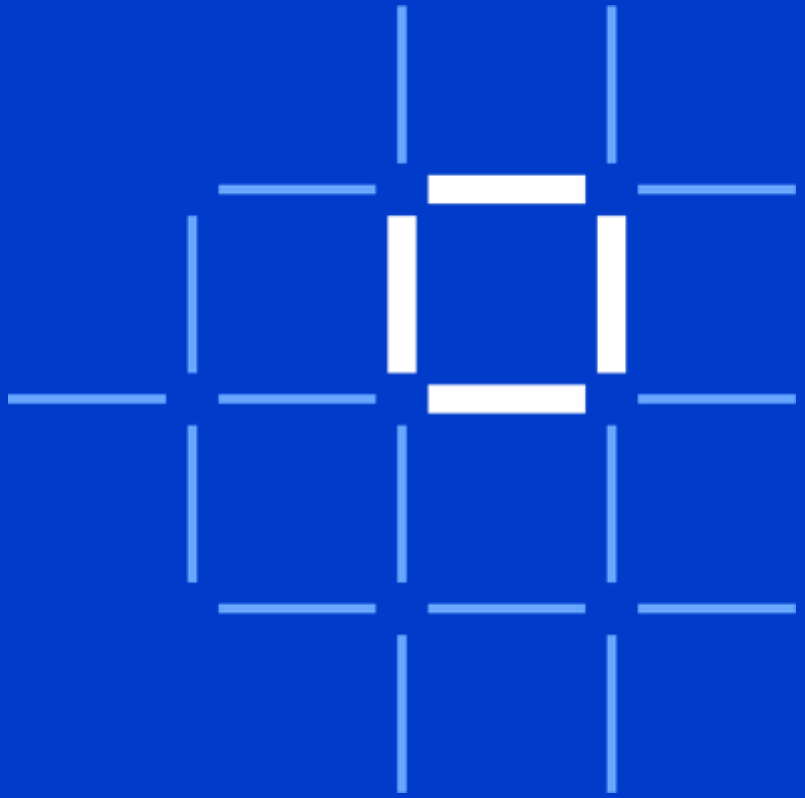
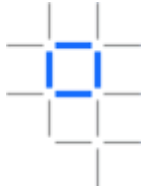
Introduction to Blockchain

NAW Billion Dollar CIO Roundtable

Kaushik Malladi
Global Technology Solutions Lead
IBM Blockchain Services
Dec 6th, 2017

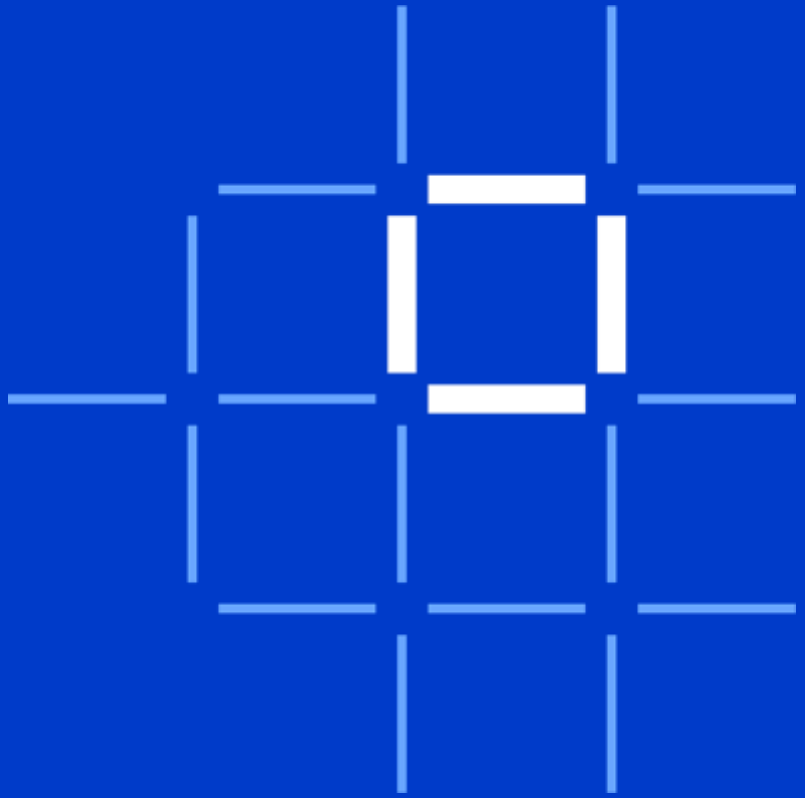


Discussion Topics

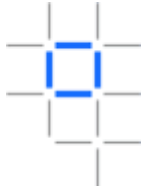


- Blockchain Concepts
- Blockchain Technology
- Typical Use Cases
- How to get started

Blockchain Concepts



Just being digital isn't the ultimate destination



You have to be willing to be disruptive...

Digital businesses are disrupting industries and professions.

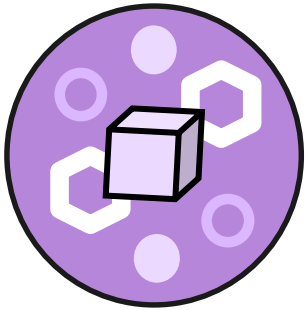
72% are vulnerable to disruption within ***three*** years

Source: FROM DATA TO DISRUPTION: INNOVATION THROUGH DIGITAL INTELLIGENCE IBM-sponsored report by Harvard Business Review Analytic Services, 2016

Harvard Business Review

Applying technology to change the game

Blockchain's early adopters – **the Explorers** – are turning uncertainty that comes with digital disruption into their unique advantage.



One in five Explorers intends to disrupt a new market or industry by completely changing the rules of the game.

66% of Explorers are experimenting with a radically different business model — the platform model — to create entirely new forms of value.

