49 7034 643 0365

Mail: elke.kunde@de.ibm.com
www.linkedin.com/in/elke-kunde
www.xing.com/profile/Elke_Kunde

Thank you!

Backup

Further Information – Use case Links

HSBC, Bank of America, IDA:

ABN AMRO:

https://www.abnamro.com/en/newsroom/blogs/arjan-van-os/2016/walking-the-walk-exploring-the-power-of-blockchain.html

Crédit Mutuel Arkéa:

http://www.coindesk.com/ibm-completes-blockchain-trial-french-bank-credit-mutuel/

JPX:

http://www.ibm.com/press/us/en/pressrelease/49088.wss

Kouvola Innovation:

http://www.ibm.com/press/us/en/pressrelease/49029.wss

London Stock Exchange:

http://www.ibtimes.co.uk/linux-foundation-blockchain-consortium-digital-asset-ibm-credits-london-stock-exchange-board-1533798

Mizuho:

http://www.coindesk.com/mizuho-digital-currency-powered-blockchain-settlement/

IBM Global Finance:

http://www.coindesk.com/ibm-building-blockchain-dispute-resolution-system/

outthink your limits

ECB: Distributed ledger technologies in securities post-trading

- Whitepaper: https://www.ecb.europa.eu/pub/pdf/scpops/ecbop172.en.pdf

Diagram 1

Post-trade processes in the securities leg of current transactions

Diagram 2

How a distributed ledger may affect the efficiency of post-trade in the securities market, assuming current business practice continues
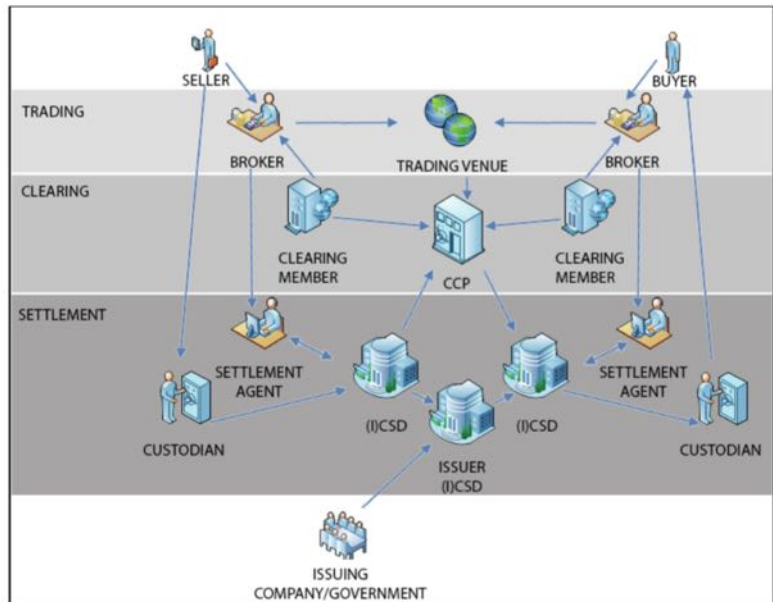

