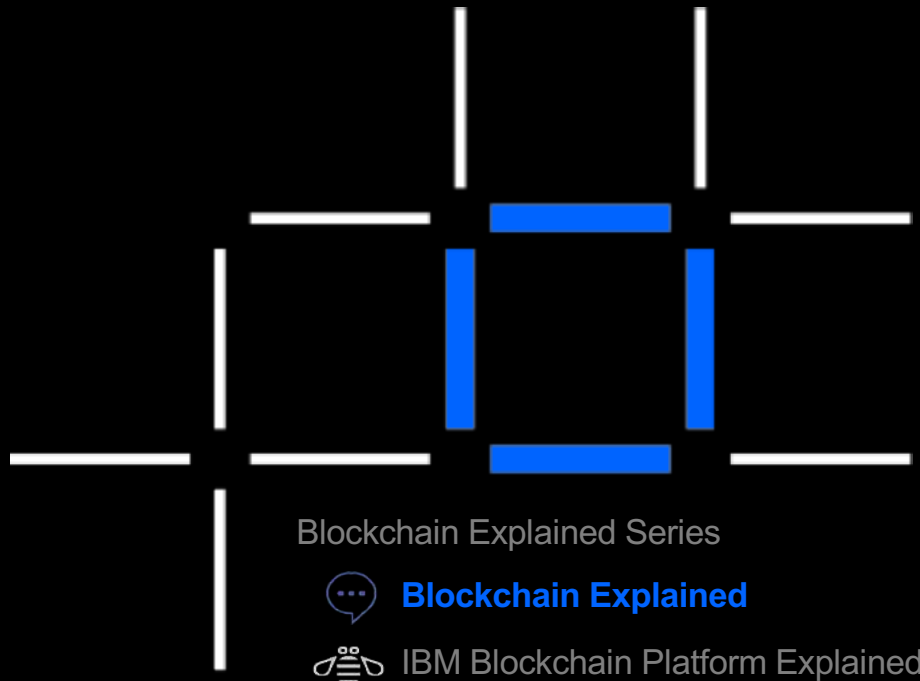
Blockchain Introduction for i-POWER

An Introduction to Blockchain for Business

International i-POWER 2020 (v), June 10

Ross Cruickshank
Developer Advocate
IBM



Blockchain Explained Series

- **Blockchain Explained**
- IBM Blockchain Platform Explained
- IBM Blockchain Usage Patterns
- Solutions Explained
- What's New
- Labs Explained

IBM **Blockchain**

IBM

Ross Cruickshank
ross@vnet.ibm.com
IBMer since 1984

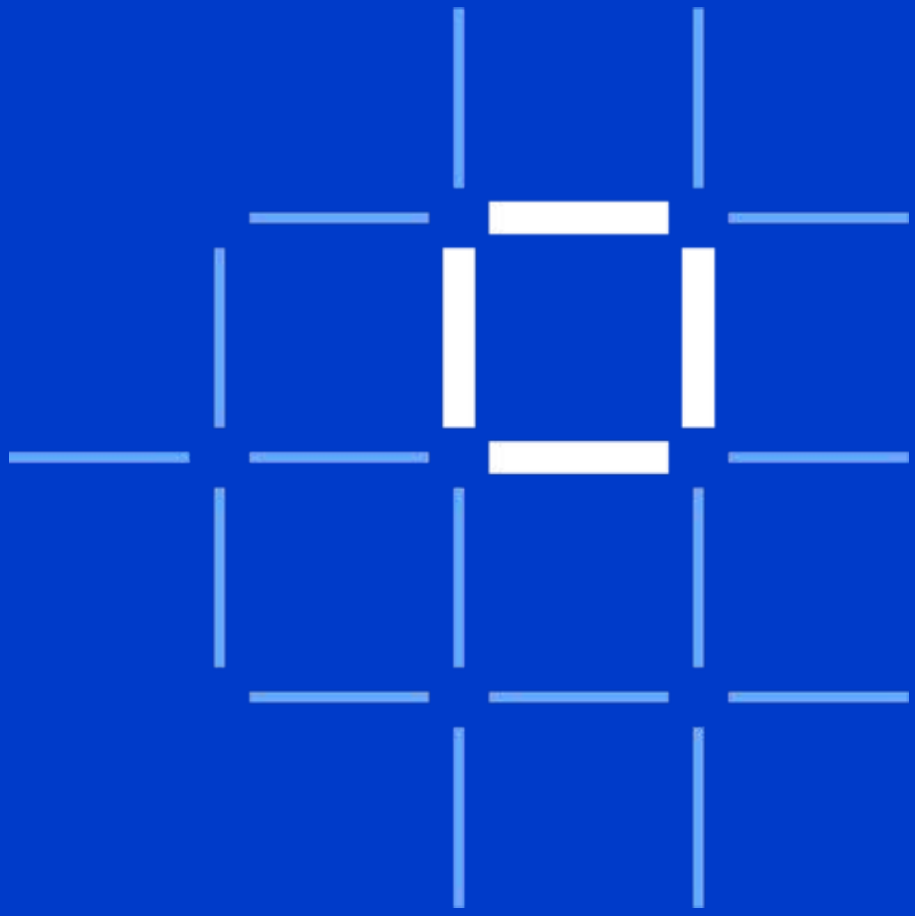
Developer Advocate
Cloud, Power, Z, pi
Open source adoption
Node-RED

