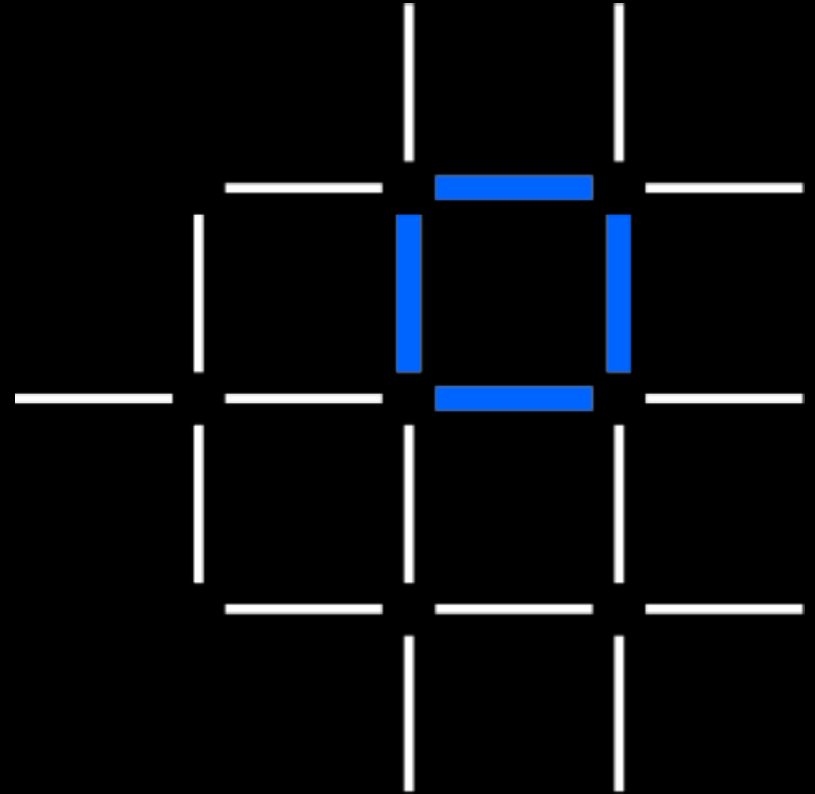# Blockchain Explained

An Introduction to Blockchain for Business
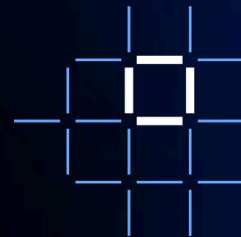
Austin Grice

IBM Blockchain

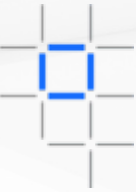IBM.