Note: (I)CSD = (international) central securities depository, CCP = central counterparty.
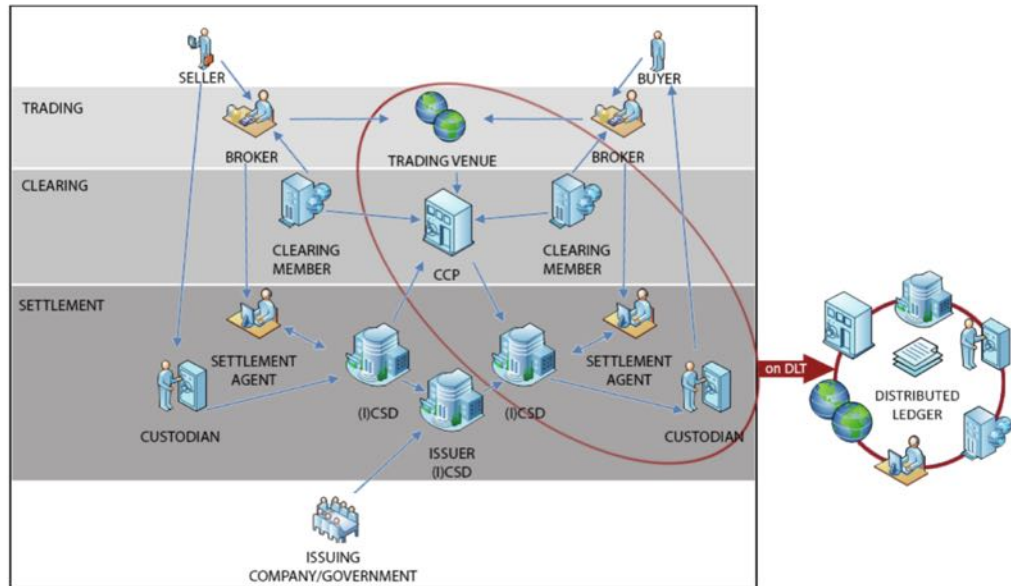
A set of post-trade institutions (in this diagram, on the buy side) may develop their own DLT for internal use. All business relations inside the red circle would then take place as straight-through processes on the distributed ledger.

outthink your limits

ECB: Distributed ledger technologies in securities post-trading (2)

Diagram 3

How a market-wide distributed ledger may affect the post-trade landscape of securities markets
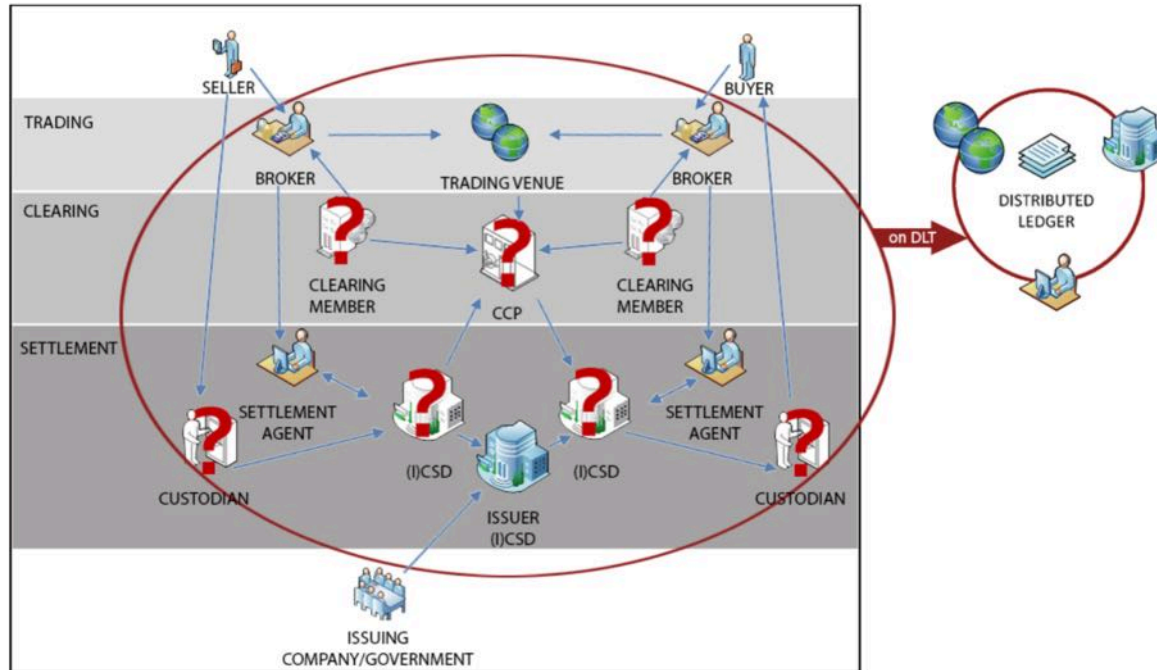