Blockchain, IOT, tools,
Integration, databases

https://youtu.be/pylMqRqdg-U?t=9520

Genesis London 2018

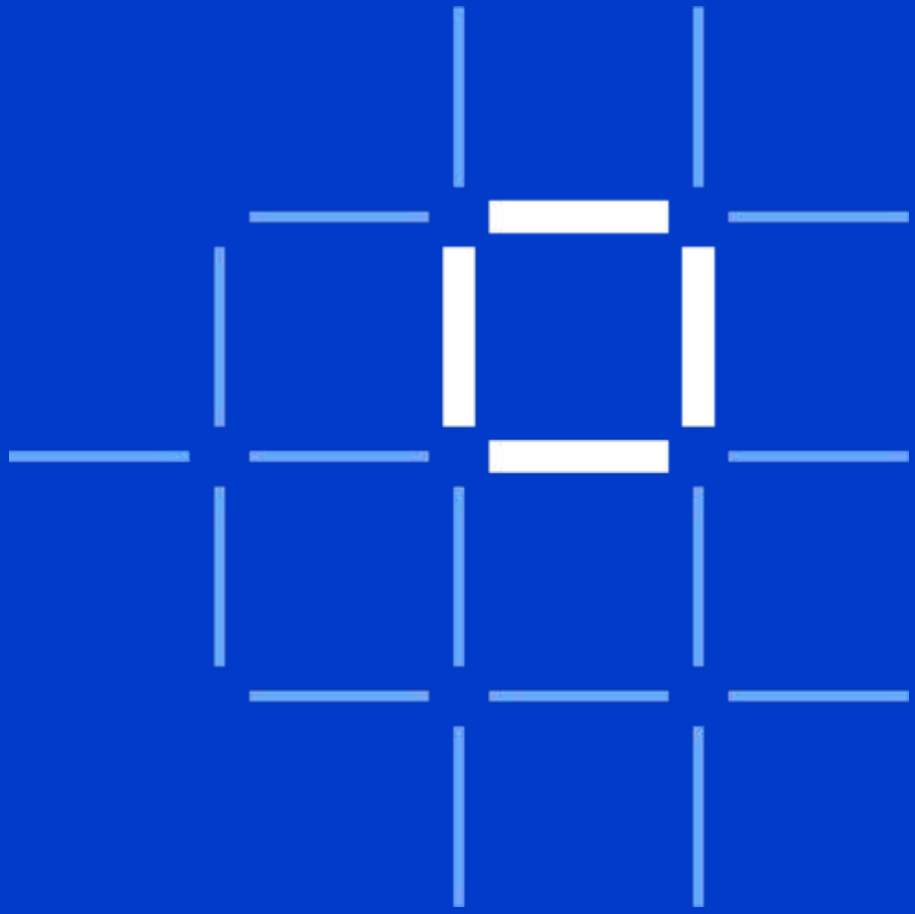
Permissioned Blockchain



Blockchain introduction

Solutions Overview

IBMi and Blockchain



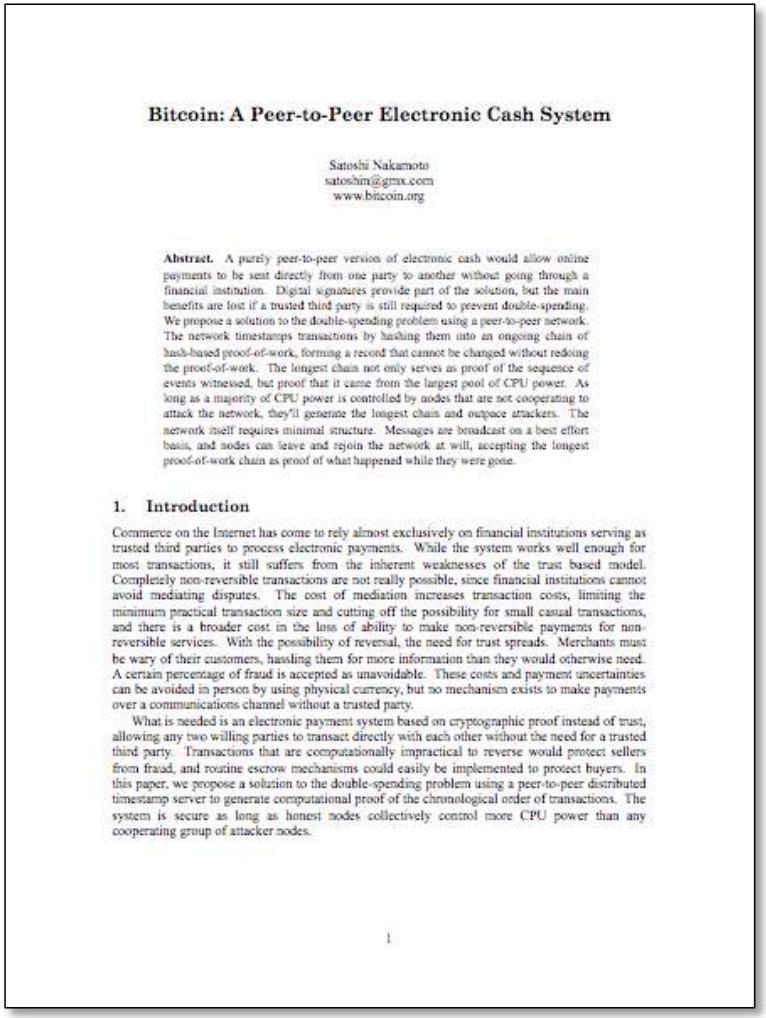
What is Blockchain?

Example networks

How can IBM help?

History of Blockchain: Bitcoin

- 2008 whitepaper by "Satoshi Nakamoto"
- Peer-to-peer electronic cash system
- No mention of blockchain!



