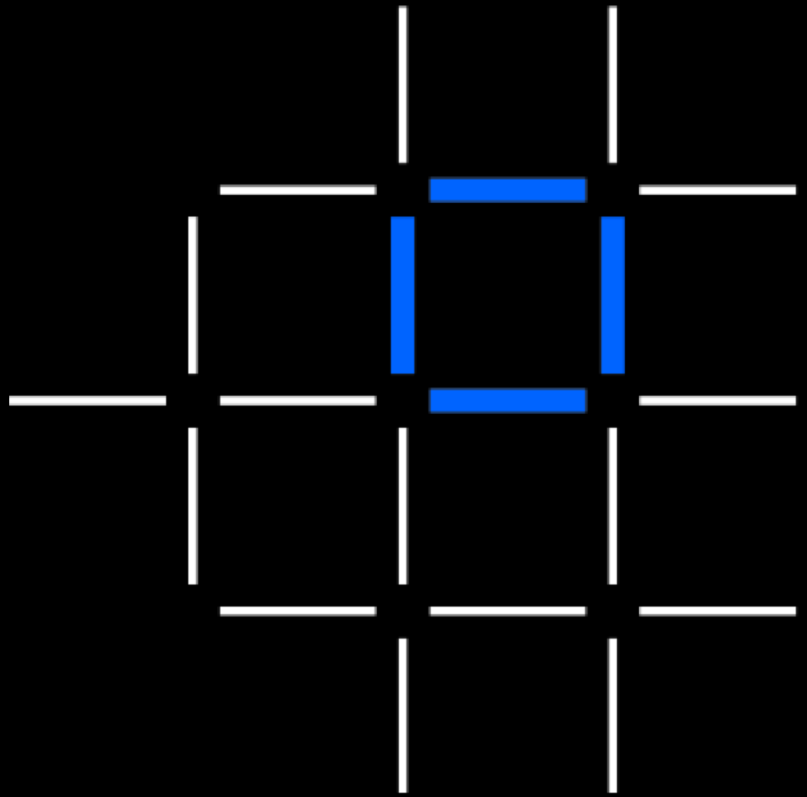
Blockchain Explained

Separating Hype from Reality



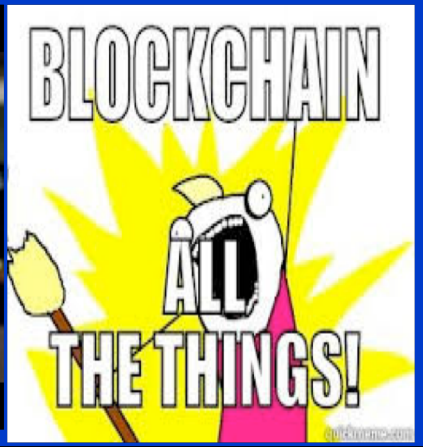
Dave Wakeman
Blockchain Evangelist, IBM
@dwakeman
linkedin.com/in/davewakeman/
https://ibm.biz/bc-stuff

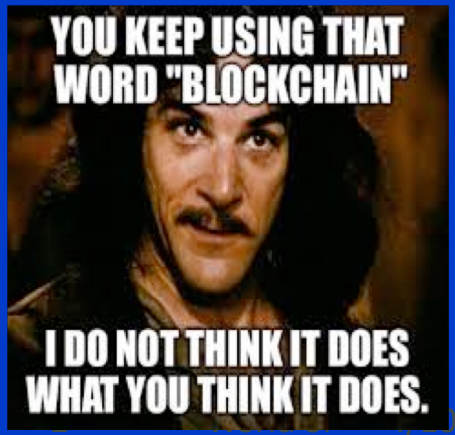
V5.15, 8 January 2019

IBM **Blockchain**

IBM

About the hype…experience and discipline required





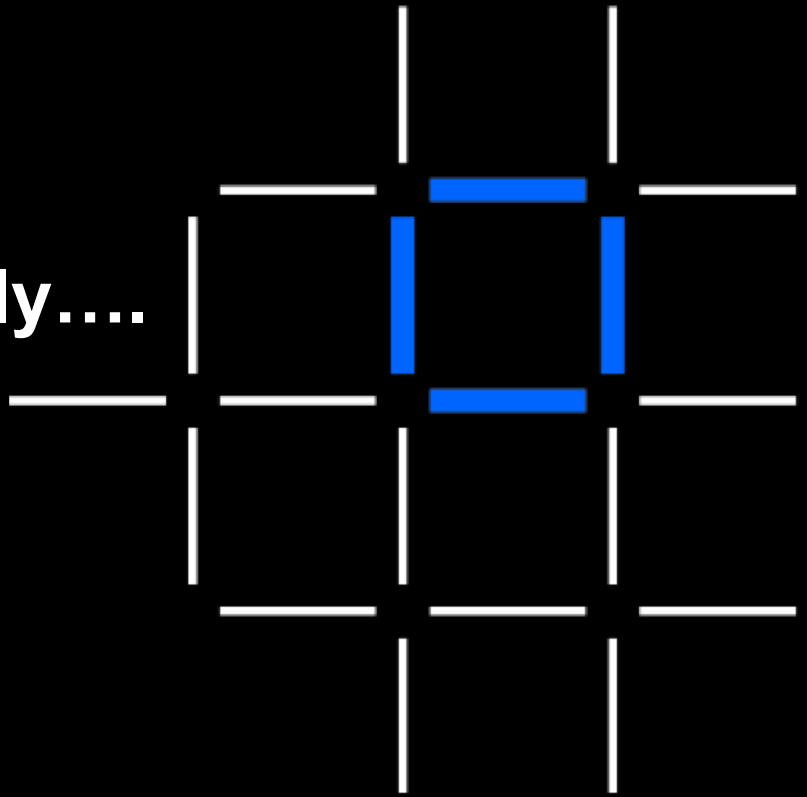
Back to the Future….

What is the ”Internet”, anyway…?

1994: Today Show

“Blockchain will be a more disruptive force on the world than the internet”

So what is Blockchain Exactly….