What is Blockchain
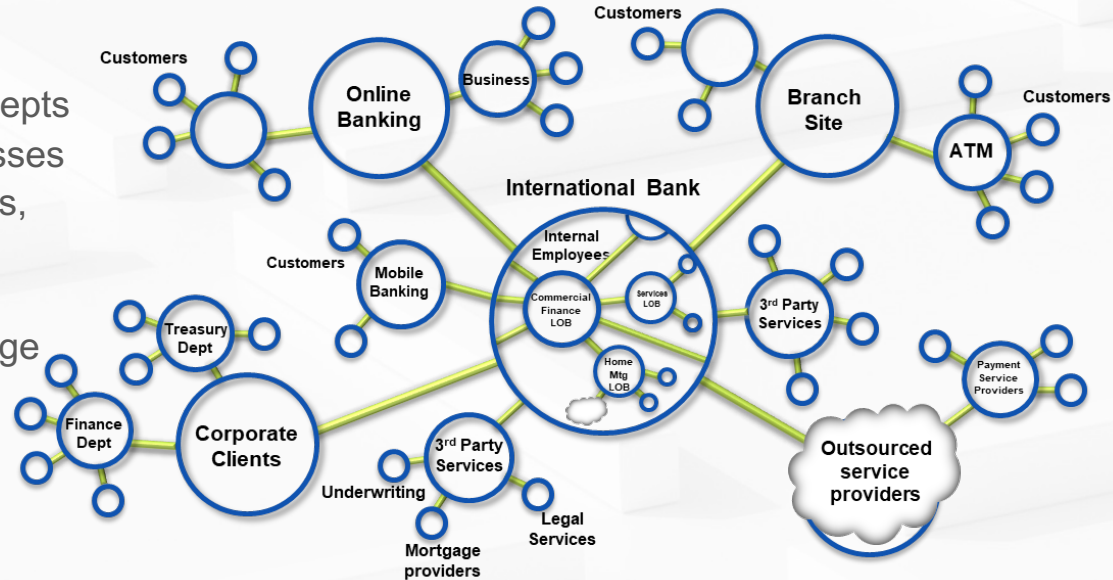
Example Networks

How IBM Can Help

Why IBM Z

What is **blockchain?**

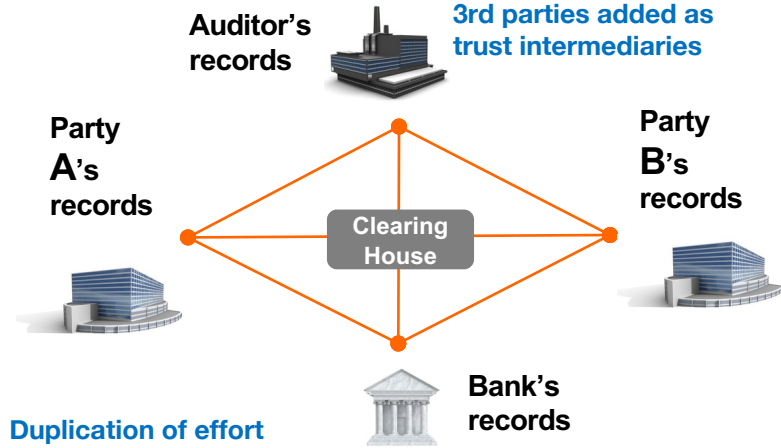- Blockchain lets you build a decentralized **business network**

- Blockchain builds on basic business concepts
  - **Business networks** connect businesses
  - **Participants** are customers, suppliers, banks, partners
  - **Assets** flow over business networks
  - **Transactions** describe asset exchange
  - **Contracts** underpin transactions
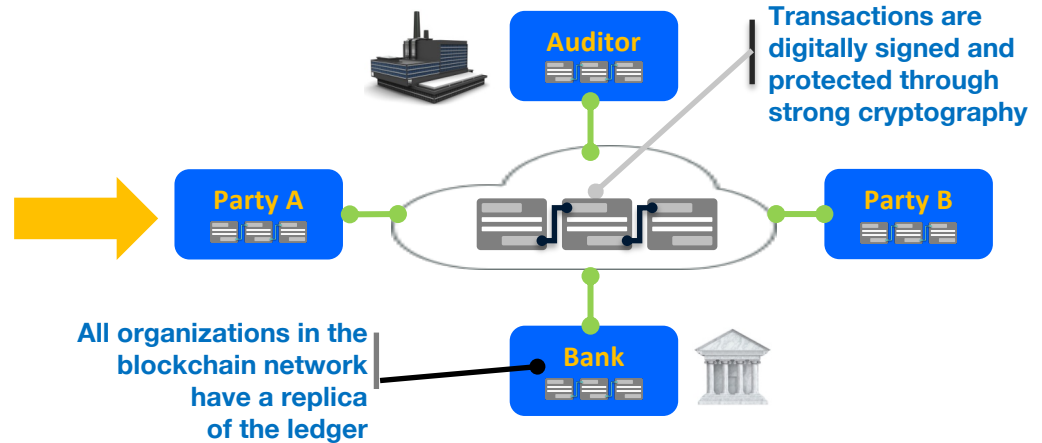 - The **ledger** is a log of transactions

IBM Blockchain

Traditional

Auditor's records

3rd parties added as trust intermediaries

Party A's records

Party B's records

Clearing House

Duplication of effort

Bank's records

Transaction fees – Cost, Time
Data exposure - Security
Centralized entities - Risk
No central source of information - Truth

…inefficient, expensive, vulnerable

With Blockchain

A shared, replicated, permissioned ledger

Auditor

Transactions are digitally signed and protected through strong cryptography

Party A

Party B

All organizations in the blockchain network have a replica of the ledger

Bank

…provenance, immutability, finality

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. data

Cash is also an asset

- Property of anonymity
- Hard to prove and track

IBM Blockchain

Ledgers, Transactions and Contracts

- **Ledger**: an important **log** of all transactions
  - Describes the inputs and outputs of the business

- **Transaction**: an **asset transfer** between participants
  - Matt gives a car to Dave (simple)