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

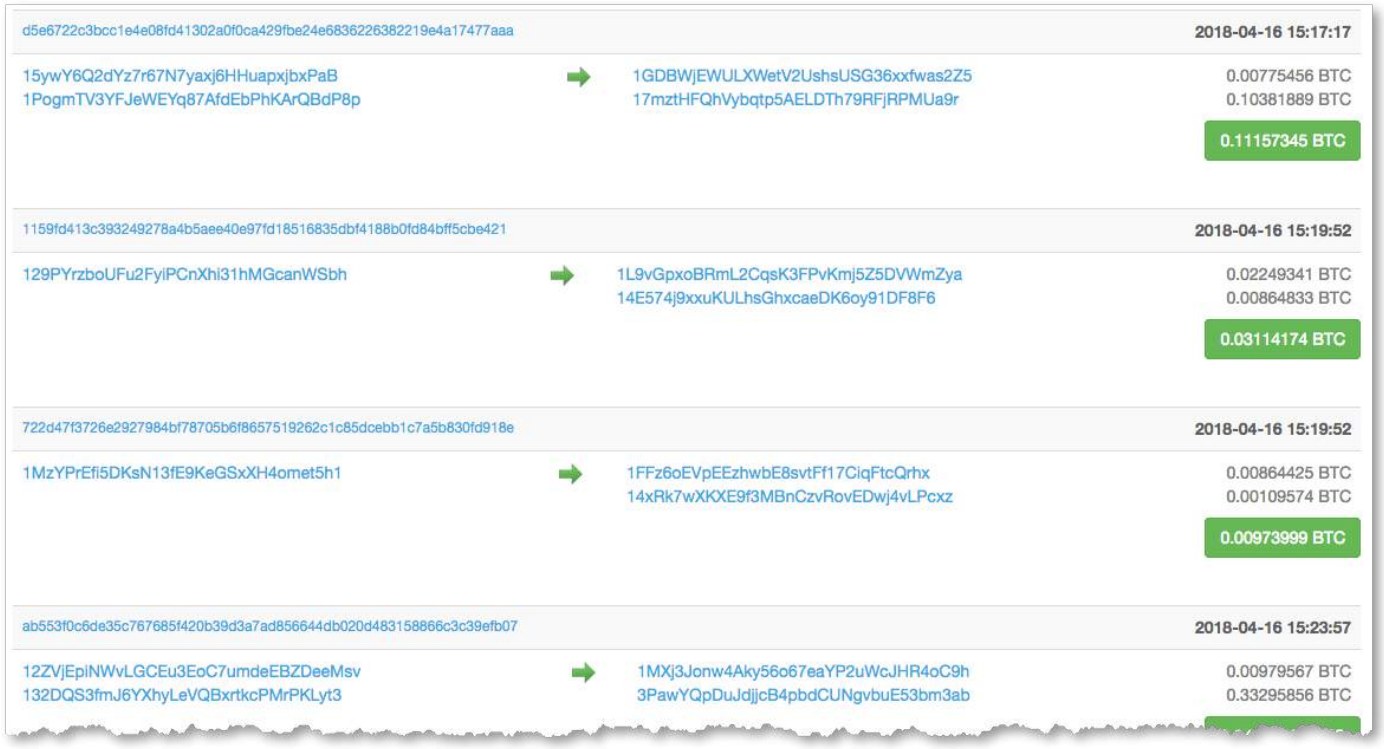
What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

1

https://bitcoin.org/bitcoin.pdf

Themes of Bitcoin

- Combination of Ledger and Asset
- Pseudonymity
- Proof-of-work



https://blockchain.info

Bitcoin in Business

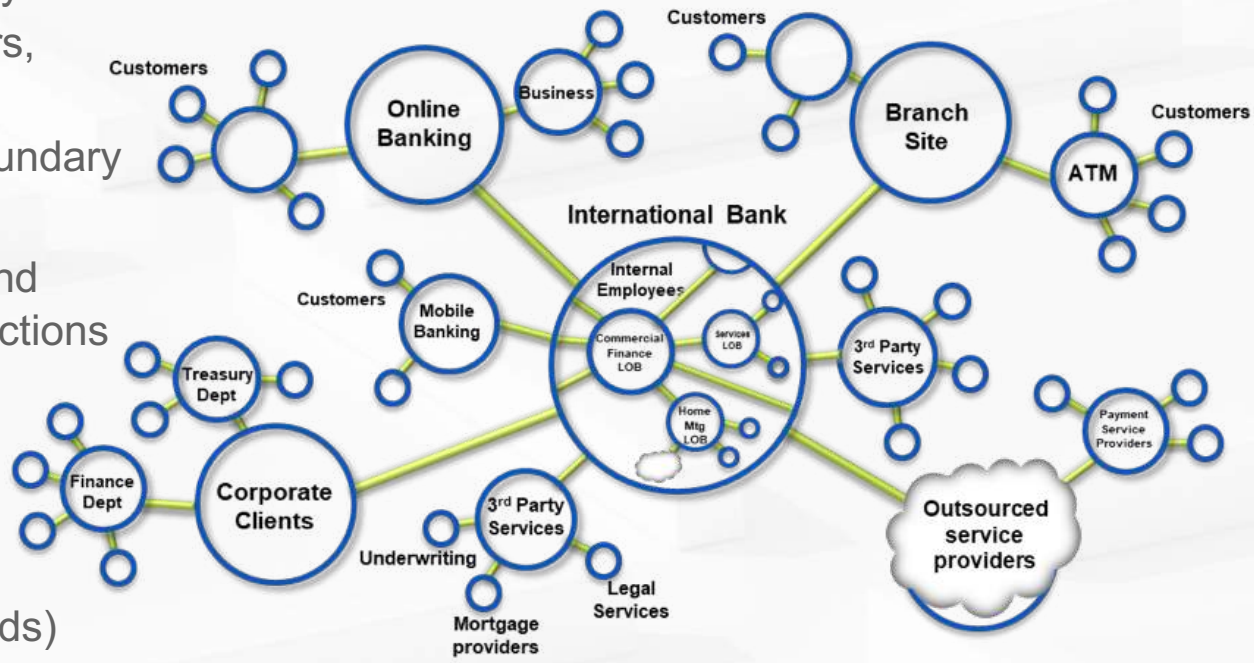
Bitcoin is generally unsuitable as a blockchain for business

- Different (and multiple) **asset** types
- Requirements surrounding **identity**
- Transaction **privacy** and confidentiality
- Timely **confirmation** of transactions

Alternative blockchain implementations (including Bitcoin forks) attempt to address these requirements.