Source: Forward Together: Three ways Blockchain Explorers chart a new direction, May 2017, Global C-suite Study, IBM Institute for Business Value

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

Create New Value

Exploit new business models and eliminate inefficiencies

Optimize Ecosystems

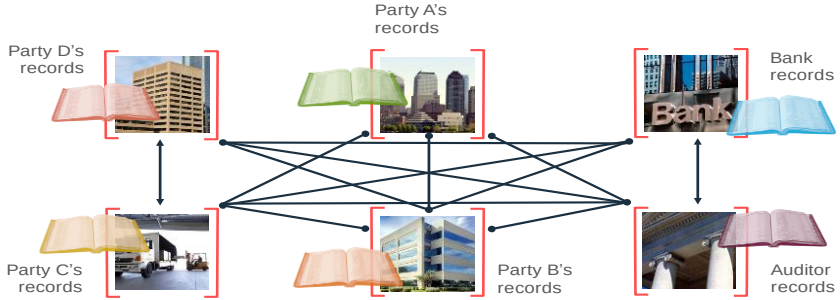
Streamline business processes and the exchange of value along your ecosystem

Reduce Risk

Replace uncertainty with transparency and a trusted decentralized ledger

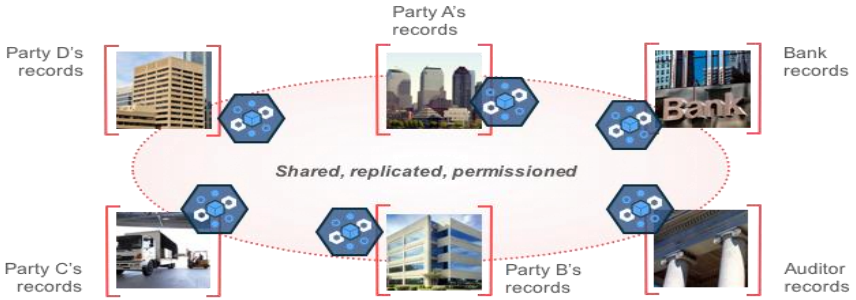
A shared, replicated, permissioned ledger …

The Problem …



… Inefficient, expensive, vulnerable

The Solution . . .



…Collaboration, immutability, trust

Blockchain needs a different perspective

Blockchain … Is a digital shared distributed ledger. It establishes trust, accountability and transparency while streamlining business processes.

Blockhain enables a business network….

- Businesses cannot operate in isolation; they benefit from connectivity
- Participants are customers, suppliers, banks, partners & regulatory bodies

... underpinned by:

- **Assets** – ownership passes across the network in return for payments, can be tangible and intangible (Product or Letter of Credit etc.)
- **Transaction** – an asset transfer onto or off the ledger
- **Contract** – Conditions for the contract to occur
- **Ledge**r – the system that records the transaction

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

Blockchain for business

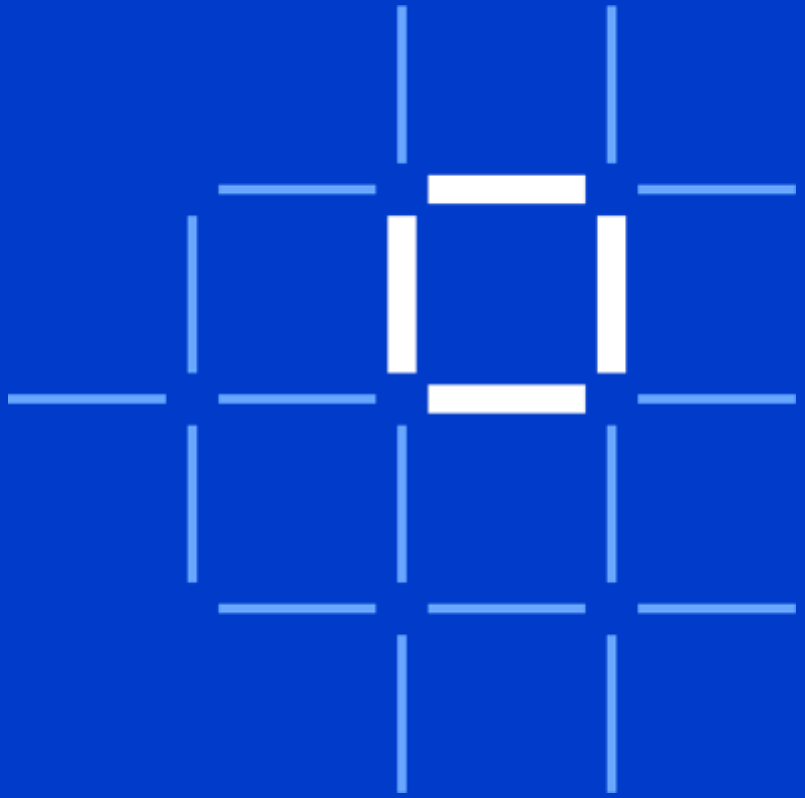
Append-only distributed system of record shared across business network

Business terms embedded in transaction database & executed with transactions

Ensuring appropriate visibility; transactions are secure, authenticated & verifiable

Transactions are endorsed by relevant participants

Blockchain Technology



Blockchain – Common Questions

What is it?

- The Blockchain is a cryptographically secured distributed ledger system that allows for the transferring or sharing of assets

How is it stored?

- The Blockchain data can be stored as a flat file, or in a database

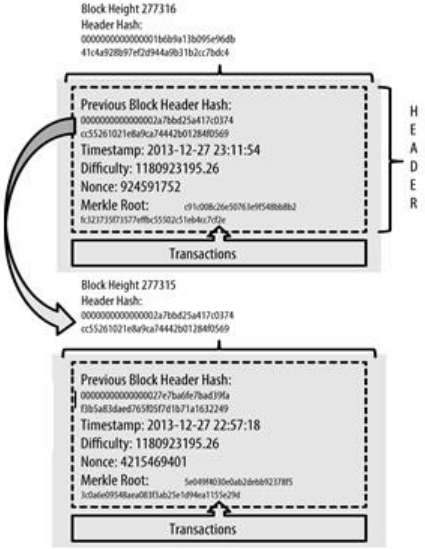
How can it be accessed?