- **Contract**: the **conditions** for a transaction to occur
  - If Dave pays Matt money, then car passes from Matt to Dave (simple)
  - If car won't start, funds do not pass to Matt (as decided by third party arbitrator) (more complex)


- *How do I know that the transaction I see is the same as the transaction you see?*

- *How do I know that the contract - the business rules associated with the transaction - are interpreted and implemented consistently between us?*

- Significant costs of reconciliation, dispute resolution and legal processes

IBM Blockchain

IBM

Blockchain aims to solve the problems of ledgers and contracts

by allowing transactions and business rules to be **shared** between participants of the network

Shared Ledger
Distributed system of record, shared across business network. Replicated and synchronized ledger with no central administrator
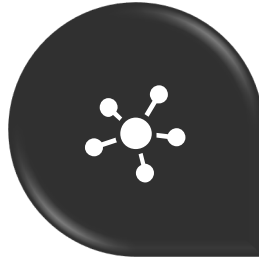
Smart Contract
Provides the shared implementation of the business rules associated with each transaction

Privacy
Ensuring appropriate visibility; transactions are secure, authenticated & verifiable
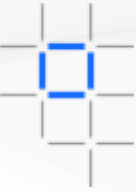
Consensus
Appropriate parties agree to valid transactions

This sharing is the foundation for innovative business solutions, including the ability to remove ambiguity and friction from trade

Broader participation, lower cost, increased efficiency

Different types of blockchain

bitcoin is an example of an unpermissioned, public ledger:

– The first blockchain application
– Peer to Peer electronic cash system
– Resource intensive

- Blockchains for business generally prioritize
  – **Assets** over cryptocurrency;   **Identity** over anonymity; **Selective endorsement** over proof of work
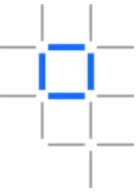
IBM **Blockchain**

Two Types of Blockchain

	Private/Permissioned	Public/Unpermissioned
Who?	Known invited parties	General public, unknown
Consensus	Selective Endorsement	Proof of Work/Stake
What is transferred?	Assets	Currency
Examples	Hyperledger Fabric	Bitcoin, Ethereum

IBM **Blockchain**

IBM

Example Networks

Further examples by (selected) industry

Financial	Public Sector	Retail	Insurance	Manufacturing
• Trade Finance • Cross currency payments • Mortgages • Letters of Credit	• Asset Registration • Citizen Identity • Medical records • Medicine supply chain	• Supply chain • **Loyalty programs** • Information sharing (supplier – retailer)	• Claims processing • Risk provenance • Asset usage history • Claims file	• Supply chain • Product parts • Maintenance tracking

IBM **Blockchain**

Today, traditional system constructs limit transparency

The Problem:

- **Data is siloed** within each company and accessing it requires a request and time

- Exchange of information takes place between a pair of partners; to get information from a distant partner may require **intermediaries** time, resources

- Most transactions are still **paper-based**, creating inefficiencies and opportunities for fraud

- Because everyone maintains their own record of transactions, **differences** take time and resources to reconcile

The food industry today

Restaurant

Logistics

Retailer

Grower

Inputs

Manufacturer
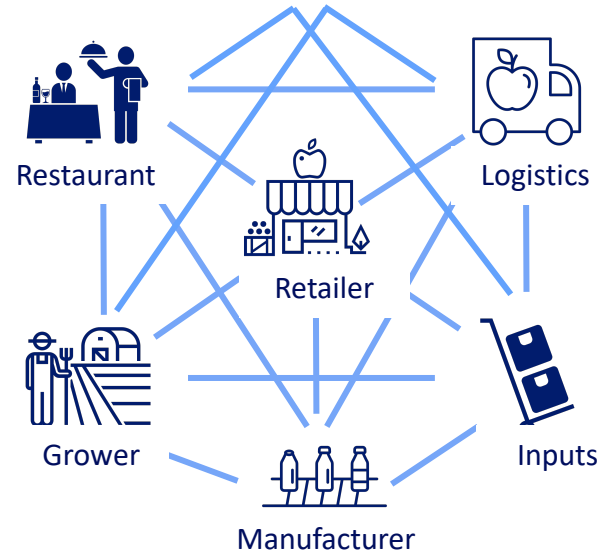
Blockchain transforms systems with trust and transparency

The Solution:

- Blockchain provides an **independent data-sharing platform**

- Once data is shared in a single data-sharing platform, everyone has **instant transparency** into the transactions they are authorized to view; no intermediation required