If the whole post-trade industry migrated to a distributed ledger settlement process, securities accounts would be updated automatically. Depending on the extent of the implementation of smart contracts, some layers of the industry could become redundant.

outthink your limits

ECB: Distributed ledger technologies in securities post-trading (3)

Diagram 4

How a peer-to-peer market for securities based on DLTs could affect the post-trade landscape
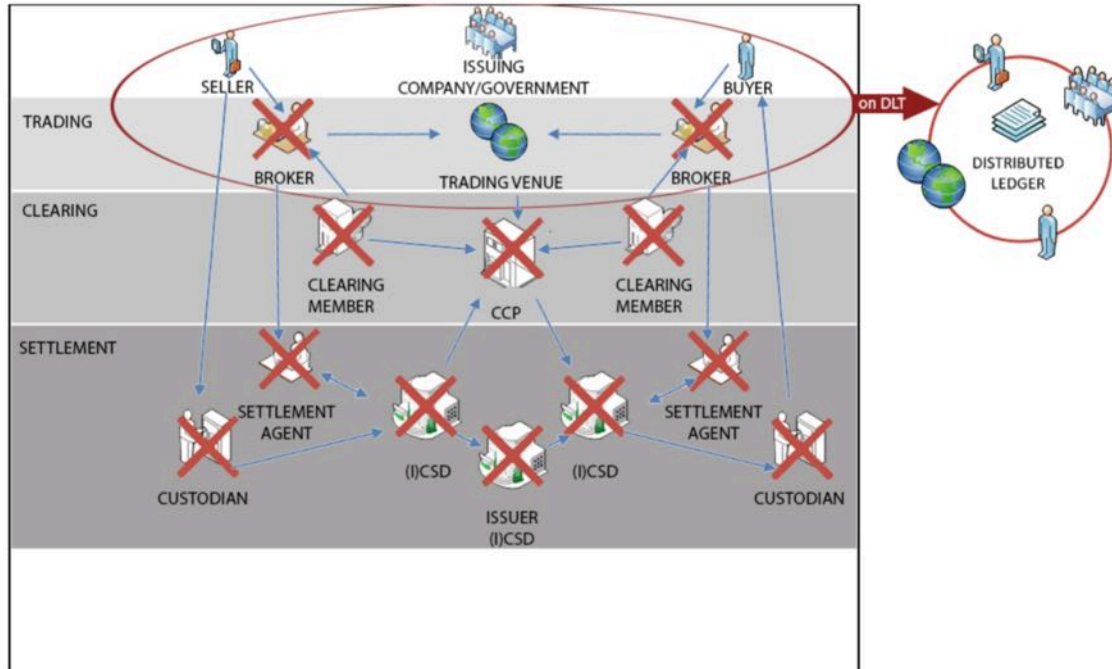
If capital markets were to migrate to a peer-to-peer model, the whole chain of intermediaries would become redundant, and companies or governments could issue their own securities on the distributed ledger.
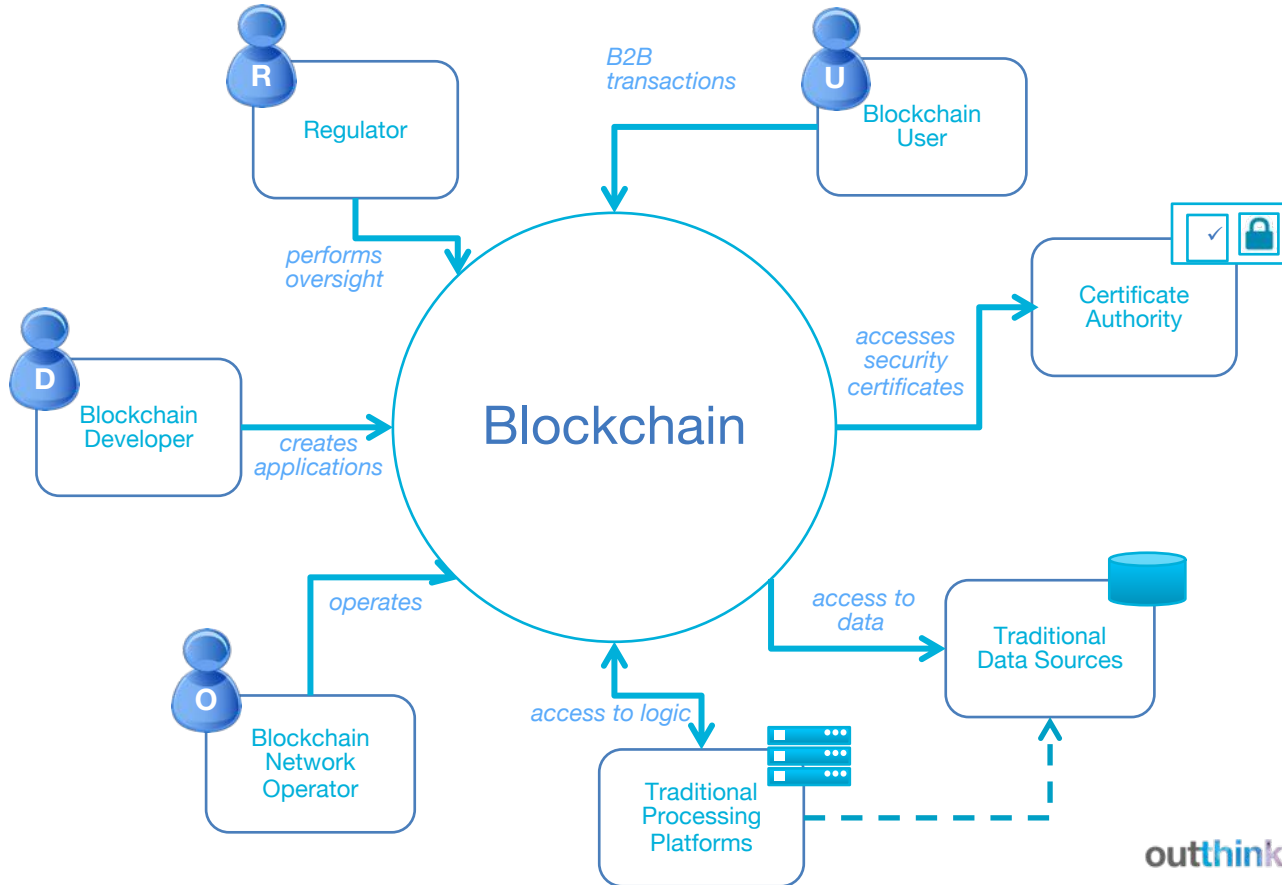
outthink your limits