BITCOIN • DIGITAL • DECENTRALIZED • PEER TO PEER
PRECIOUS METALS

Permissioned vs. Non-Permissioned and Public vs. Private Blockchains

Permissioned

- Identity
- Restricted access
  - Create/execute smart contracts
  - Participate in consensus
- Higher transaction throughput ✹
- No mining / low energy consumption

Private: an invitation is required to join

Non-Permissioned/Permissionless

- Anonymity
- Unrestricted
- Lower transaction throughput ✹
- Mining / high energy consumption

Public: anyone can participate

https://www.forbes.com/sites/laurashin/2016/12/20/hackers-have-stolen-millions-of-dollars-in-bitcoin-using-only-phone-numbers/#2c4291a038ba

Forbes

Digital Money / #AllThingsMobile

Hackers Have Stolen Millions Of Dollars In Bitcoin -- Using Only Phone Numbers

https://www.theguardian.com/technology/2018/mar/20/child-abuse-imagery-bitcoin-blockchain-illegal-content

Bitcoin

Child abuse imagery found within bitcoin's blockchain

Researchers discover illegal content within the distributed ledger, making possession of it potentially unlawful in many countries

	Permissioned	Non-Permissioned
Public	Academic degrees, Land titles	Bitcoin, Ethereum, etc.
Private	Medical records	Polls, Voting

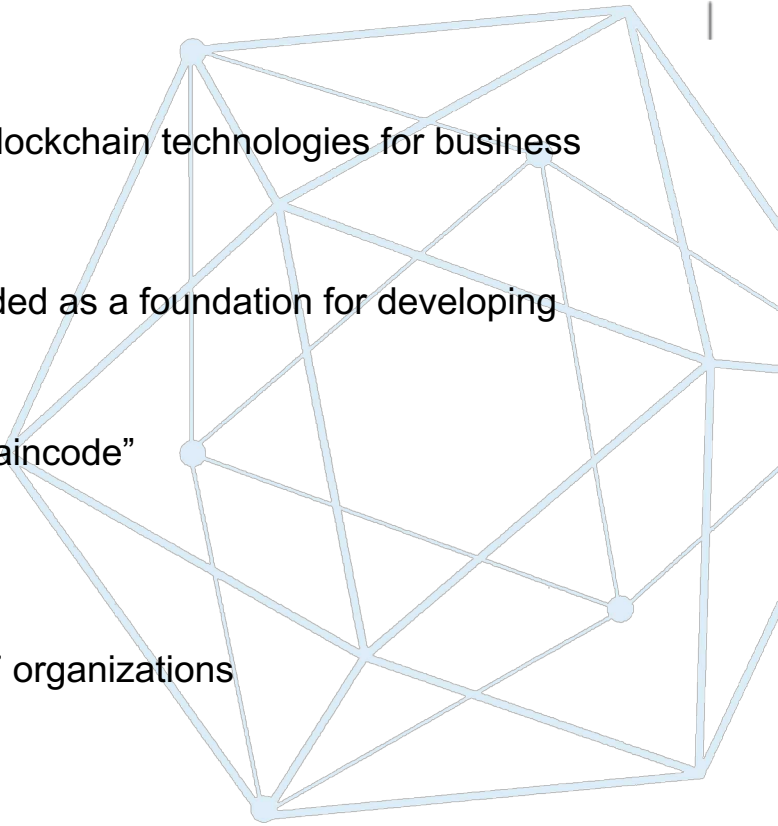
For its use in government and large scale industry applications, a *Permissioned* Blockchain is needed

✹ There is on-going work to speed up consensus protocols.

Behind the Architecture of Hyperledger Fabric

Hyperledger Fabric deployed in a single cloud data center achieves an end-to-end throughput of more than 3,500 transactions per second with latency less than one second.

What is Hyperledger Fabric



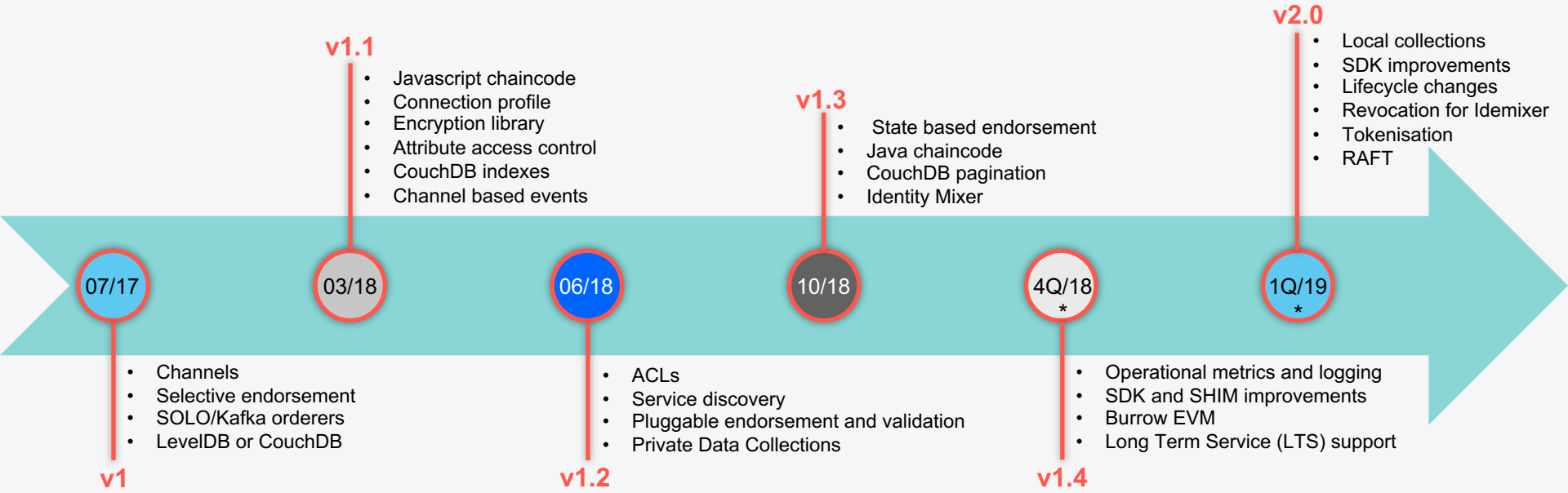
- Linux Foundation Hyperledger
  - A collaborative effort created to advance cross-industry blockchain technologies for business

- Hyperledger Fabric
  - An implementation of blockchain technology that is intended as a foundation for developing blockchain applications
  - Key technical features:
  - A shared ledger and smart contracts implemented as “chaincode”
  - Privacy and permissioning through membership services
  - Modular architecture and flexible hosting options

- V1.0 released July 2017: contributions by 159 engineers from 27 organizations
  - IBM is one of the contributors to Hyperledger Fabric