- **Data immutability** creates an auditable record of all transactions, disincentivizing fraudulent behavior

- **Dispute resolution** from the shared ledger can be automated saving time and resources

The food industry with blockchain

Restaurant
Retailer
Logistics
Grower
Manufacturer
Inputs
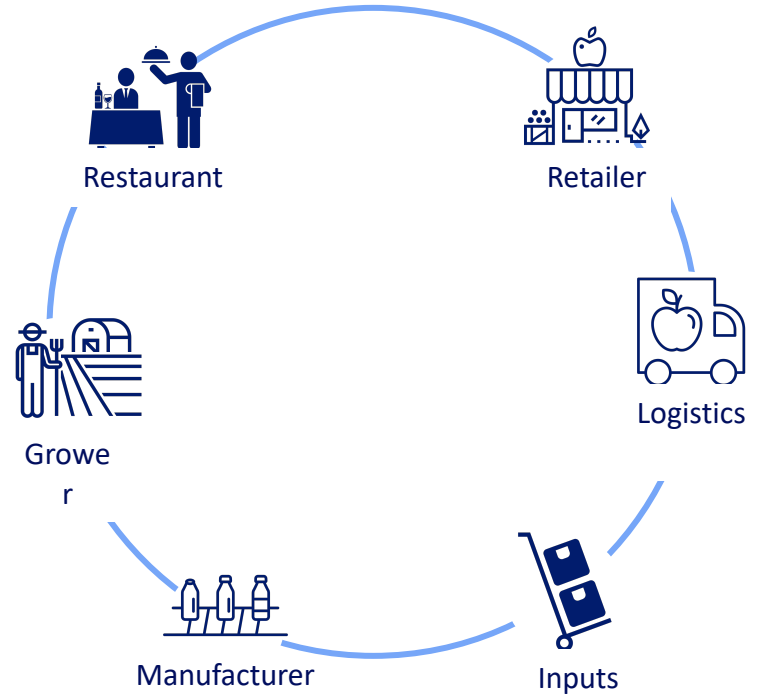
Cross-border payments today remain costly, complex and slow

Limited end-to-end transparency, fee opacity & delivery uncertainty

The Challenges

o **Slow**: Current international payments systems rely heavily on **coordination between several counterparties** exchanging both information and value, taking **days** or **even weeks to complete** transactions.

o **Costly**: **Reconciliation**, regulatory **compliance**, foreign exchange and the cost of trapped **liquidity** in correspondent banking accounts are a few factors that continue to **inflate** the true cost of cross-border payments.

o **Limited Transparency**: The involvement of multiple intermediaries creates a **complex** web of procedures and **hinders the end-to-end visibility** of cross-border payments – often resulting in **error-prone** and faulty transactions that must be reconciled later. Parties are also rarely aware of where exactly fees are deducted along the way.

o **Complicated**: Privacy and security concerns have given rise to new, often **competing regulatory requirements**, creating a **barrier** for payment processing in certain regions, **cutting off** high-potential emerging markets from participating in the global economy.

## International Payments System Today
SWIFT + Correspondent Banking

World Wire simplifies clearing & settlement to streamline cross-border payments

Faster, Cheaper & More efficient

World Wire targets industry pain points

o **Clear & Settle Faster**: Near **real-time clearing and settlement** reduces a process that traditionally takes 2-10 days, to mere **seconds**.

o **Reduce Costs**: Costs per transaction are reduced – this includes the removal and reduction of correspondent banking fees, capital requirements, regulatory costs, and reconciliation costs – allowing for **improved capital efficiency**.

o **Increase Transparency**: Financial institutions receive unprecedented **end-to-end transparency** of a payment from initiation through receipt by the receiving financial institution – **reducing the occurrence of disputes** and need for reconciliation.

o **Build Trust**: The use of distributed ledger technology creates the irrevocable and irrefutable audit trail of transactions, **enhancing regulatory reporting** capabilities and easing compliance concerns, while also **removing barriers of entry** for Financial Institutions entering **new markets**.