- One can connect to the Blockchain account through web interface, mobile apps and desktop clients

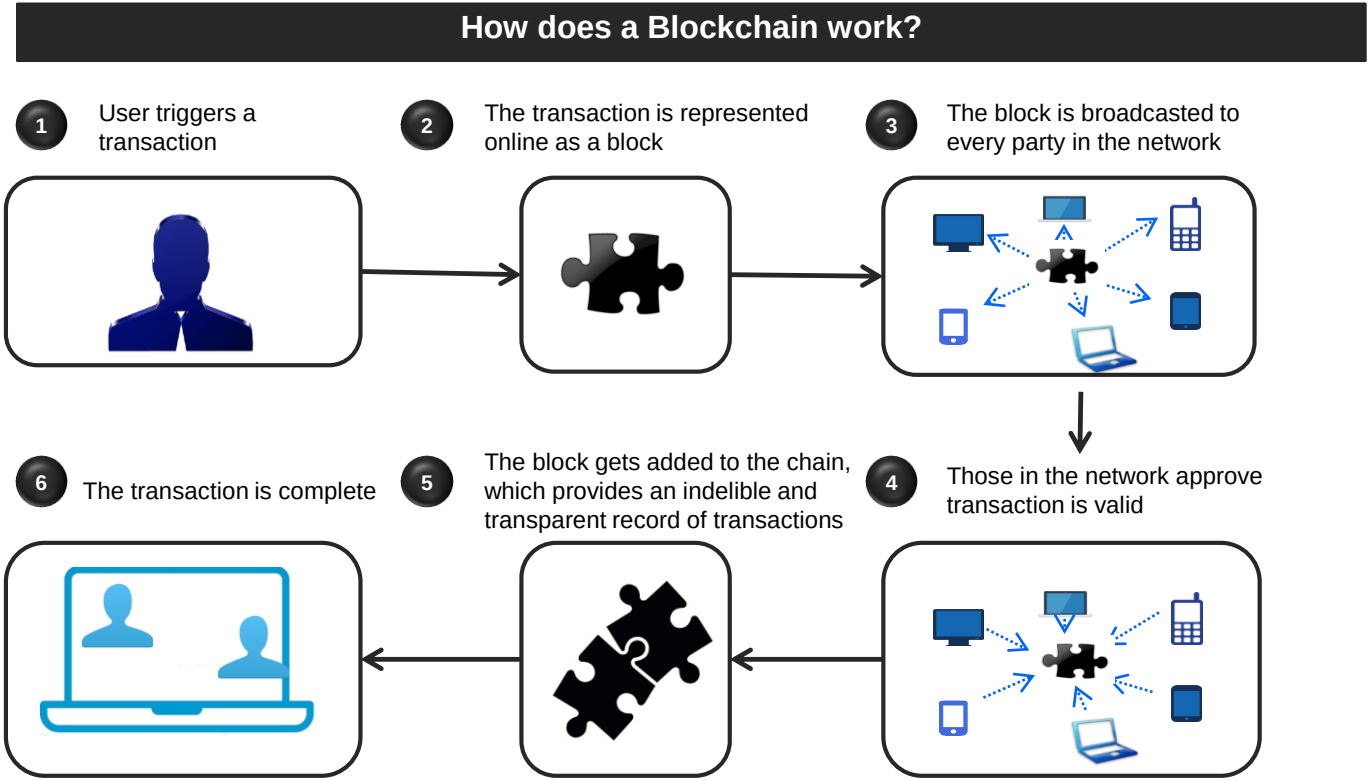
How is it structured?

- The Blockchain data structure is an ordered, back-linked list of **blocks of transactions**
- A block is a container data structure that aggregates transactions. The block is made of a header, followed by a long list of transactions that make up the bulk of its size
- Blocks are linked "back," each referring to the previous block in the chain
- Each block within the Blockchain is identified by a hash generated using cryptographic hash algorithm, which will also have references to a previous block, known as the *parent* block

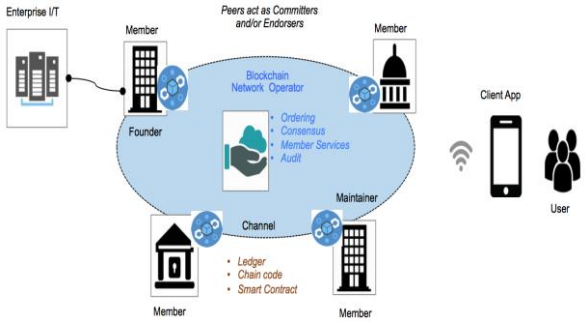
Blockchain Structure



How Transactions are updated in Blockchain



The Architecture

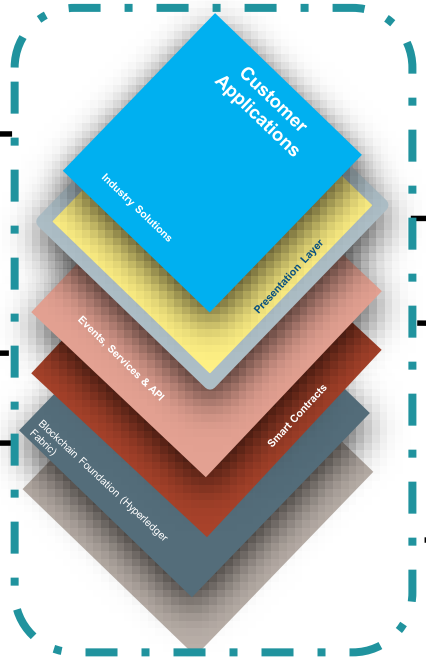


The Network

- Industry specific solutions like Trade Finance, Cross Border Payments, Trade Securities, Healthcare Records, Government Records etc.
- Cross Industry solutions like Supply Chain, KYC etc.