HYPERLEDGER FABRIC

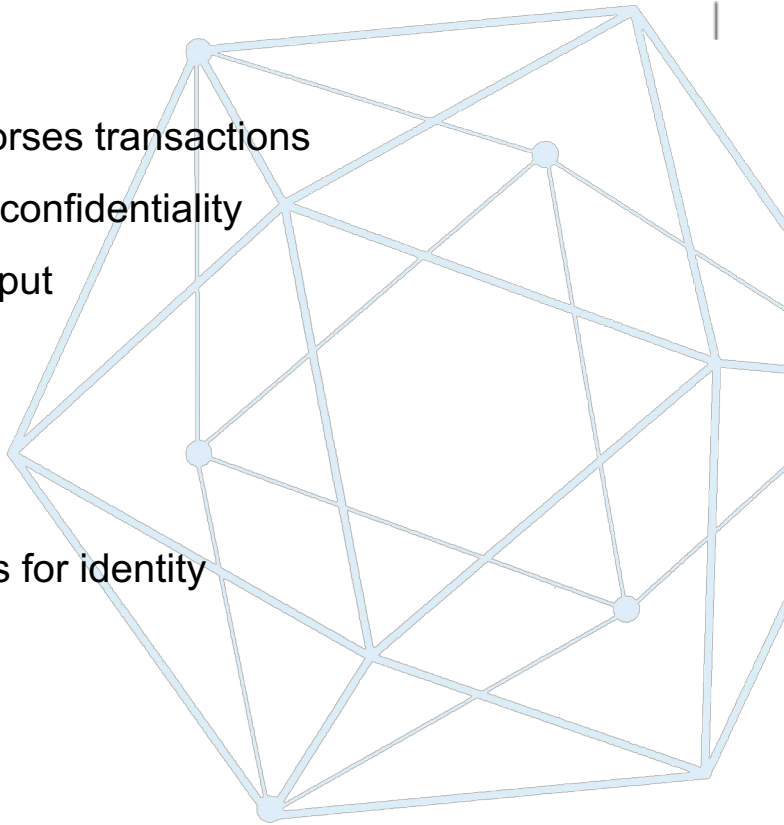
Roadmap



HYPERLEDGER
BLOCKCHAIN TECHNOLOGIES FOR BUSINESS

Based on https://wiki.hyperledger.org/projects/fabric/roadmap - Dates determined by the Hyperledger community - (*) Subject to change

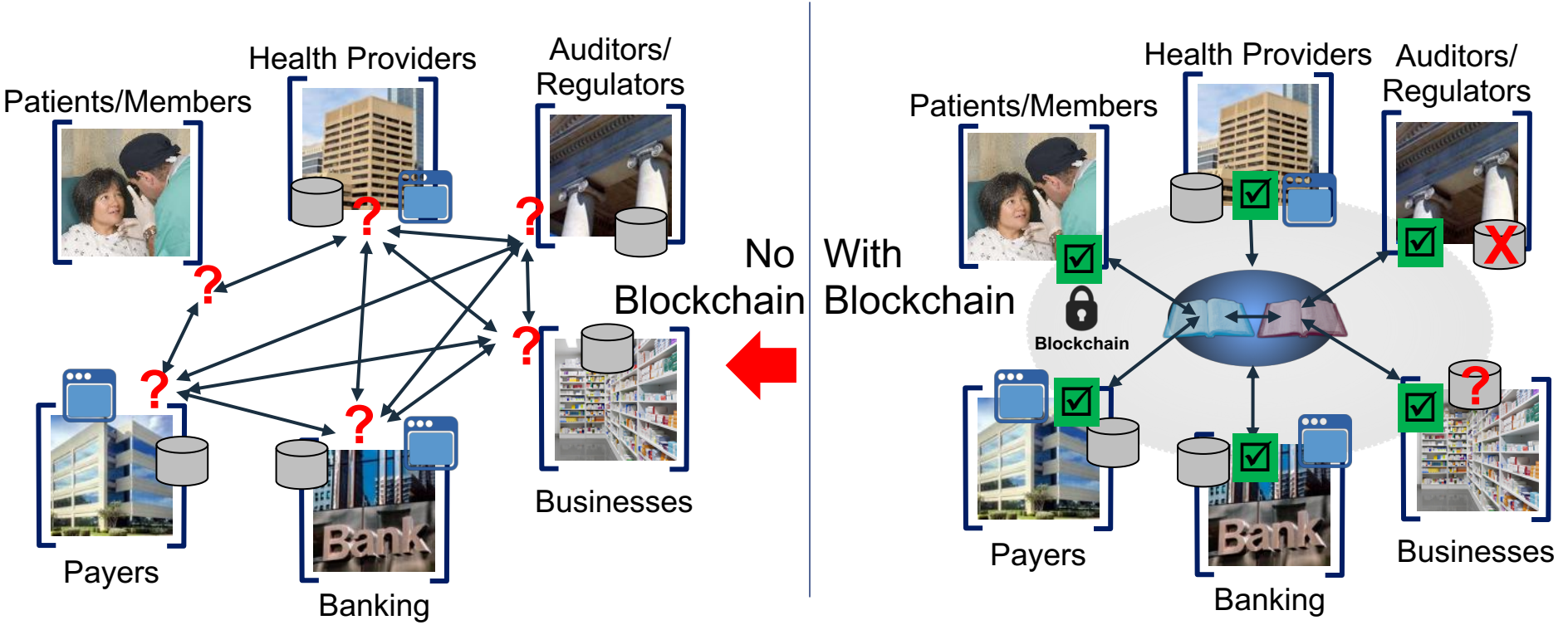
Overview of Hyperledger Fabric v1 – Design Goals



- Better reflect business processes by specifying who endorses transactions
- Support broader regulatory requirements for privacy and confidentiality
- Scale the number of participants and transaction throughput
- Eliminate non deterministic transactions
- Support rich data queries of the ledger
- Dynamically upgrade the network and chaincode
- Support for multiple credential and cryptographic services for identity
- Support for ”bring your own identity”

Blockchain solves fragmentation by providing a shared, replicated ledger …

App
Data



… with consensus, provenance, immutability and finality

Key Elements of **Blockchain**.

Shared Ledger

Append-only distributed system of record shared across business network

Smart Contract

Business terms embedded in transaction database & executed with transactions

Privacy

Ensuring appropriate visibility, transactions are secure, authenticated and verifiable

Consensus

All parties agree to network verified transaction

- Blockchain establishes a shared, secure record of information flows; a ‘shared version of events’ across networks for supply chain transactions, processes and partners.
- **Blockchain** will be used to provide a synthesized record of information flows. This level of shared visibility will offer organizations an opportunity to optimize multi-party processes across their business ecosystems.

Blockchain: A distributed, shared, ledger.

Saves Time

Transaction time from days to near instantaneous

Removes Cost

Overheads and cost intermediaries

Reduces Risk

Tampering, fraud & cyber crime

Increases Trust

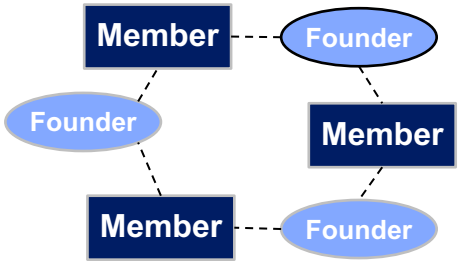
Through shared processes and recordkeeping

- **Blockchain** holds records of digital transactions in such a way that makes them **accessible and visible to multiple participants** in a network, while keeping them **secure**.