Business networks, wealth and markets

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



Transferring **assets**, building value

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

Two fundamental types of asset

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

Intangible assets subdivide

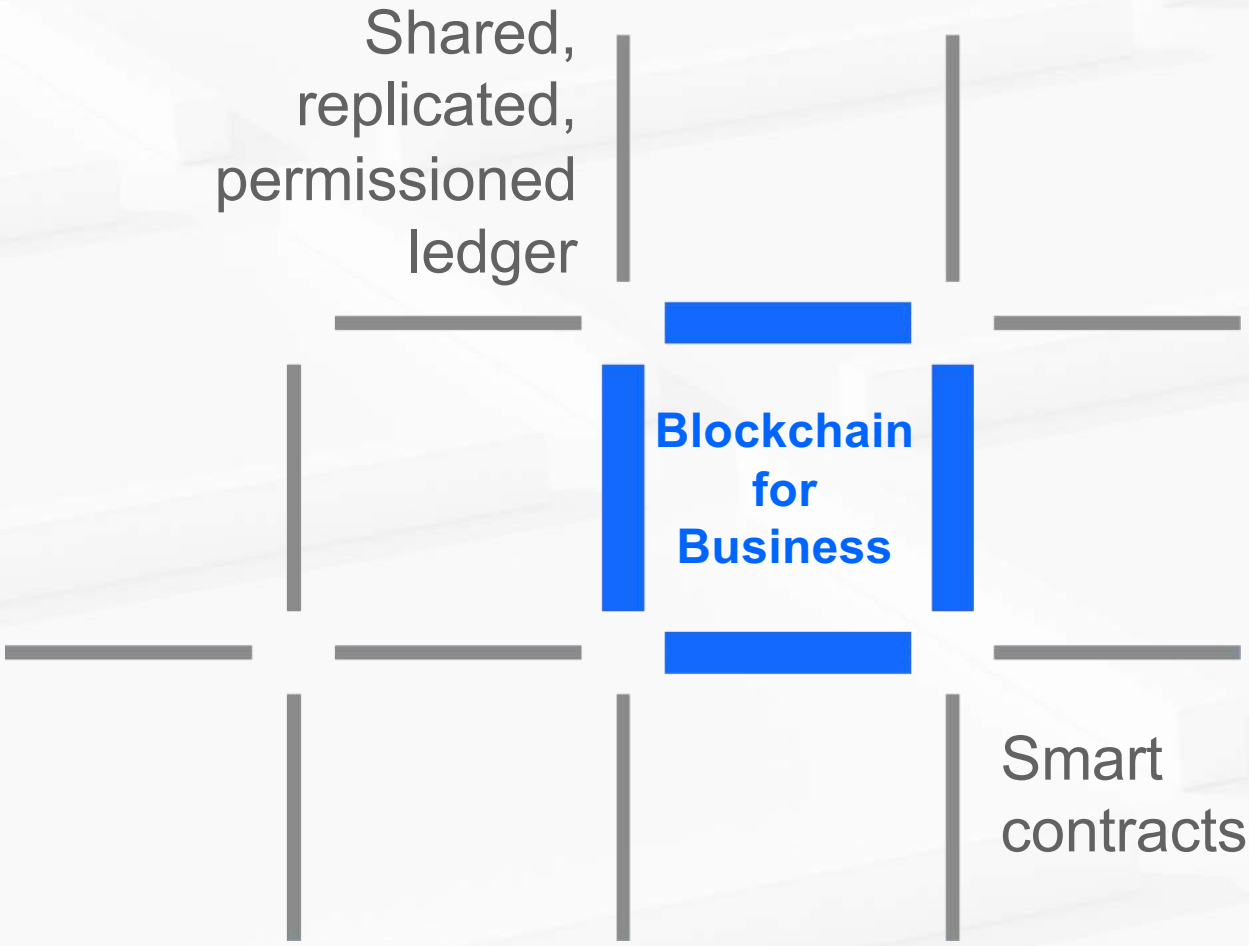
- Financial, e.g. bond
- Intellectual, e.g. patents
- Digital, e.g. data

Cash is also an asset

- Has property of anonymity

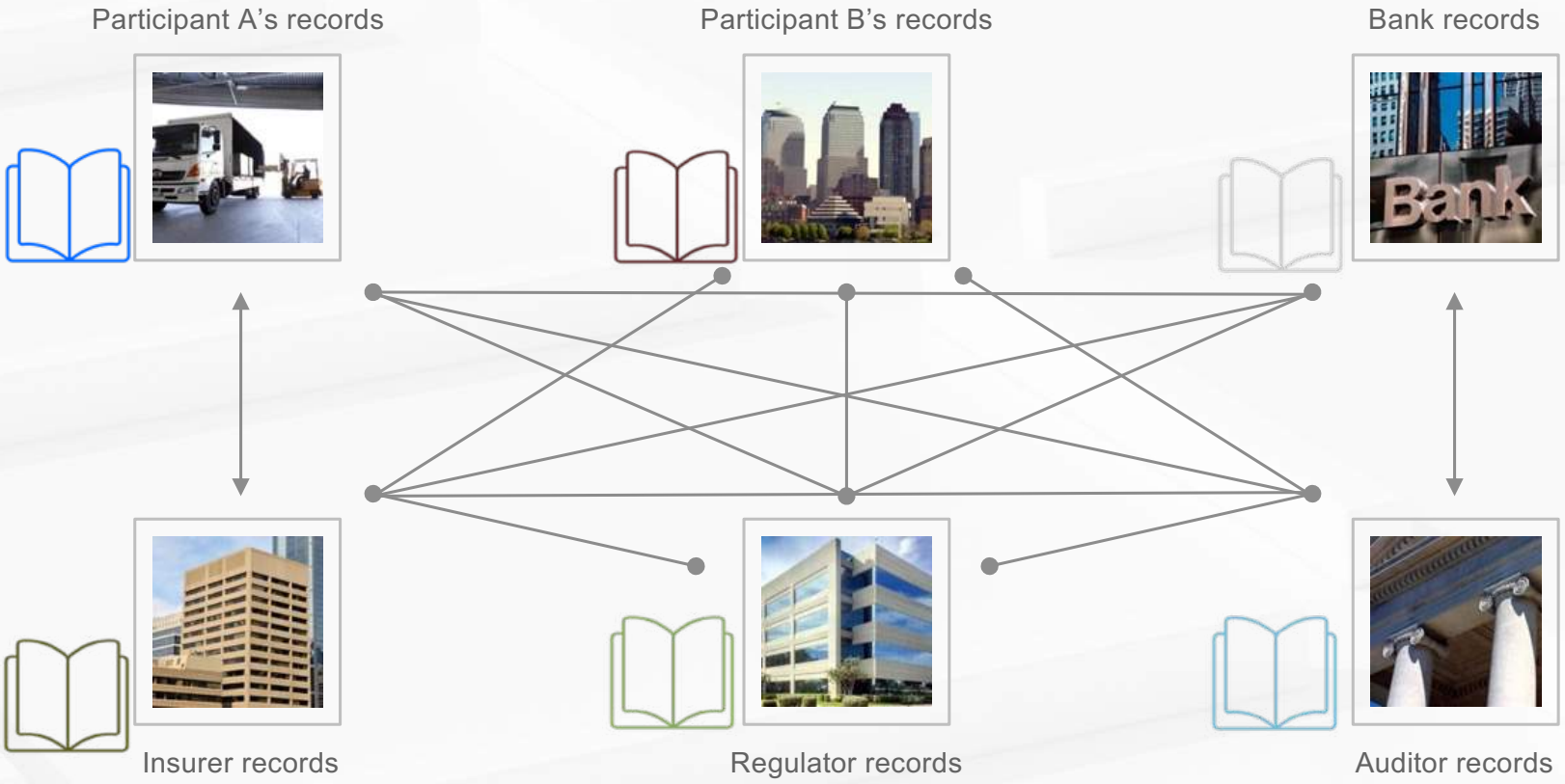
Ledgers, Transactions and Contracts

- 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)