- Solution specific logic and workflow
- Business Rules
- Data model supporting the smart contracts

- Core Blockchain Platform as a service
- Tools and assets for building Blockchain solutions



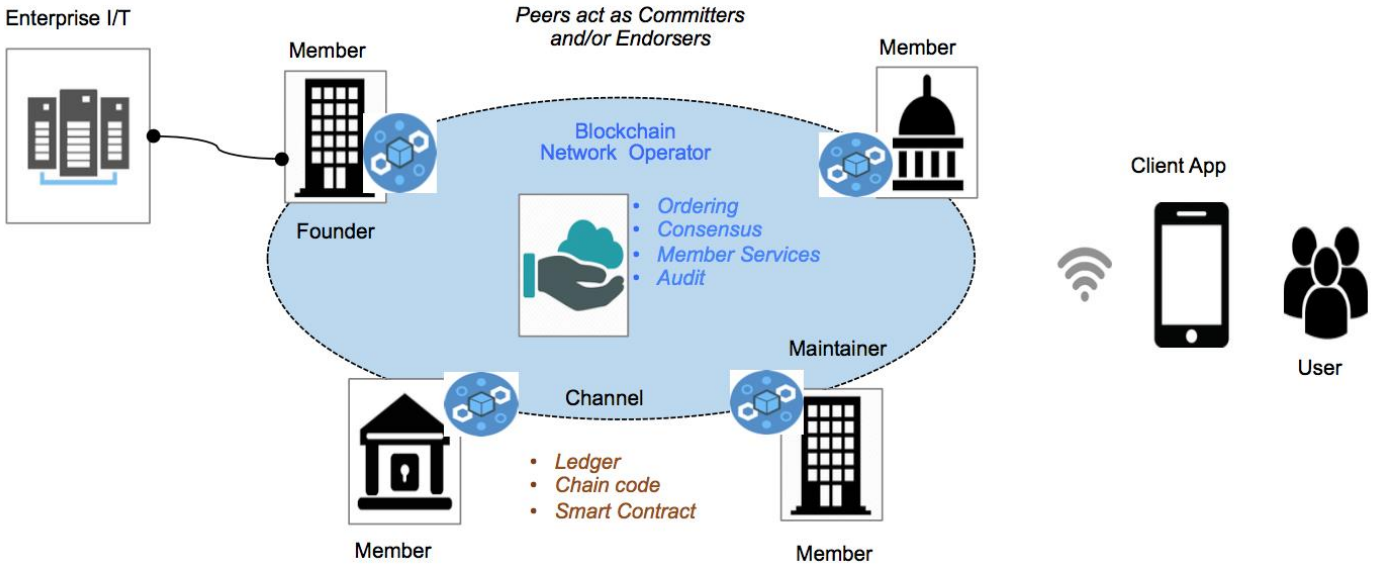
- UI Development (Web, Mobiles, iPad etc.)
- UI Design
- Customer experience Services

- Integration services with participant systems
- APIs and API management services
- Integration between the Smart Contracts and the presentation layer

- Cloud Infrastructure (Soft Layer, LinuxOne)

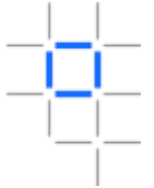
The Stack

Under the covers of a Blockchain



Role	Key Activities
Developer	Develops Client App, Chain Code, and Integration/Connectors to Blockchain Network
Member	Operates Blockchain Node & Chaincode executed against network ledger
Service Provider	Provides Blockchain Services or Solution Development
Network Operator	Operates Blockchain Business Network

Fabric is the foundation



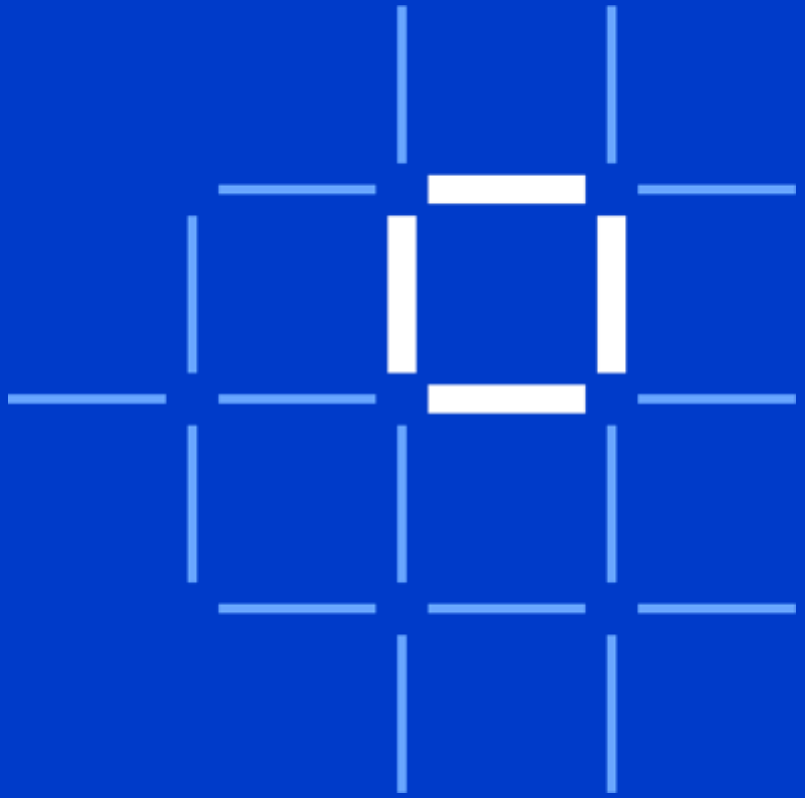
	Hyperledger	Ethereum	Ripple	Bitcoin
Description	General purpose Blockchain	General purpose Blockchain	Payments Blockchain	Payments Blockchain
Governance	Linux Foundation	Ethereum Developers	Ripple Labs	Bitcoin Developers
Currency	None	Ether	XRP	BTC
Mining Reward	N/A	Yes	No	Yes
State	Key-value database	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

Blockchain Fabrics are rapidly evolving. Please check to ensure the most current information.