- The digital shared ledger is updated and validated with each transaction, resulting in a secure, permanently recorded exchange.
- The result? Faster, permissioned, and auditable B2B interactions between parties such as passengers, buyers, sellers and logistics providers

Building Communities in Blockchain Networks

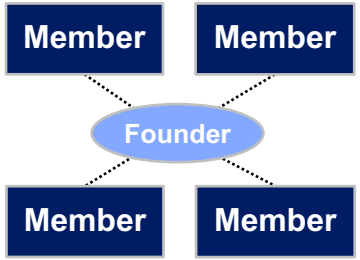
Consortium Based Network



Founders are equal among other participants, may include a joint legal entity among the founders (e.g. – JV)

Examples: JPX, we.trade

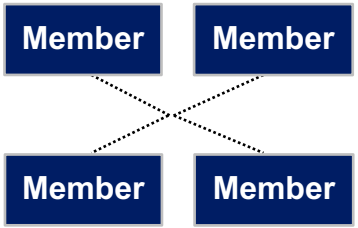
Founder Directed Network



Individual founder in a position to provide strong direction

Examples: Northern Trust, CLS Fundamental to FX

Community Based Network

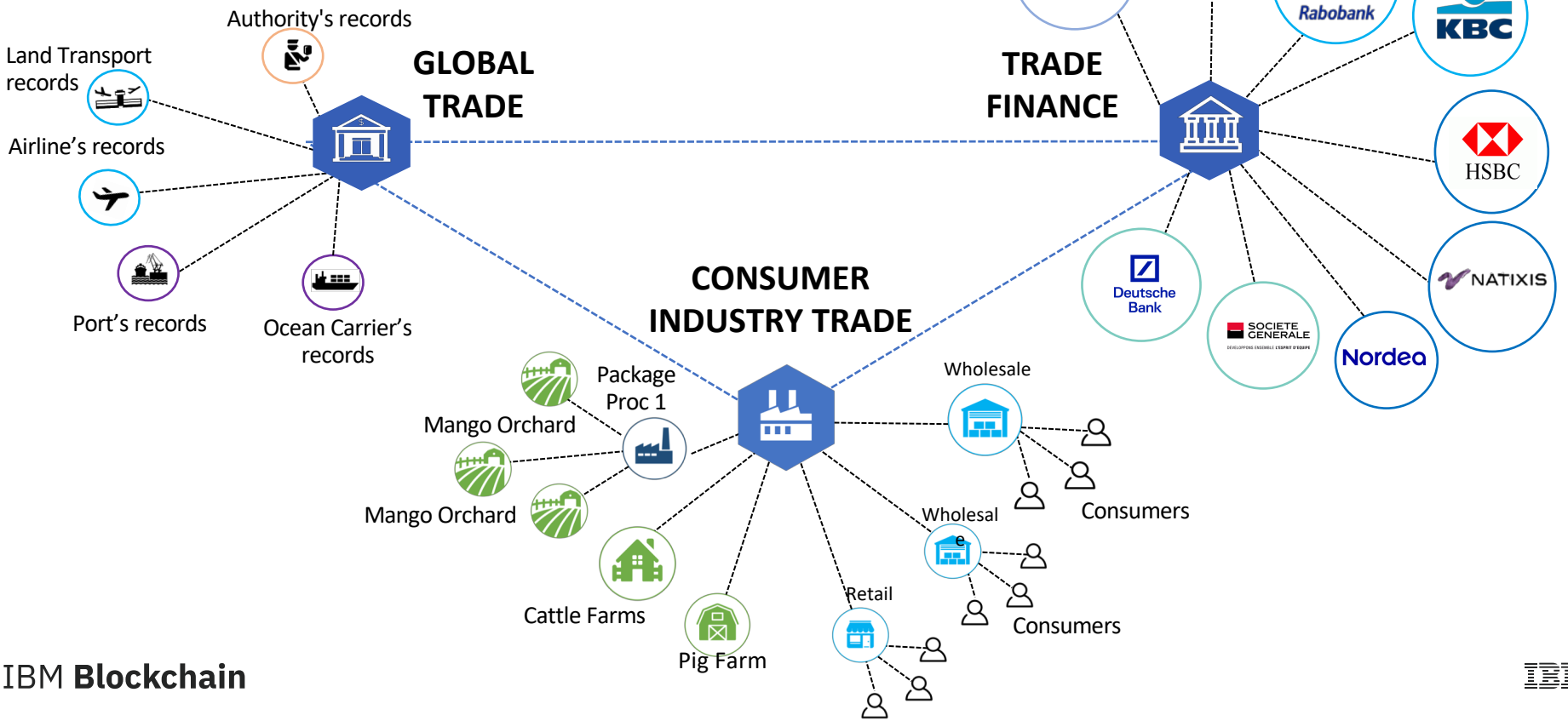


Driven by industry standards bodies or existing non-blockchain network owners

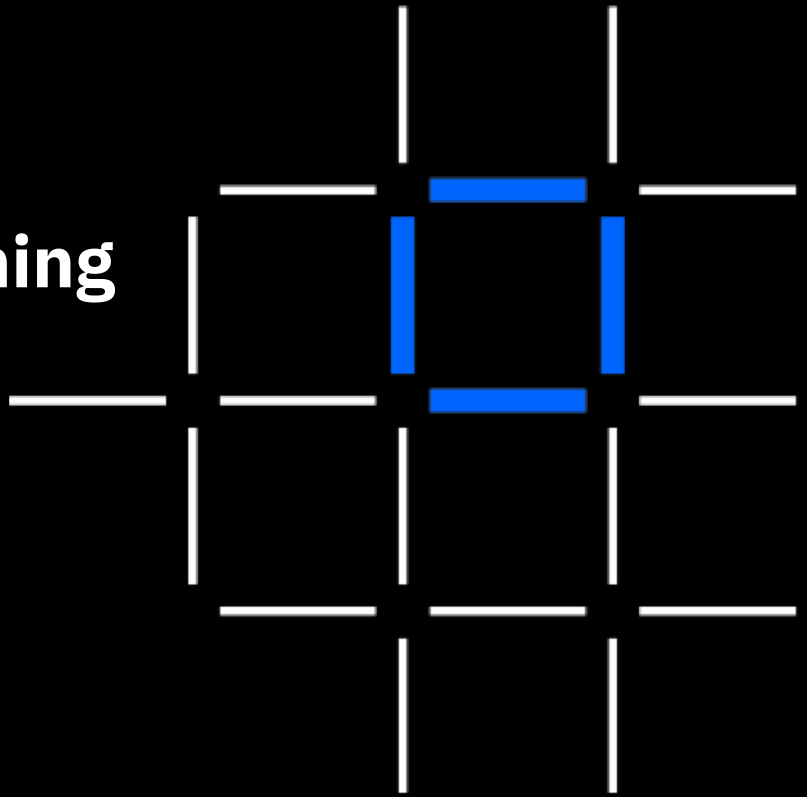
Examples: IBM Watson Supply Chain, SWIFT

A Network of Networks

… *New Channels, Trust, Transparency*



Real Blockchain Work Happening Today in Supply Chain.....



Supply Chain Use Cases

Supply Chain Workflow

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

Supply Chain Visibility

Blockchain technology provides visibility to all the participants involved in moving goods by tracking the purchase order and shipment status

Food Safety

Blockchain holds the history of food items through entire supply chain providing traceability of food from “farm to fork”

Manufacturing Provenance

Blockchain holds complete provenance details of each component part, accessible by each manufacturer in the production process

Trade Finance

Blockchain network designed to simplify and facilitate domestic and cross-border trade while helping to increase overall trade transaction transparency

Supply Chain Financing

Blockchain solution creates a consolidated and detailed view of transactions visible to all parties resulting in a reduction in # disputes, dispute cycle time, and improvement in productive use of working capital.