Comparison Matrix of Blockchain Implementations

	Hyperledger	Ethereum	Ripple	Bitcoin
Description	General purpose Blockchain	General purpose Blockchain	Payments Blockchain	Payments Blockchain
Governance	Linux Foundation	Ethereum Developers	Ripple Labs	Bitcoin Developers
Currency	None	Ether	XRP	BTC
Mining Reward	N/A	Yes	No	Yes
State	Key-value database	Account data	None	Transaction data
Consensus Network	Pluggable : PBFT	Mining	Ripple Protocol	Mining
Network	Private or Public	Public or Private	Public	Public
Privacy	Open to Private	Open	Open	Open
Smart Contracts	Multiple programming languages	'Solidity' programming language	None	Possible, but not obvious

outthink your limits

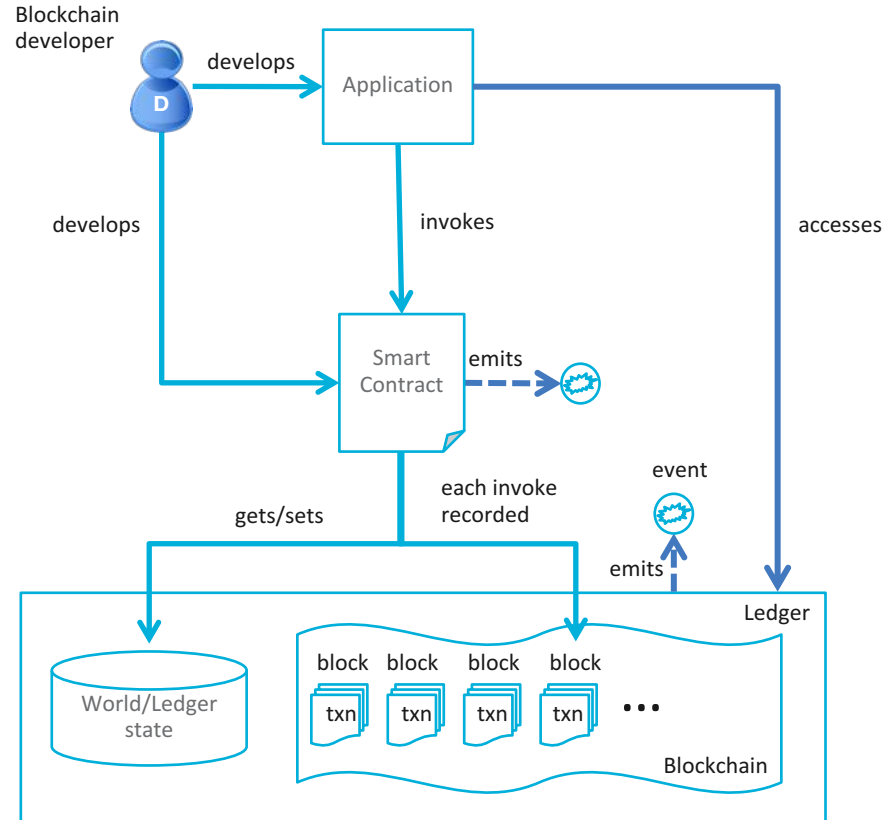# The Participants in a Blockchain Network

Blockchain Components

Ledger — contains the current world state of the ledger and a Blockchain of transaction invocations

Smart Contract — encapsulates business network transactions in code. transaction invocations result in gets and sets of ledger state

Consensus Network — a collection of network data and processing peers forming a Blockchain network. Responsible for maintaining a consistently replicated ledger

Membership — manages identity and transaction certificates, as well as other aspects of permissioned access

Events — creates notifications of significant operations on the Blockchain (e.g. a new block), as well as notifications related to smart contracts. Does not include event distribution.

Systems Management — provides the ability to create, change and monitor Blockchain components

Wallet — securely manages a user's security credentials

Systems Integration — responsible for integrating Blockchain bi-directionally with external systems. Not part of Blockchain, but used with it.

outthink your limits

Blockchain Applications and the Ledger

* Smart Contract implemented using chain code

Permissioned Ledger Access

Certificate Authority

Ecert

Tcert

Membership

Enrollment certificates (Ecerts) and Transaction certificates (Tcerts) can only be linked by CA and user

Blockchain User A

Requests certificates 1xEcert, NxTcert (stored in wallet)

uses

invokes SC txn (signed with TkeyA, encrypted with TkeyA, TkeyB...)

Application

Blockchain User B

TkeyB

shares Tcert public key

uses

Application

TkeyA
TkeyB

Accesses ledger

TkeyB

Smart contract

(signed with Ekey of origin, encrypted with validators' key)

deployed on every validating peer

SC

Consensus Network

outthink your limits