Shared,
replicated,
permissioned
ledger
Blockchain
for
Business
Smart
contracts

Problem

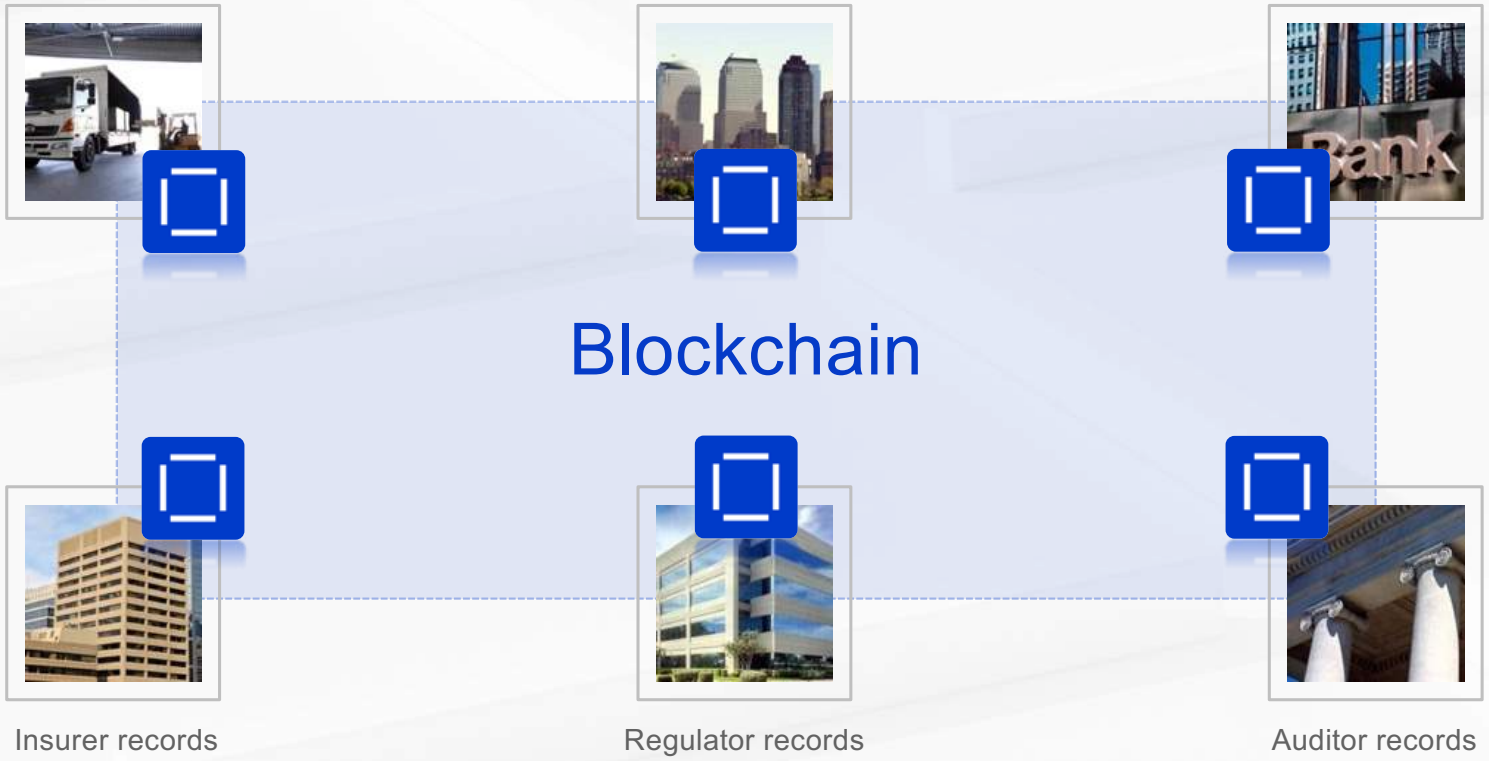
inefficient, expensive, vulnerable



Solution

A shared, replicated, permissioned ledger…

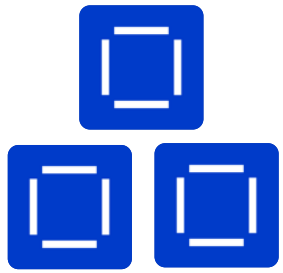
…with consensus, provenance, immutability and finality



Traditional databases cannot be used in untrusted networks

- A traditional database is **centralized**
- Everyone needs to **trust** the administrator managing the database
- There's typically **no immutability or provenance**

- Databases shared across organizations do not alleviate the **trust** issue
- There are now **more copies** to worry about and **more administrators**



- **Blockchain** allows the concept of a distributed database to be deployed across an **untrusted network**
- Something a traditional database cannot handle

Different types of blockchain

- All blockchains aim to provide irrefutable proof that a set of transactions occurred between participants

- Different types of blockchain exist:

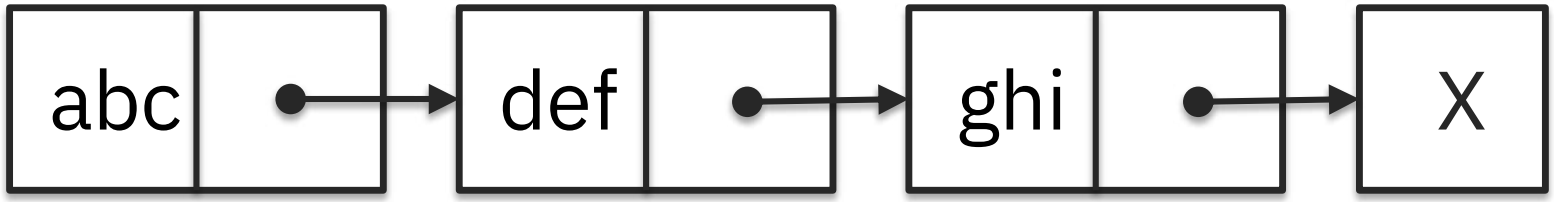
  bitcoin is an example of an unpermissioned, public blockchain
  - The first blockchain application
  - Defines a shadow-currency and its ledger
  - Resource intensive