Introducing IBM Food Trust built on Blockchain technology

IBM Food Trust is a modularized solution available as a service providing traceability to improve food transparency and efficiency

Blockchain is used to create a trusted connection with shared value for all ecosystem participants, including end consumers

The solution offers connectors for interoperability and leveraging existing standards (e.g., GS1)

IBM Food Trust provides value to the entire food ecosystem

- Prove farm is not a source of outbreak
- Ease of connectivity to the supply chain

Growers

- Instill trust between retails, suppliers & customers
- Automate & reduce manual certificate management

Food Manufacturers/CPGs

- Conduct targeted recalls
- Enable internal data sharing

Wholesalers/ Distributors

- Enhance ability to meet compliance standards
- Reduce manual processes

Food Logistics

- Assure customers food supplied is safe
- Conduct targeted recalls quickly

Food Retailers

- Learn about recalls and increased transparency
- Reduce risk of being victimized by food fraud

Consumers

- Reduce fraudulent certificates
- Increase renewal speed

Certification Bodies

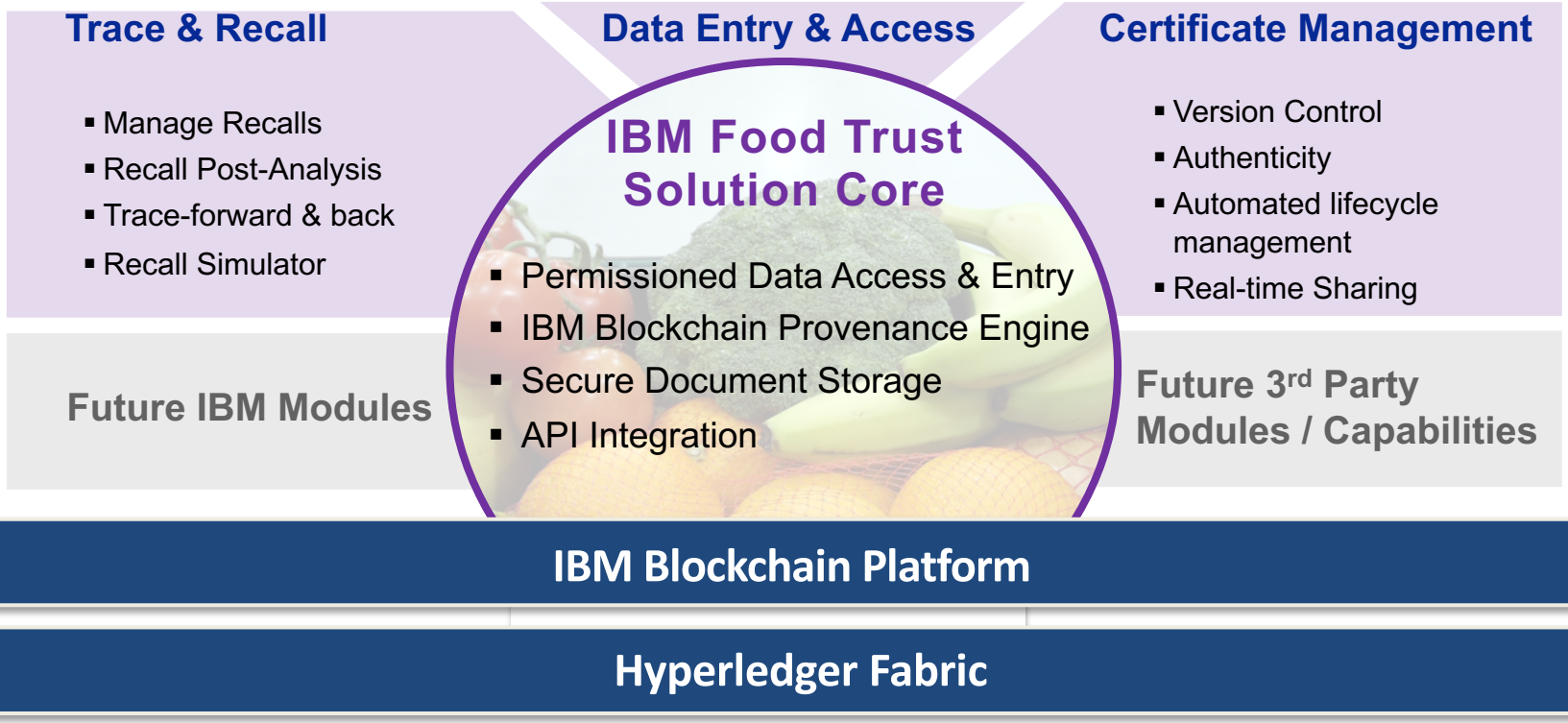
- Assure customers food supplied Is safe
- Reduce wasted food

Food Service

- Identify contamination quickly
- Reduce unnecessary testing

Regulators

IBM Food Trust solution



TRADE LENS

MAERSK

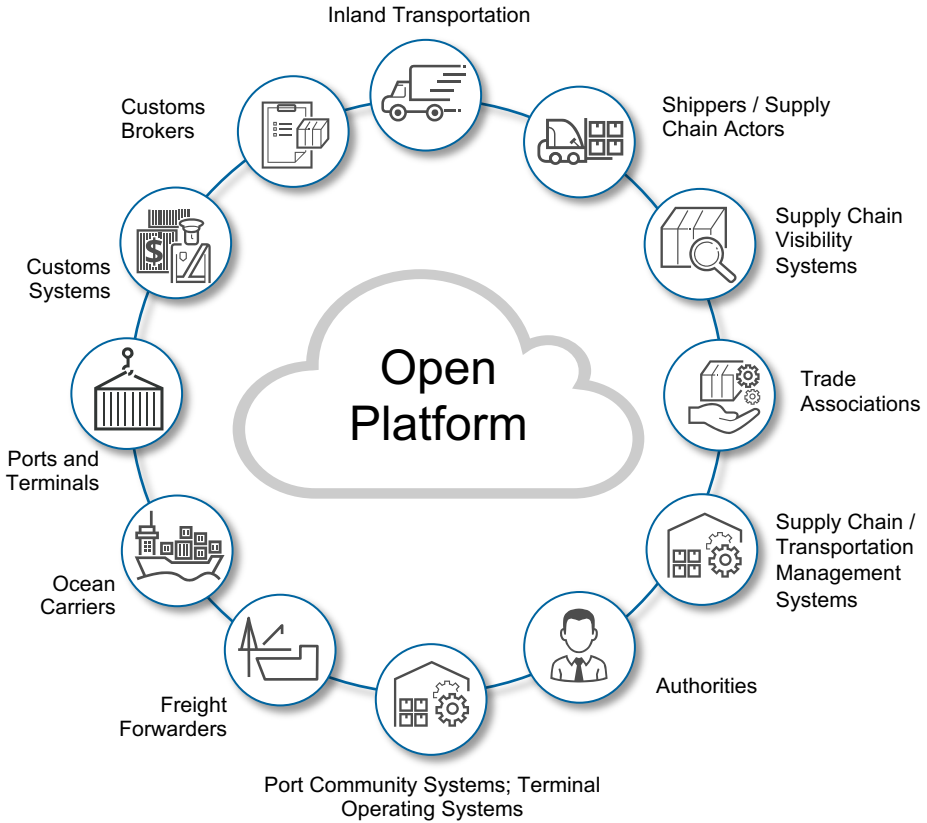
Improving in-transit inventory management

Real-time tracking shipment of goods across multiple global supply chain checkpoints

Digitizing the end-to-end supply chain process to increase transparency and security among all trading partners, reduce fraud and errors, decrease product time spent in the transit, and lower waste and cost.