International Payments with World Wire

— **Clearing and settlement flow**
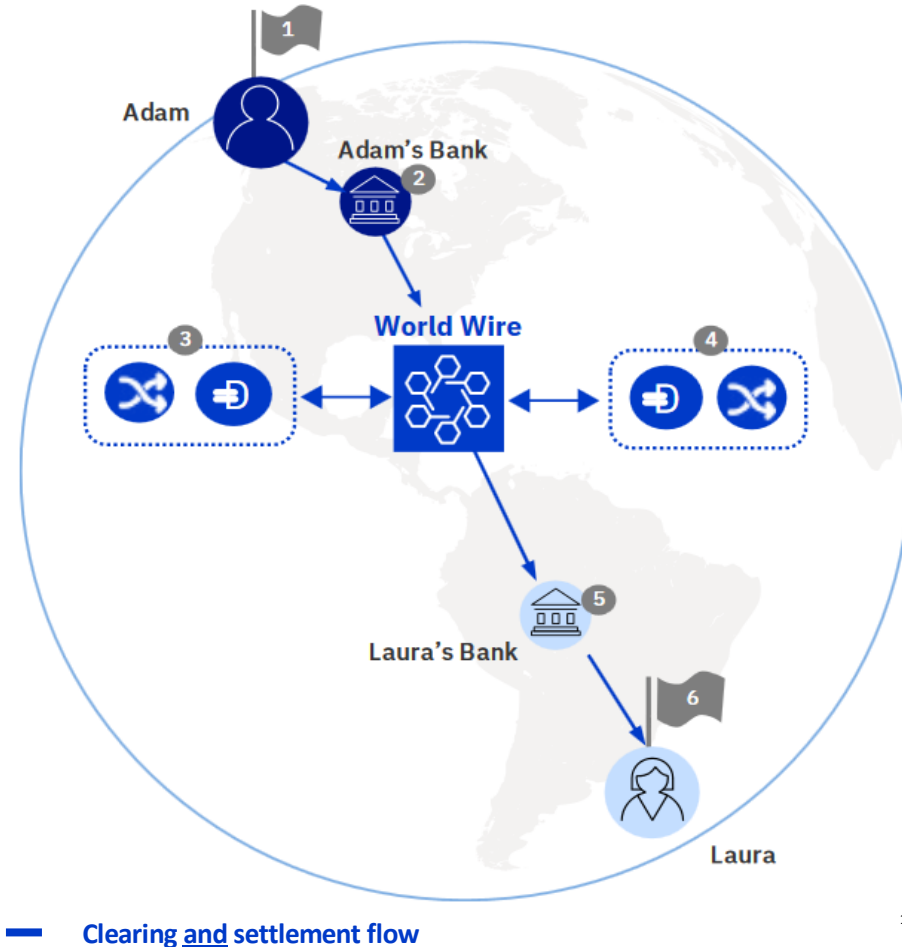
TradeLens improves global trade efficiency

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

o Shared visibility and shared state for container shipments

o Increase speed and transparency for cross border transactions through real time access to container events.

o Reduced cost and increased efficiency through paperless trade

IBM Blockchain
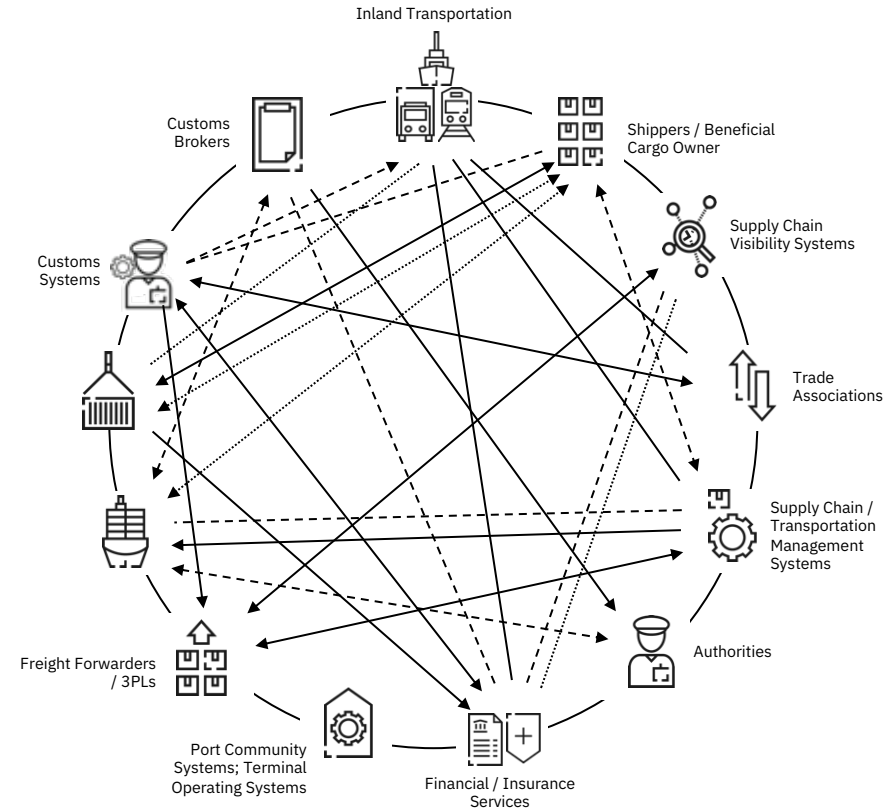
Decentralized trusted identity