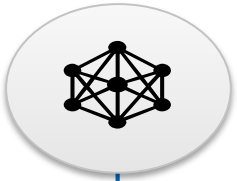
Protocol comparison

MUST HAVE	Hyperledger Fabric	Ethereum	Quorum	Corda	Chain
Maturity	✓ First Hyperledger project to graduate to General availability with multiple production networks	× Limited POC implementation of mainnet forks for enterprise	× Developer sandbox only	× Limited to R3 Consortium and Financial Services	× Limited enterprise adoption
Confidentiality	✓ Partitioned execution, channels, and permissioned membership	× Only possible through forks of the mainnet	× All nodes are aware of the existence of transactions	✓ Supported through ”flow” logic structure	× Limited confidentiality built in
Security	✓ Internal and external security review ✓ FIPS 4+ and HSMs ✓ SSC protect entire Blockchain stack	× No data encryption or channel partition	✓ Private transactions, limited confidentiality	× Intel SGX chips only protect verification portion of Blockchain	× Permissioned model with limited data encryption
Modularity	✓ Pluggable consensus, database, and membership	× None	✓ Pluggable, supports QuorumChain and RAFT-based consensus	× Modular data store and some programmable modularity through flows	✓ Designed to be extensible
Interoperability	✓ Designed to integrate with external Blockchain fabrics ✓ Backwards compatible	× Interoperability dependent on third-party extensions	× Unclear	✓ Supports interoperability	× None
Governance	✓ Linux Foundation’s Hyperledger Project	× Ethereum Foundation drives development	× Developed internally at JPMC	× Developed internally at R3, no governance structure for open-source code	× Unclear
Licensing	✓ Apache 2 or MIT licensing	× Numerous licenses for different parts of the code	× GPL/LGPL	✓ Apache 2	× Unclear
Developer tools	✓ Hyperledger Composer free to use for developers	× Only available through third parties	✓ Cakeshop	× None – written in Kotlin, a very limited programming language	✓ Desktop application supporting developer exploration
Scalability	✓ Designed for consortium deployment with high throughput	× Designed for public network, limited by proof of work consensus	✓ Design for consortium deployment, expected to reach high throughput	× Potential for nodes to get out of sync at scale as a result of non-deterministic execution	✓ Design for consortium deployment, expected to reach high throughput
Industry	✓ Cross-industry	✓ Cross-industry	× Financial Services, aiming to become multi-purpose	× Financial Services	× None

Typical Usecases



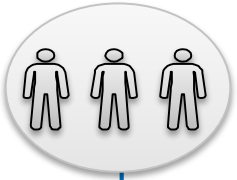
Blockchain can help solve core issues in the Distribution industry



Traceability across the value chain

Increasing speed & flexibility of supply chains drives demand for companies real time tracking

Examples:
Supply chain Finance
Supply chain visibility
Government compliance



Fraud & Provenance

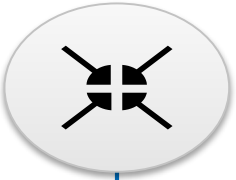
Customers and watchdogs want to know where goods come from

Examples:
Food & Product safety
Organic food verification
Authenticity

Redundant & Incomplete Data

Existing data systems (e.g. EDI) are based on messages between silos, with different organizations having different or incomplete data

Examples:
Intercompany disputes
Master Data Management



High Friction Enterprise Integration

Transaction volumes and the speed of the business lead to a highly disputed environment and eroding trust

Examples
Dispute Resolution
Trade promotions
Digital Media

Food Safety Provenance

What

- Providing consumers, suppliers, manufacturers carriers, retailers, and regulators greater transparency on their goods
- Increasing ability for key participants to meet new regulatory pressures

How

- Digitize the existing food safety process and product information on Blockchain creating a single historical record
- Vendors create new levels of trust through information sharing

Benefits

1. Improved track & trace capabilities for the consumer & industry result in decreased response time to product recalls
2. Enhanced food flow has material impact on shelf life management
3. Lower compliance costs

Supply Chain Visibility

What

- Participants have complete visibility rather than point to point messaging that is often delayed and incomplete
- Visibility granted only to participants involved in the transaction