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

Blockchain implementations vary

The Linked List

- **Linear collection of data elements**
- **Each element is linked to the next**
- **Concept dates from 1955**



One-Way Hash Functions

- Any function that can be applied to a set of data that is guaranteed to produce the same output for the same input
- One-way means that you can't derive the input from the output
- Often, outputs are *unlikely* to repeat for different inputs
- Forms the basis of much cryptography

h(abc) = 7859
h(def) = 8693
h'(7859) = ?
h(abc) = 7859

The Hash Chain

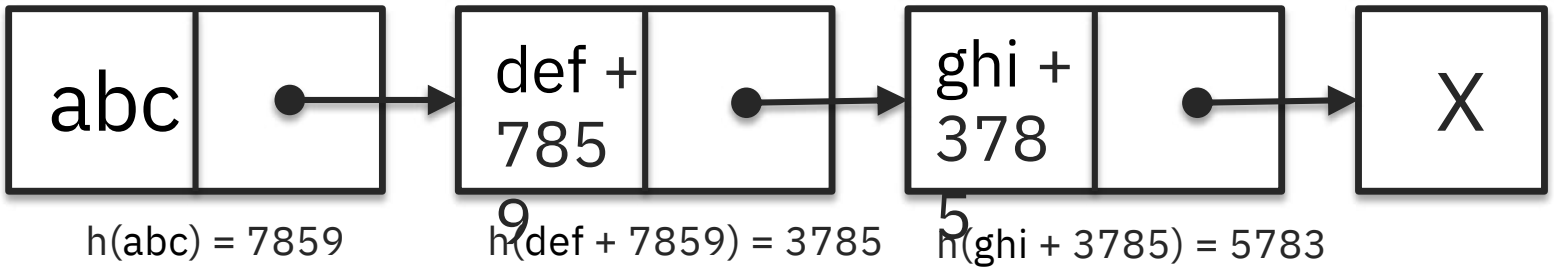
- **Hash chain: A successive application of a hash function**

$$h(h(h(abc))) = 1859$$

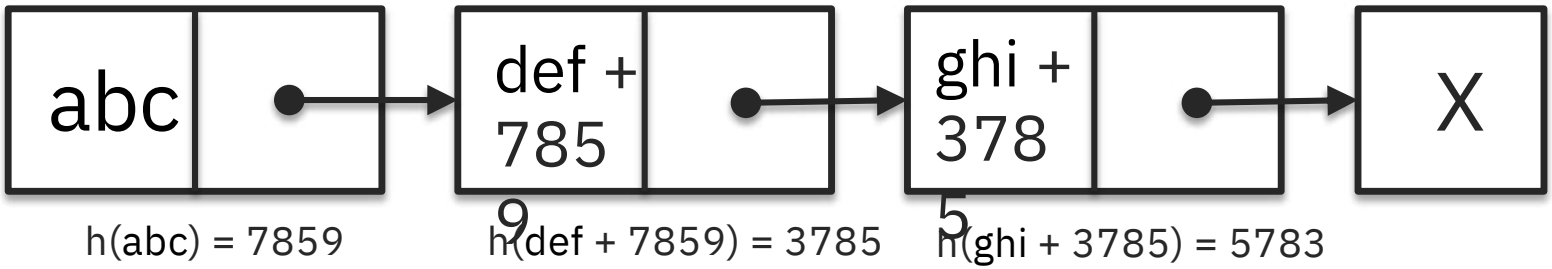
- **Can combine new data with each successive hash:**

$$h(ghi+h(def+h(abc))) = 5783$$

- **Using this concept you can produce a tamper resistant linked list:**

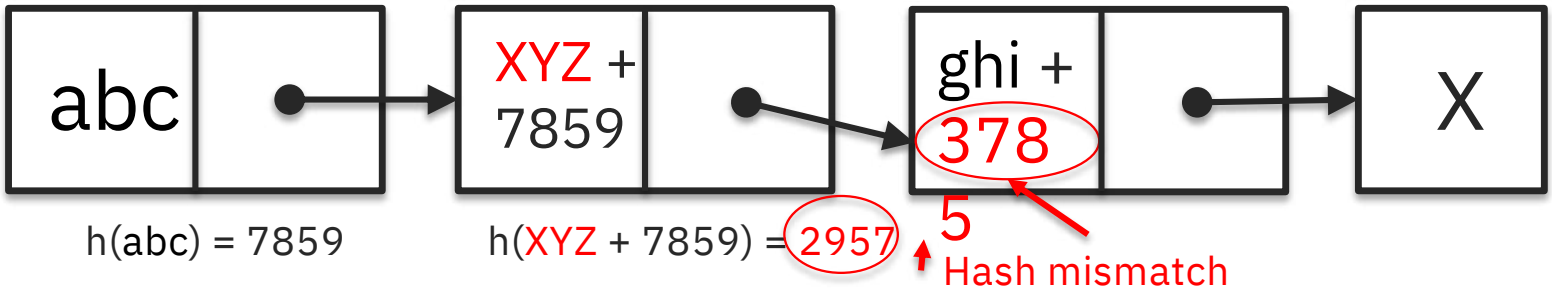


How is This Tamper Resistant?