Personally manage your digital IDs online with the Sovrin Network – an open source project creating a global public utility for self-sovereign identity

o Pushes identifies to the edge of the network frictionless, secure identity verification of self-sovereign identity. It's time to evolve the current system of siloed identities, endless passwords, and insecure databases.

o The Sovrin Network is the new standard for digital identity – designed to bring the trust, personal control, and ease-of-use of analog IDs – like driver's licenses and ID cards – to the Internet.

o Cryptographic, point to point exchange of identity - Every person, organization, and thing has a digital wallet to control the flow of their identity

o Based on Hyperledger Indy technology

CURRENT MODEL OF IDENTITY   SELF-SOVEREIGN IDENTITY
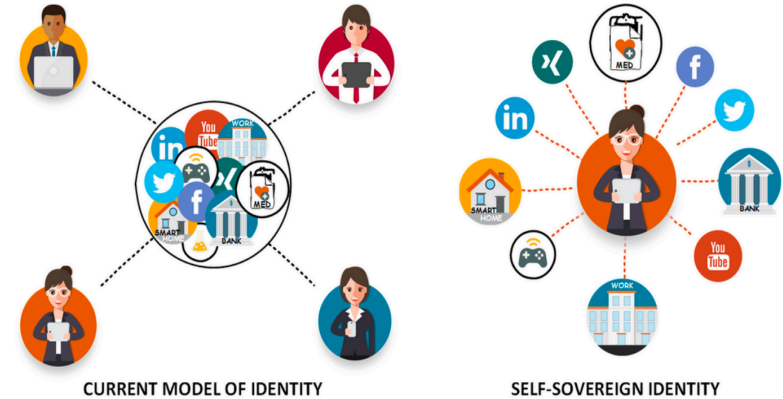
sovrin
identity for all

HYPERLEDGER
INDY

Further examples by (selected) industry

Financial	Public Sector	Retail	Insurance	Manufacturing
• Trade Finance • Cross currency payments • Mortgages • Letters of Credit	• Asset Registration • Citizen Identity • Medical records • Medicine supply chain	• Supply chain • **Loyalty programs** • Information sharing (supplier – retailer)	• Claims processing • Risk provenance • Asset usage history • Claims file	• Supply chain • Product parts • Maintenance tracking

IBM **Blockchain**

How IBM Can Help

How **IBM can help**
The certainty to solve business challenges together

Security at Scale

Enterprise-grade security and control on a platform where businesses and industries are reinventing themselves

Trusted Expertise

Reinventing business processes through unrivaled industry and technical knowledge as you start, accelerate and innovate your blockchain network.

Network Convening Power

Bringing together an expansive partner network of innovators, regulators and suppliers to establish, join or run your blockchain network.

IBM Blockchain

IBM®

IBM's end-to-end **Blockchain Strategy**
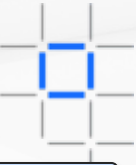
Services

Collaborate with services teams from ideation all the way to production

Ecosystem
Tap into our diverse ecosystem to develop strategic partnerships and create your competitive advantage

Solutions
Solve critical industry challenges by building and joining new business networks and applications

IBM Blockchain Platform
Build, operate and grow blockchain networks in heterogeneous environments

HYPERLEDGER
A founding, premier member of Hyperledger, IBM is committed to open source, standards & governance

IBM Blockchain

IBM **Blockchain Platform**

Advanced tooling allows you to quickly build, operate and grow blockchain networks

Build	Operate	Grow

Open technology uses the popular Hyperledger Fabric distributed ledger

HYPERLEDGER
FABRIC

Deploy anywhere fully managed, or flexible deployment on-premises or on other cloud vendors
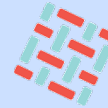
IBM Cloud   On-Premises   Other clouds