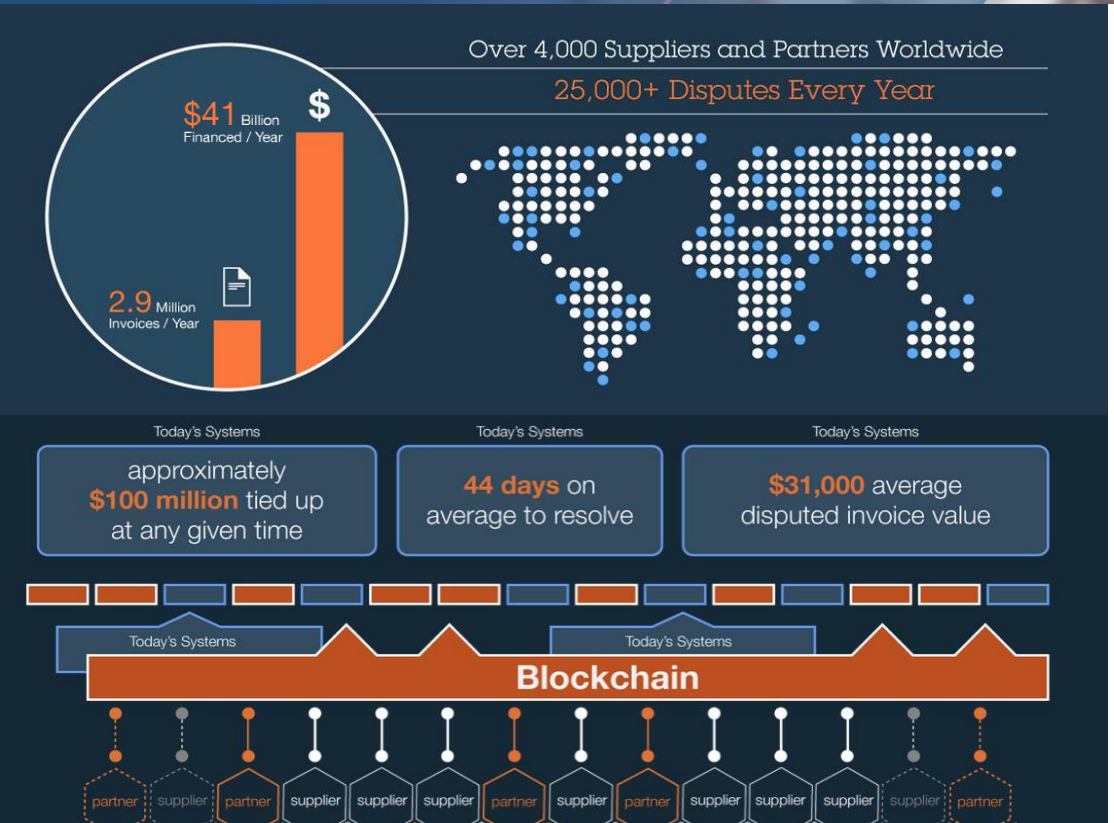
How

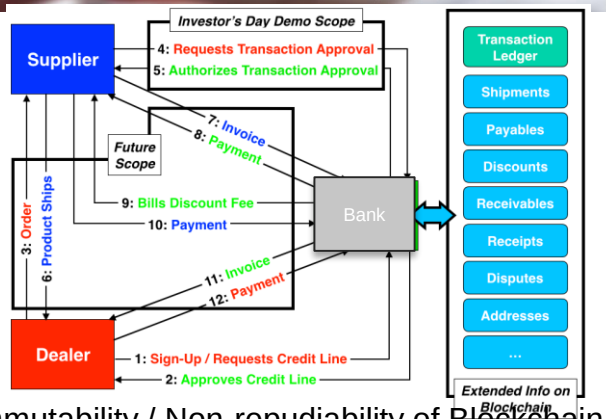
- Each participant sends their purchase order information to the Blockchain
- Real-time view into status of load based on immutable and verifiable information

Benefits

1. Trusted & holistic view into goods arriving allowing for more effective & faster order fulfillment
2. Decrease in dispute resolution time
3. Proof of delivery to meet delivery requirements by vendors