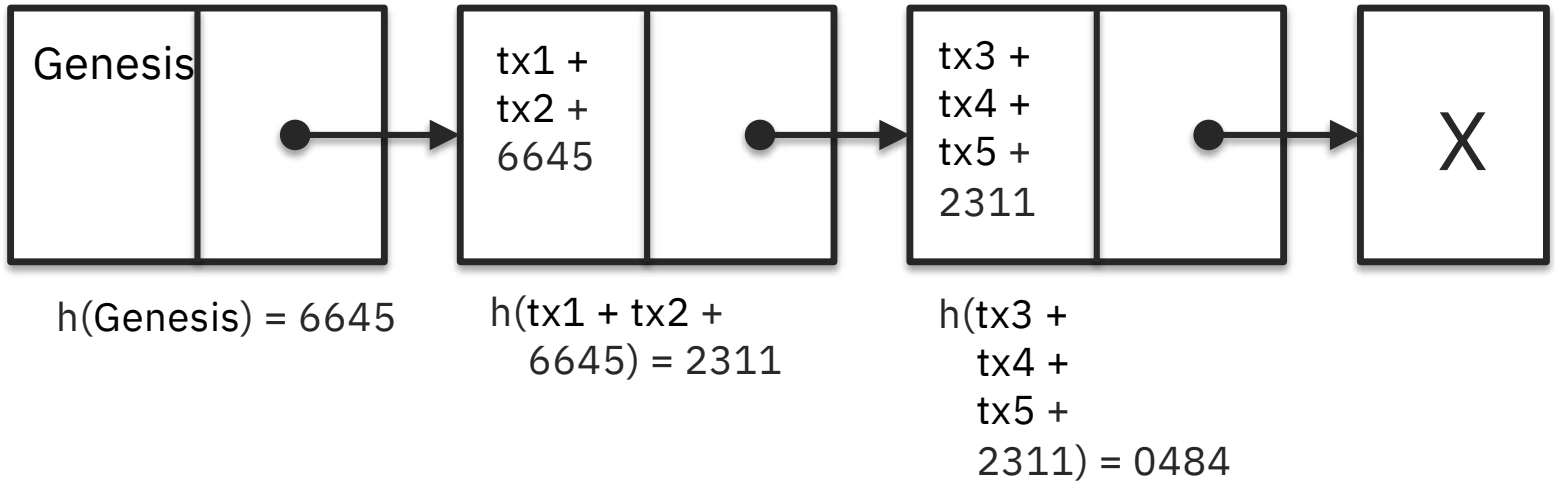
Any modification to a data element means that the hashes will not match up

You would need to recreate the downstream chain



Applied to Blockchain

- **A blockchain is a hash chain (*with optimizations* that we'll cover shortly)**
- **Each element (block) in the linked list is a set of zero or more transactions**
  - Transactions are an implementation-dependent data object
- **First block known as a genesis block**
  - May contain some identifying string or other configuration metadata



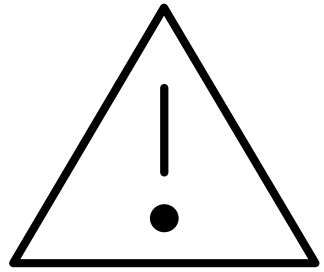
Try this at home - ILE RPG implementation

```
// creating a list listPtr = list_create();
// check if the list is empty (it should be)
 if (list_isEmpty(listPtr));
            dsply 'List is empty';
            else;
            dsply 'List is not empty';
endif;
 // create a new list which is populated with
// a subset of data from the original list
sublistPtr = list_sublist(listPtr : 2);
// iterate through the entries of the list
valuePtr = list_iterate(sublistPtr);
dow (valuePtr <> *null);
            value = %str(valuePtr);
             len = %len(%trimr(value));
             //Set the HASH Algorithm you want to use !
            alg.HashAlg = HASH_SHA1;
            //API to calculate the SHA1 hash
            Qc3CalculateHash( %addr(value)  : len   : 'DATA0100'  : alg  : 'ALGD0500'  : '0'  : *OMIT  : bin  : ErrorNull);
            //Convert to HEX
            cvthc( $hex: bin: %len(bin)*2);
            dsply $hex;
            valuePtr = list_iterate(sublistPtr);
enddo;
 // freeing the allocated memory list_
dispose(listPtr);
```

https://www.mysamplecode.com/2011/05/rpgle-generate-sha-1-hash-use.html
https://bitbucket.org/m1hael/llist/src/master/README.md

Some Problems with This Approach

- **In the event of tampering, it can be difficult to identify which transaction was modified** (particularly when there are many transactions in a block)
  - It is not feasible to have one transaction per block
- **It requires all transaction data in order to retain integrity of chain**
- **Searching transactions is linear** (time consuming)



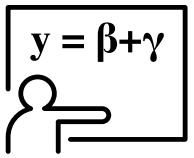
Advantages of Blockchain

Blockchain adds irrefutable proof that a transaction occurred

- **Consensus**: Agreement that a transaction occurred
- **Provenance**: History of transactions
- **Immutability**: An append-only data structure
- **Finality**: An agreed source of truth

Note that proof is not the same as trust!

Consensus Mechanisms



Proof of work

Require validators to solve difficult cryptographic puzzles

PROs: Works in untrusted networks

CONs: Relies on energy use; slow to confirm transactions

Example usage: Bitcoin, Ethereum

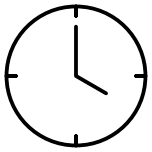
Proof of stake

Require validators to hold currency in escrow

PROs: Works in untrusted networks

CONs: Requires intrinsic (crypto)currency, ”Nothing at stake” problem

Example usage: Nxt



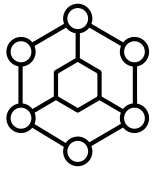
Proof of Elapsed Time

Wait time in a trusted execution environment randomizes block generation

PROs: Efficient

CONs: Requires processor extensions

Example usage: Hyperledger Sawtooth



BFT-based

Byzantine Fault Tolerance implementations

PROs: Reasonably efficient and tolerant against malicious peers

CONs: Validators are known and totally connected

Example usage: Sumeragi in Hyperledger Iroha

Raft

Ordering service distributes blocks to peers

PROs: Efficient and fault tolerant

CONs: Does not guard against malicious activity

Example usage: Hyperledger Fabric V1.4.1+

http://thesecretlivesofdata.com/raft/

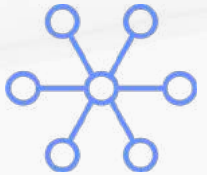
Requirements of **blockchain for business**