Tomorrow: Reducing global trade barriers and increasing efficiency across international supply chains

- Transparent, near-instant access to end-to-end supply chain data
- Assurance of the immutability of digital documents
- Trusted cross-organizational workflows
- Better risk assessments
- Fewer unnecessary interventions
- Far lower administrative expenses



The establishment of the joint venture remain subject to receipt of regulatory approvals. None of the information provided in this document should be construed in any way as a representation or undertaking with regard to the position to be adopted by Maersk or IBM.

The Plastic Bank

Tackling ocean plastic and global poverty with blockchain-based token rewards

As scientists predict more plastic than fish in the ocean by 2050, what can we do to protect the natural world? Working with IBM and service provider Cognition Foundry, The Plastic Bank is mobilizing recycling entrepreneurs from amongst the world's poorest communities to clean up plastic waste in return for life-changing goods.

Results

Creates

secure asset-backed rewards to underpin the exchange of plastic waste for goods

Sparks

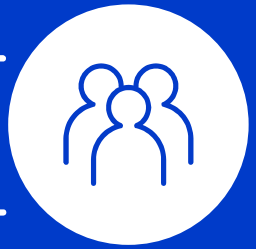
massive expansion from startup to global platform for cleaner oceans

Enables

the most disadvantaged to transcend poverty as recycling entrepreneurs

How did they do that?

Concepts and Components

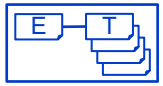


Considerations for the Developer, Operator and Architect

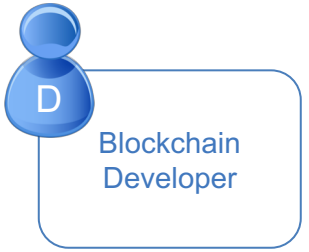
Actors in a blockchain solution

Blockchain Architect		Responsible for the architecture and design of the blockchain solution
Blockchain User		The business user, operating in a business network. This role interacts with the Blockchain using an application. They are not aware of the Blockchain.
Blockchain Regulator		The overall authority in a business network. Specifically, regulators may require broad access to the ledger's contents.
Blockchain Developer		The developer of applications and smart contracts that interact with the Blockchain and are used by Blockchain users.
Blockchain Operator		Manages and monitors the Blockchain network. Each business in the network has a Blockchain Network operator.
Membership Services		Manages the different types of certificates required to run a permissioned Blockchain.
Traditional Processing Platform		An existing computer system which may be used by the Blockchain to augment processing. This system may also need to initiate requests into the Blockchain.
Traditional Data Sources		An existing data system which may provide data to influence the behavior of smart contracts.

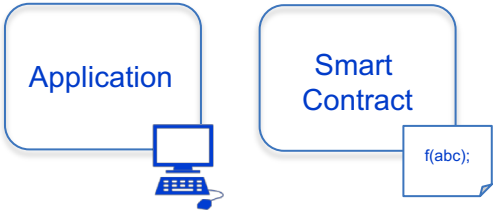
Components in a blockchain solution

Ledger		A ledger is a channel's chain and current state data which is maintained by each peer on the channel.
Smart Contract		Software running on a ledger, to encode assets and the transaction instructions (business logic) for modifying the assets.
Peer Network		A broader term overarching the entire transactional flow, which serves to generate an agreement on the order and to confirm the correctness of the set of transactions constituting a block.
Membership		Membership Services authenticates, authorizes, and manages identities on a permissioned blockchain network.
Events		Creates notifications of significant operations on the blockchain (e.g. a new block), as well as notifications related to smart contracts.
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.

The blockchain developer



Blockchain developers' primary interests are…

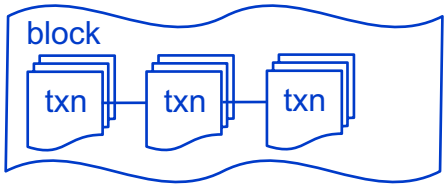


…and how they interact with the ledger and other systems of record:

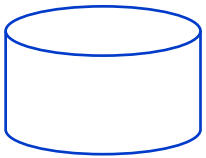
They should NOT have to care about operational concerns, such as:

X Peers Consensus Security

A ledger often consists of two data structures



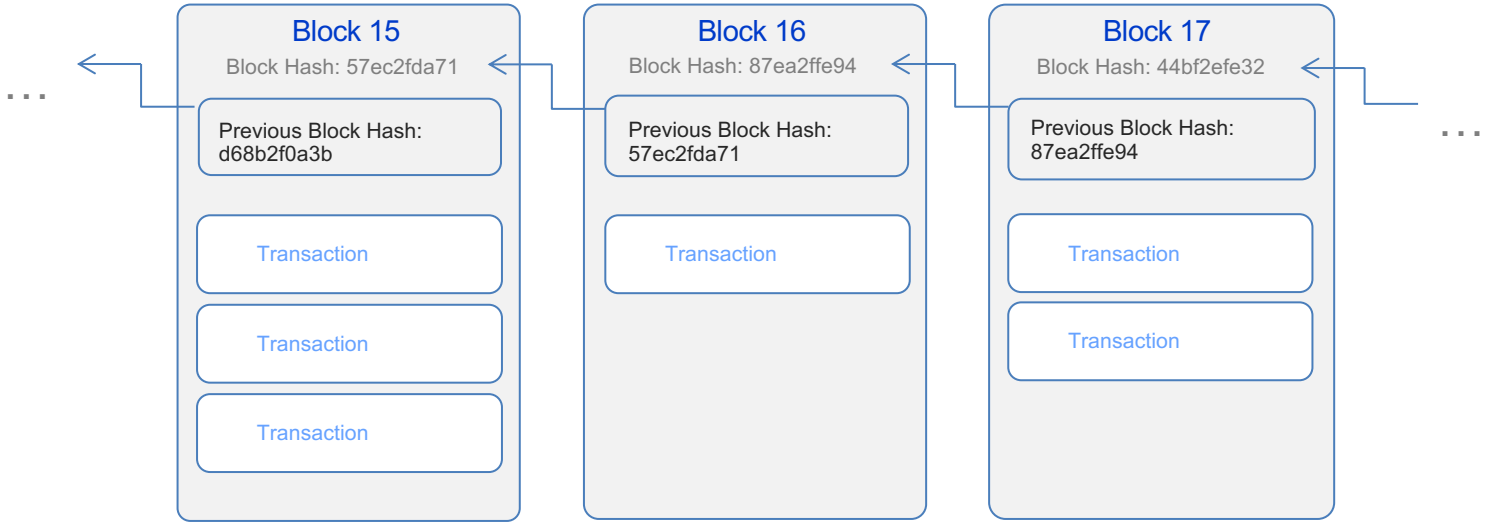
Blockchain


World state

- Blockchain
  - A linked list of blocks
  - Each block describes a set of transactions (e.g. the inputs to a smart contract invocation)
  - Immutable – blocks cannot be tampered