Resolving Disputes thru consensus and trust





Immutability / Non-repudiability of Blockchain ledger

Comprehensive view of all operational data

Less disputes, faster settlement

Free flow of capital between parties

Distributed & Replicated

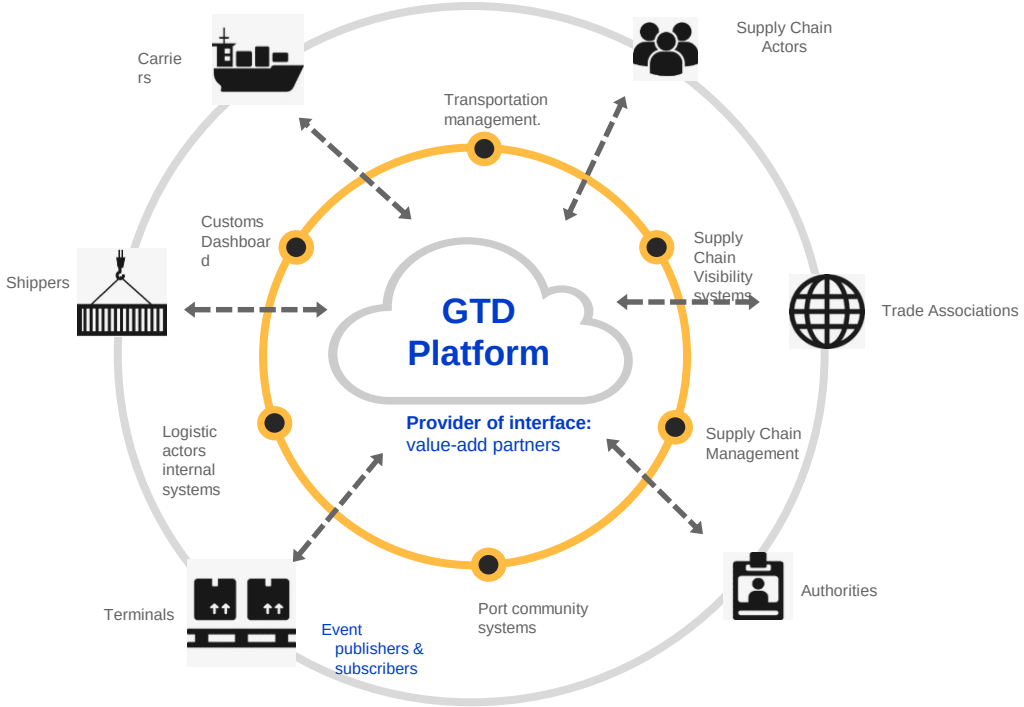
Less Outages, Highly extensible

Digitizing the Global Trade

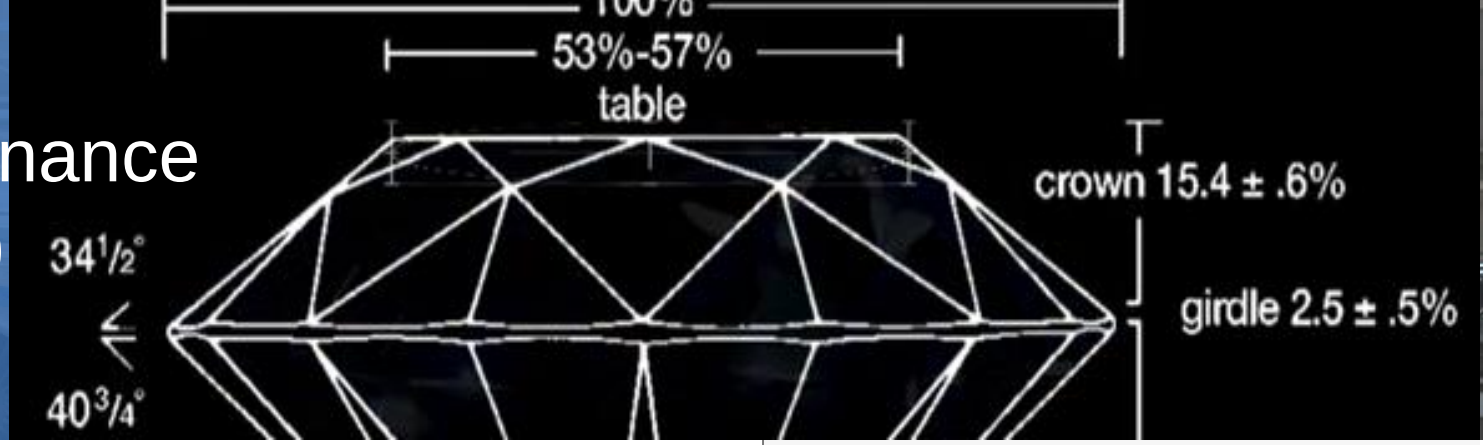
An open, extensible platform for sharing shipping events, messages, and documents across all the actors and systems in the supply chain ecosystem.

Important principles

- Detailed information remains under the control of the owner
- Neutral
- Fault Tolerant
- Everyone can work in their own systems



Asset Provenance (Everledger)



What

- Everledger develops and deploys technological solutions to markets where evidence is critical
- Starting with diamonds, 980k+ encrypted to date, but plans to expand into other industries, e.g. art, wine

How

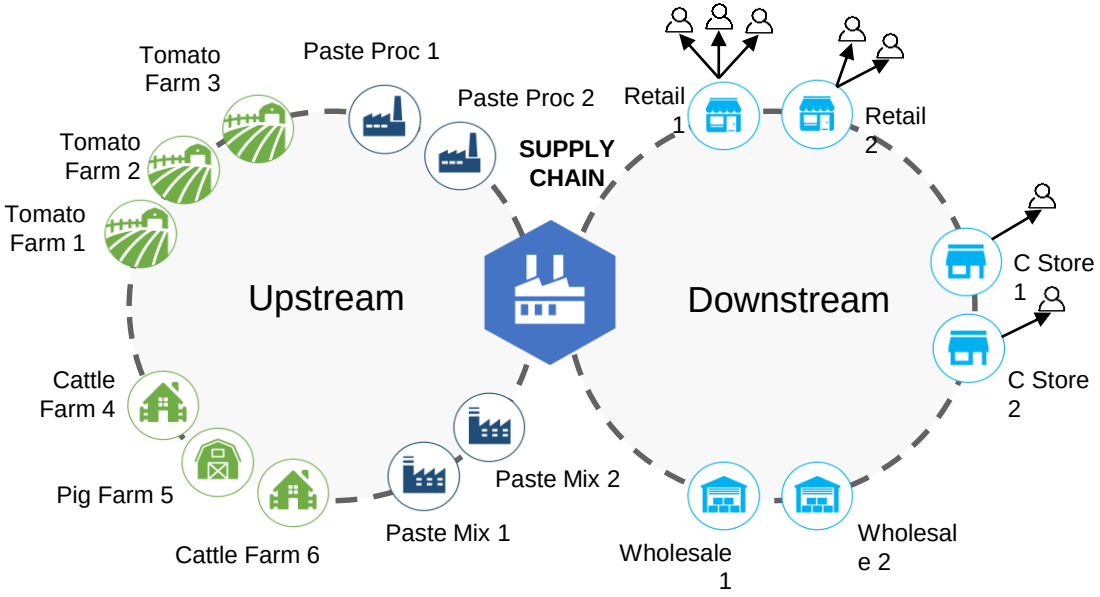
- Using Blockchain & smart contracts, Everledger provides ecosystem participants (e.g., B2B traders, consumers, etc.) immutable historical context
- Create a digital DNA signature of all diamonds written to the Blockchain (e.g. 4Cs: cut, color, carat, clarity

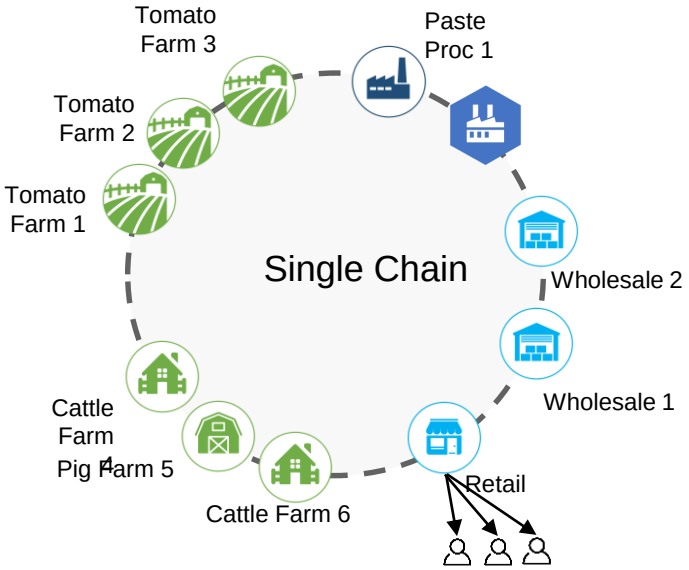
Benefits

1. Minimize fraud – 65% of fraudulent crimes go undetected
2. Address problems of double financing
3. Reduce amount of conflict stones through improving identifiability