Hyperledger: A **Linux Foundation** project
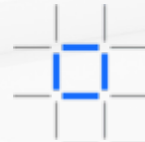
- IBM Blockchain Platform is underpinned by technology from the Hyperledger project

- Hyperledger is a collaborative effort created to advance cross-industry blockchain technologies for business

- Founded February 2016; now more than **280 member organizations**

- Open source
  Open standards
  Open governance model

Source: https://www.hyperledger.org/members
Updated: 11 September 2019

Premier

Associate

General

General

Academia Associate

IBM Blockchain

Distributed ledger
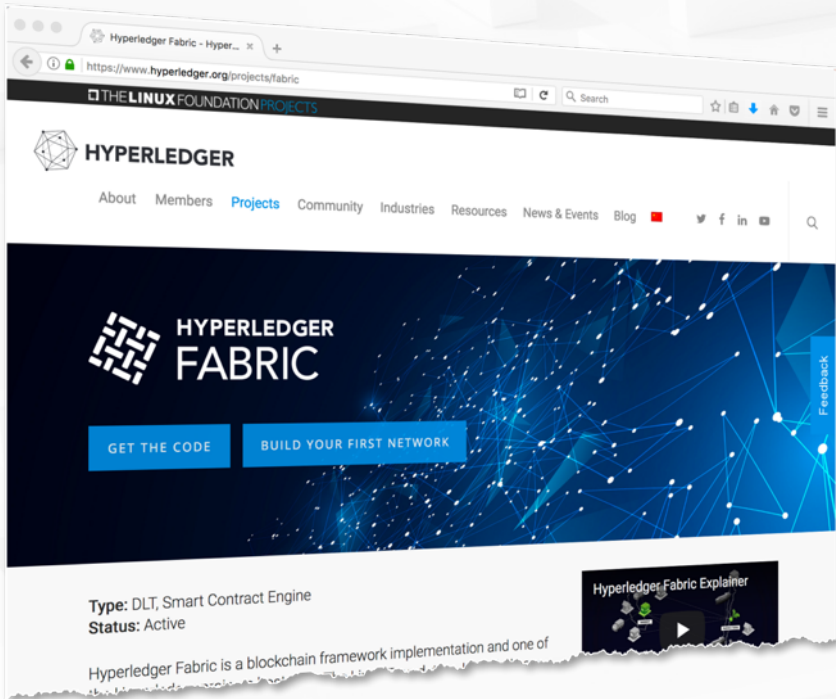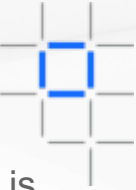
- An implementation of blockchain technology that is a foundation for developing blockchain applications

- Emphasis on ledger, smart contracts, consensus, confidentiality, resiliency and scalability.

- V1.4.6 released in February 2020
  - V1.4.x Long Term Service release with emphasis on production operational and serviceability enhancements; new programming model abstractions for ease of development
  - V2.0 is out now

- IBM is one of the many contributing organizations

IBM Blockchain

Why IBM Z

IBM Blockchain Platform benefits from Z Security

Workload Isolation	Enables isolation of network components on one system from each other and from other processes
Integrated Crypto Hardware	Every transaction requires signatures and verification which involves crypto (make sure this is done right)
Key Encryption & Management	Protect your keys -> your keys are your identity (estimated 1.1 $billion worth of cryptocurrency stolen in 1st half of 2018)
Data Encryption	Blockchain has potentially sensitive data -> protect with encryption
Network Encryption	Protect data transmitted between application, blockchain components, and integrated systems
Time Source Security	Blockchain timestamps crucial to keeping accurate ledger
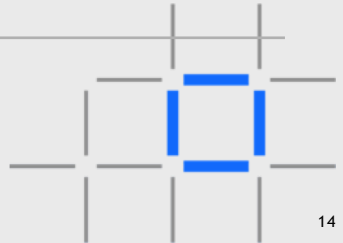
IBM Hyper Protect Virtual Servers

(On Premises)

Protect critical Linux workloads during build, deployment, and management on-premise

The Solution

Trusted CICD

Image »» Protected Image

Create
Cloud-Ready applications

Protect
against internal and external threats

Manage applications with cloud services

You're Protected Against

Remote Attack → restricted SSH access

Privilege Escalation → peer isolation between virtual servers

Insider Attack → Access to physical hardware does not mean data is compromised

Image Tampering/Malware → Only signed images are deployed via Secure Build

LinuxONE

IBM Hyper Protect Virtual Servers
(On Premises)