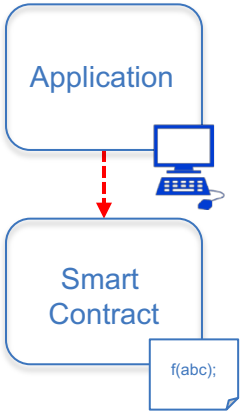
- World State
  - An ordinary database (e.g. key/value store)
  - Stores the combined outputs of all transactions
  - Not usually immutable

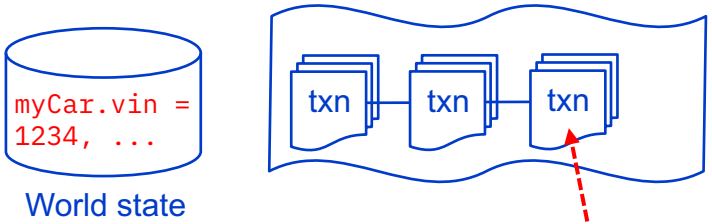
Block detail (simplified)



- 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

Working with the ledger example: a change of ownership transaction





Transaction input - sent from application

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

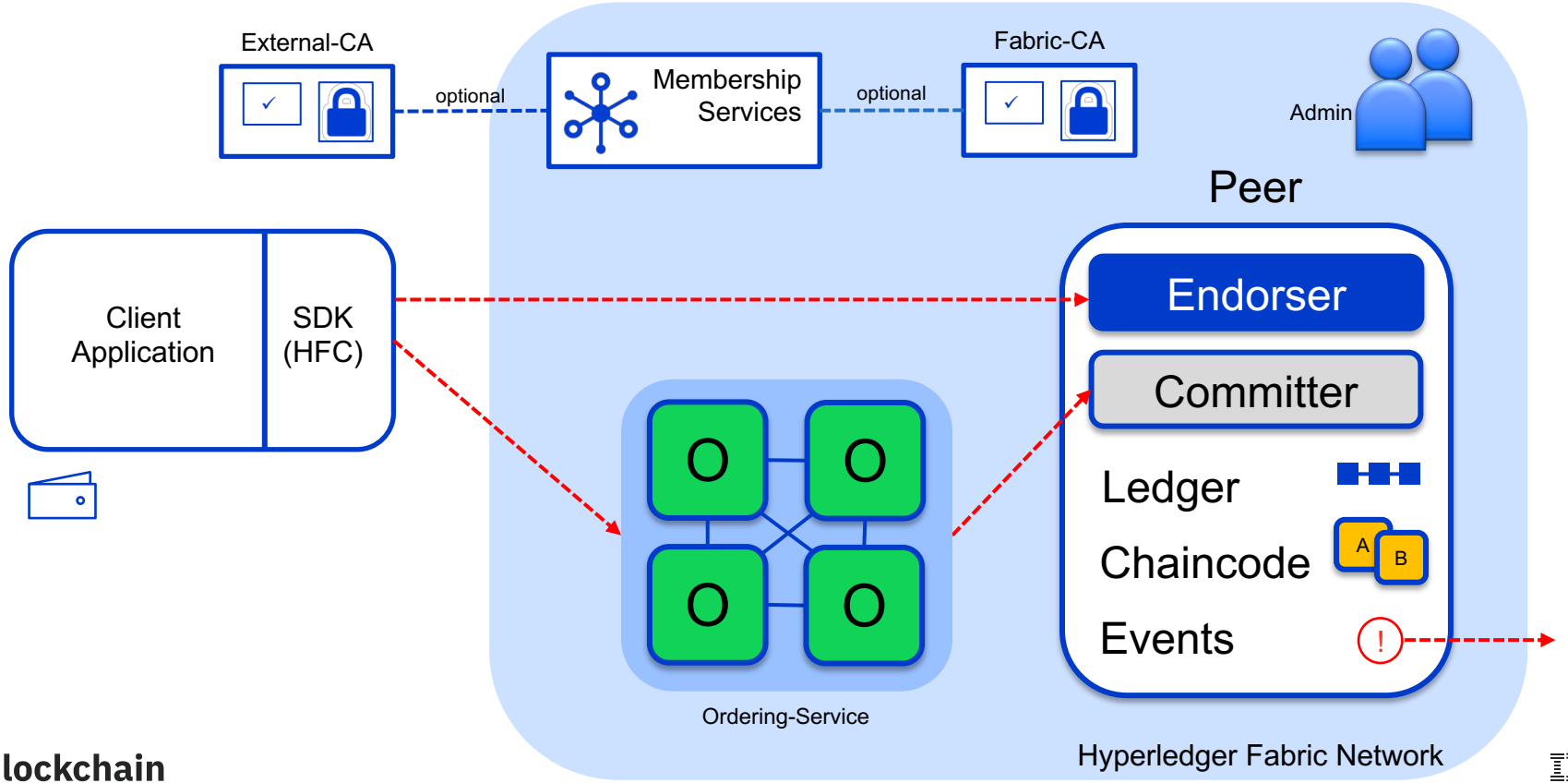
Smart contract implementation

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

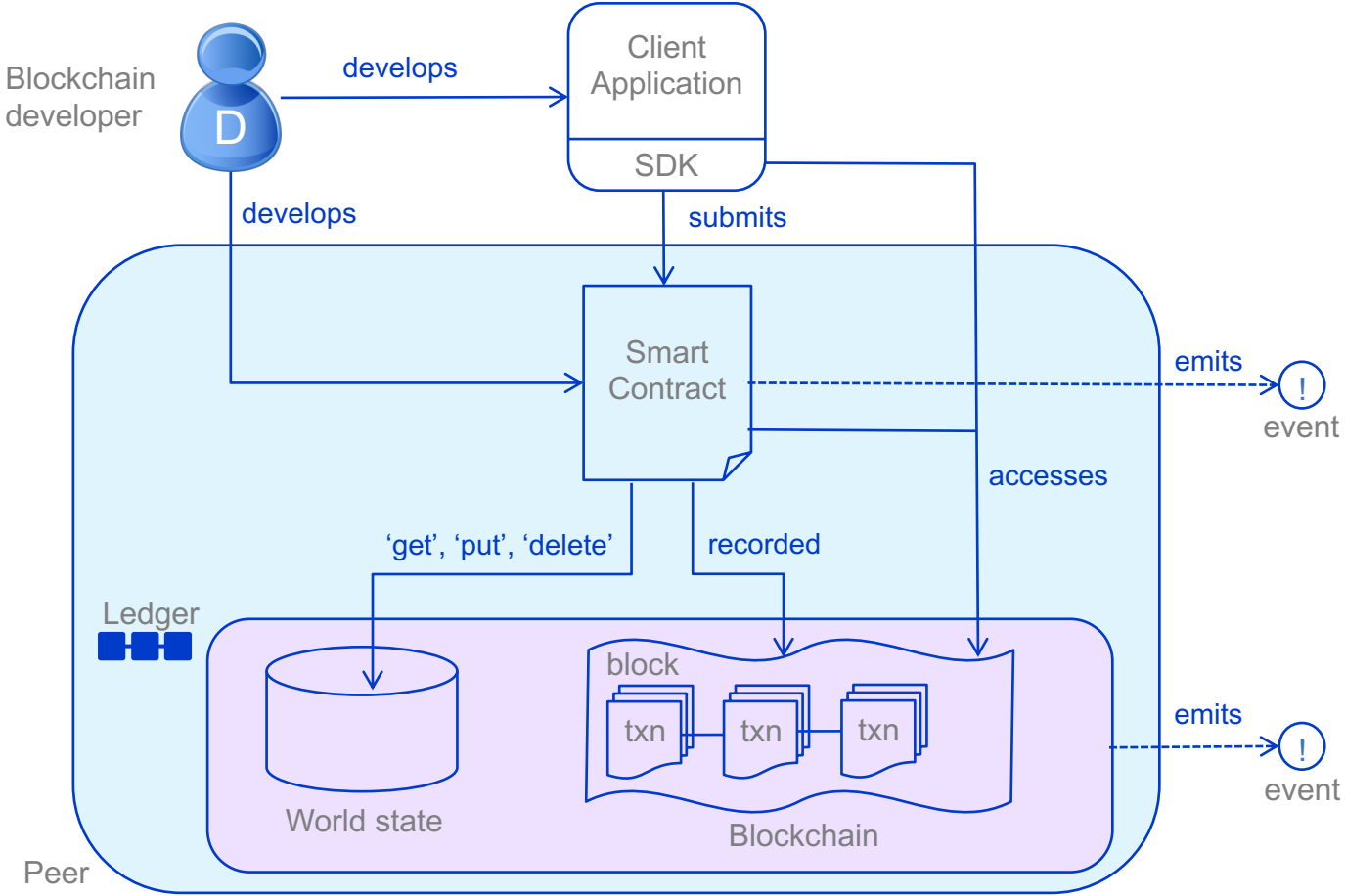
World state: new contents

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

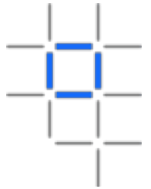
Hyperledger Fabric V1 Architecture



How applications interact with the ledger



Non-determinism in blockchain



- Blockchain is a distributed processing system
  - Smart contracts are run multiple times and in multiple places
  - As we will see, smart contracts need to run deterministically in order for consensus to work
    - Particularly when updating the world state