Source: British Association of Insurers

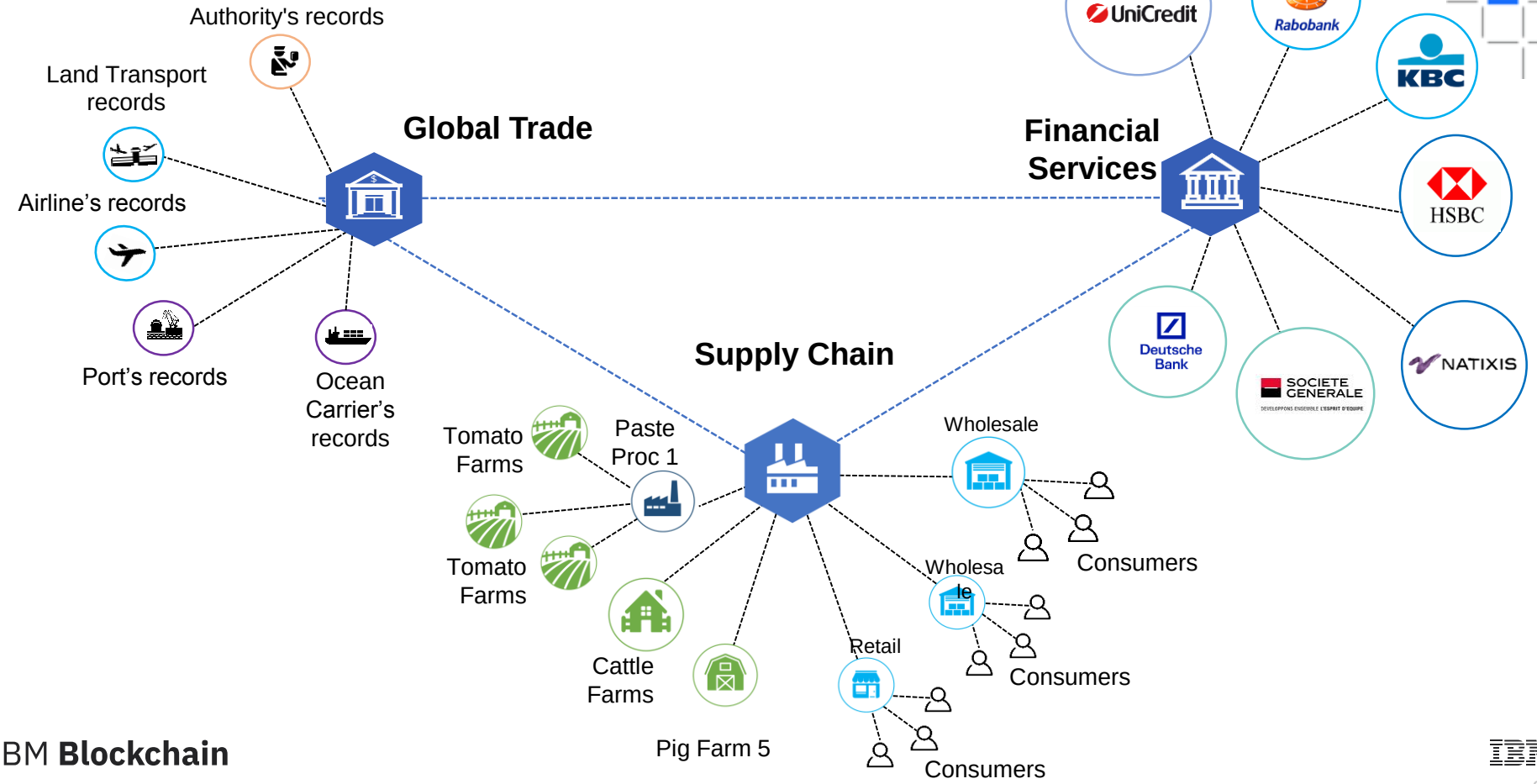
There are multiple ways to architect the network





Interoperability of chains allow seamless integration and scalability

The Vision: Network of Networks



How To Get Started

Key Considerations in defining a use case

Can we eliminate friction in the process?

Are multiple parties, Internal or External, involded?

Why Can't a single database handle it?

How can we drive trust?

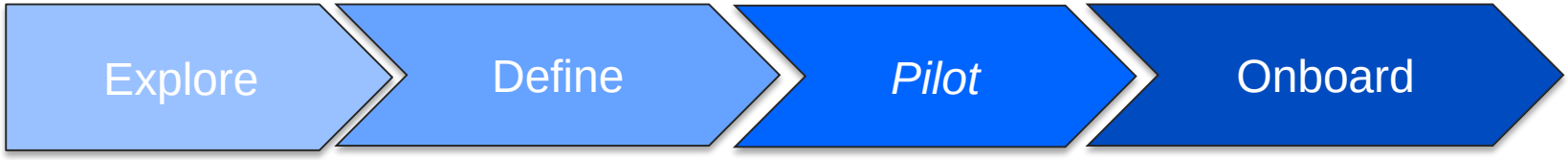
Is the sum greater than the parts?

Can business rules be applied upstream or downstream to improve the value chain?

Can we drive new business models?

Can we drive additional revenue streams?

The End to End Life Cycle



Explore	Define	Pilot	Onboard
Technology Review	Finalize Usecase	Develop solution	Onboard Partners
Technology learning thru PoT	Initial Business Case	Initial partner onboarding	Run solution
Identify Requirements Skills Infrastructure Potential partners	Network Partners (Pilot)	Refine solution	
Identify Usecases			
Stakeholder education			

Typically PoT's 6- 12 weeks long and are NOT heavy on enterprises.
Key skills required are an Data Analysts, Architect and Java like skills.

Thank you

Kaushik Malladi
kmalladi@us.ibm.com
203-482-0433

Questions? Tweet us or go to ibm.com/Blockchain

@IBMBlockchain
IBM Blockchain
IBM Blockchain

IBM **Blockchain**

IBM