Client Value

- **Image Integrity**
  - Developers can securely build own images and enhance them via Trusted CI/CD flow

- **Control over Privileges**
  - Infrastructure providers can manage images via RESTful APIs
  - No provider access to sensitive data, memory, decryption keys, secrets or application logs

- **Image Provenance**
  - Validate that images originate from trusted source, no backdoor has been introduced in image builds
  - Enable auditors to approve deployment of images

IBM Blockchain Platform benefits from Co-location on IBM Z with core transaction systems

Integration with transaction systems
Integrate Blockchain apps with legacy systems that contain connected information such as PII

Performant communication
Important for blockchain to reduce latency between network components to increase tx/s and to reduce wait time when connecting to legacy systems for information
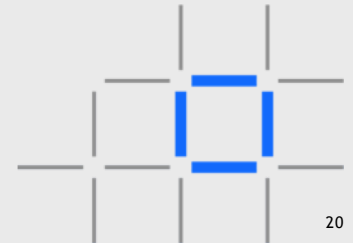
Scalability
'Data center-in-a-box'
Grow your blockchain network to suit your needs (CPU, Memory, Network)

Operational efficiency
Manage your system efficiently and securely

IBM Blockchain Platform benefits from IBM Z RAS

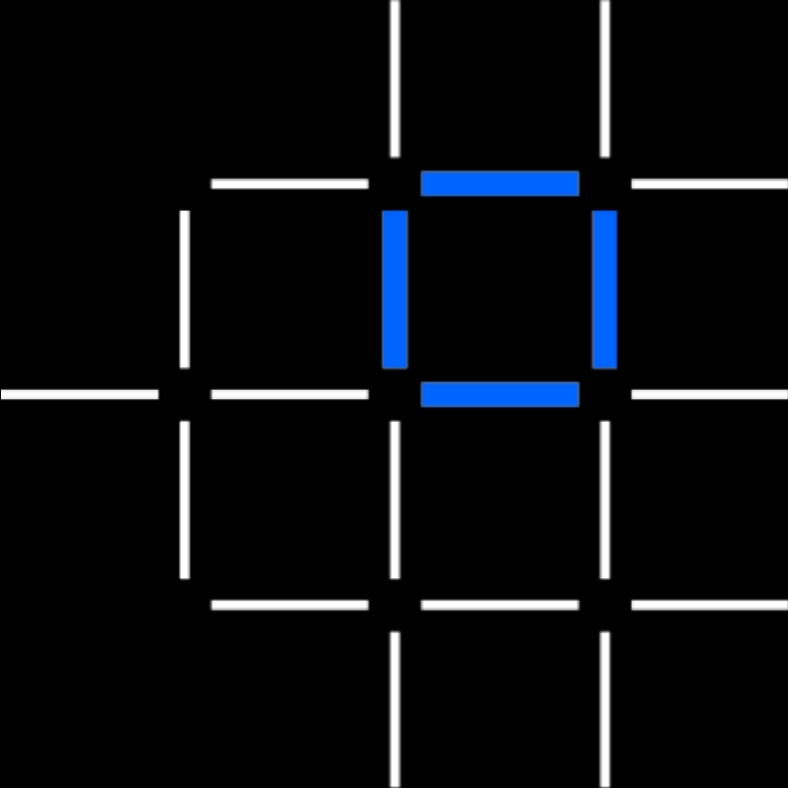|	
Extensive self-checking and self-recovery capabilities	Keep your blockchain up and running
Concurrent replace, repair, and upgrade	Make upgrades as needed
Redundant array of independent memory (RAIM) technology	You use blockchain to come to a consensus on which data should be on the ledger, make sure all this work is preserved by protecting data in case of emergency
Near-continuous availability and disaster recovery solutions	Make your blockchain network available to all participants all the time
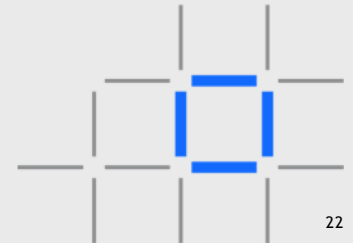
Thank you

Austin Grice
austin.grice@ibm.com

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

🐦 @IBMBlockchain

f IBM Blockchain

▶ IBM Blockchain

IBM **Blockchain**

IBM