- It's particularly difficult to achieve determinism with off-chain processing
  - Implement services that are guaranteed to be consistent for a given transaction, or
  - Detect duplicates for a transaction in the blockchain, middleware or external system

random()

getExchangeRate()

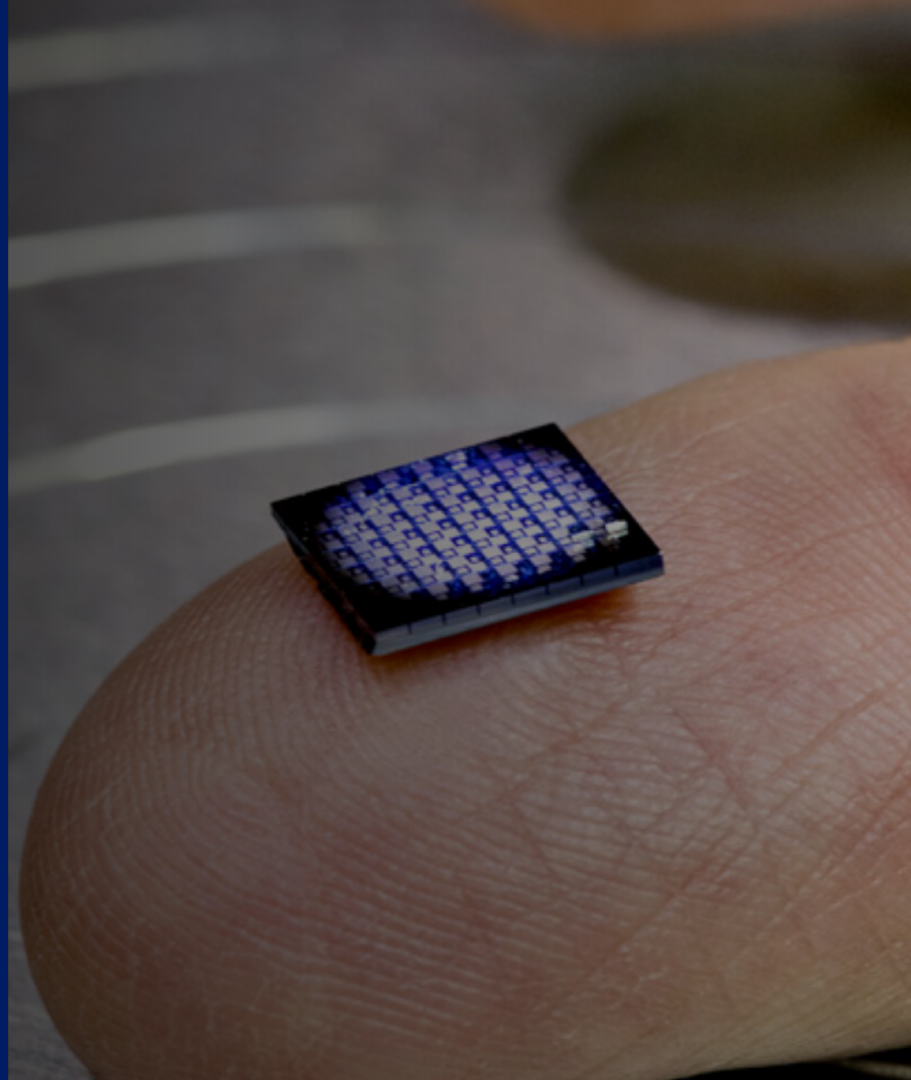
getDateTime()

getTemperature()

incrementValue inExternalSystem(…)

A glimpse of the future…

- *The world's smallest computer is an IBM-designed edge device architecture and computing platform called a Crypto Anchor that is smaller than a grain of salt will cost less than ten cents to manufacture and can monitor, analyze, communicate, and even act on data.*
- *Crypto anchors extend blockchain's value into the physical realm. Tamper-proof digital signatures will authenticate products, from medicine to diamonds and make counterfeiting nearly impossible.*



What will you do with blockchain?

Thank you

Dave Wakeman
Blockchain Technical Leader, IBM Cloud
linkedin.com/in/davewakeman
ibm.biz/cloud4developers
@dwakeman

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

@IBMBlockchain
IBM Blockchain
IBM Blockchain