ASSETS

Participants decide which assets to share

IDENTITY

Participants know who they are dealing with; information shared is need-to-know



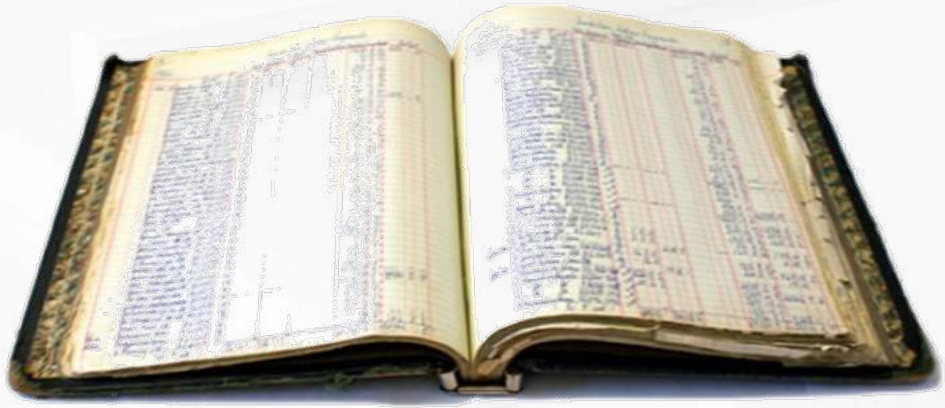
ENDORSEMENT

Participants give provable endorsement

Assets

The business network decides what to share on the ledger

- Assets are anything of value
  - On the blockchain, these are represented digitally using a pre-agreed format
- Transactions change the state of an asset and are provably recorded on the blockchain
  - e.g. transfer ownership, change color
- Transactions are underpinned by smart contracts
  - Verifiable business rules that cause the asset to change state



Identity

Knowing who you're dealing with

- Various regulations applied to businesses require them to know who they are dealing with
  - e.g. KYC, AML, CFT
- Identity is used to ensure business networks are kept private and individual transactions confidential
  - With transparency for the regulator
- There are established methods for obtaining and asserting identity
  - Cryptography is central to these
  - Identity allows transactions to be signed and encrypted

Transaction Endorsement

Provable verification by relevant participants

- Endorsement is the process in which a transaction is verified as “good”
  - Ensures that participants are happy to accept the transaction according to the smart contract, prevent double spending, etc.
- Endorsement can be expensive in public blockchains
  - Without identity, transactions are thrown to the whole network for endorsement
  - Proof of work is particularly CPU intensive
- In the real world, transactions are endorsed by a smaller number of participants
  - e.g. sender bank, receiver bank, payments provider
  - Must be completed in an appropriate timeframe

Privacy and Confidentiality

Identity also gives us a mechanism to make the blockchain private and confidential

Blockchain networks are generally **private**

- And restricted to the scope of the business network

Individual transactions are usually **confidential**

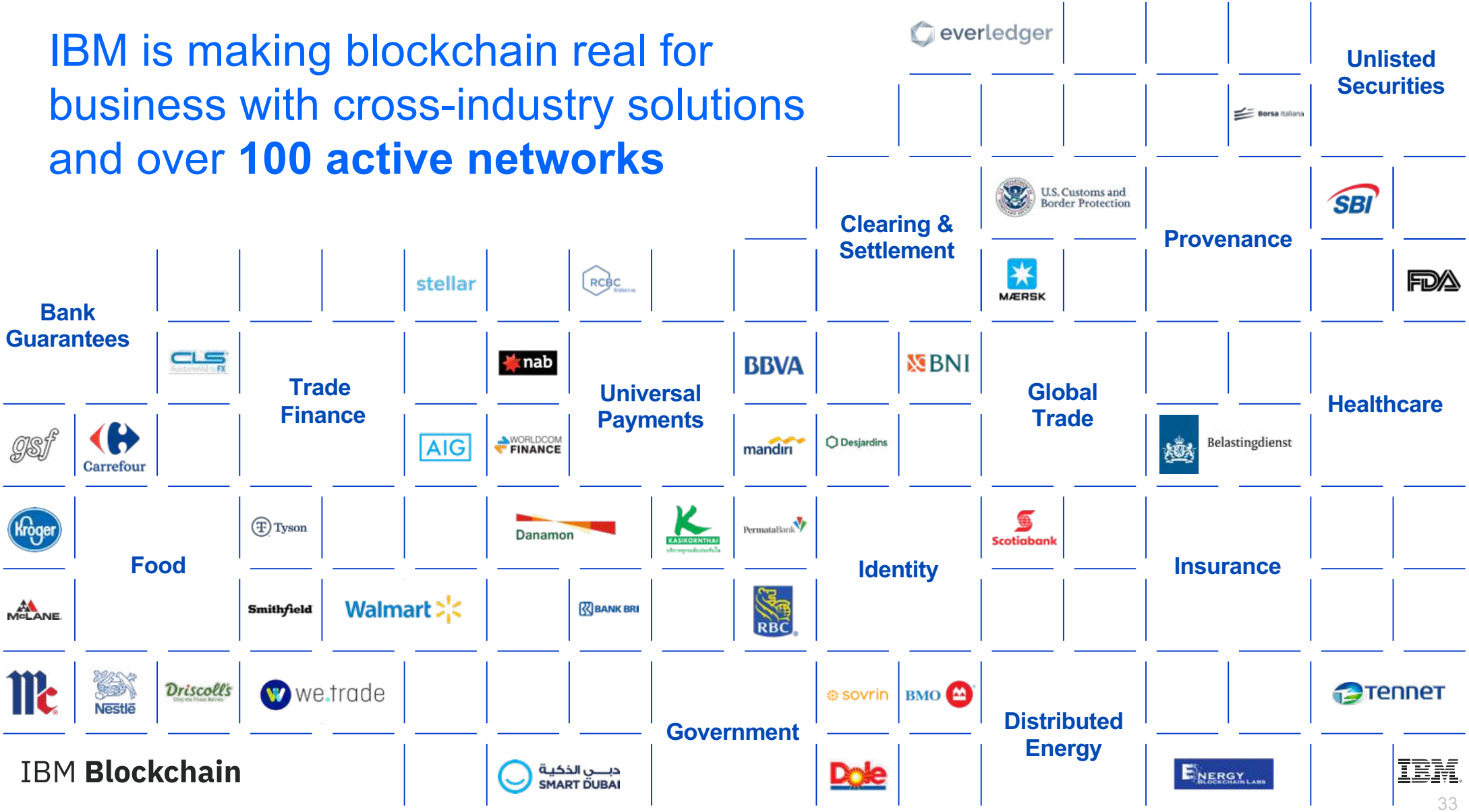
- Transparency for regulator is critical
- However visibility to some participants could give unfair advantage

What is Blockchain?

Example networks

How can IBM help?

IBM is making blockchain real for business with cross-industry solutions and over **100 active networks**

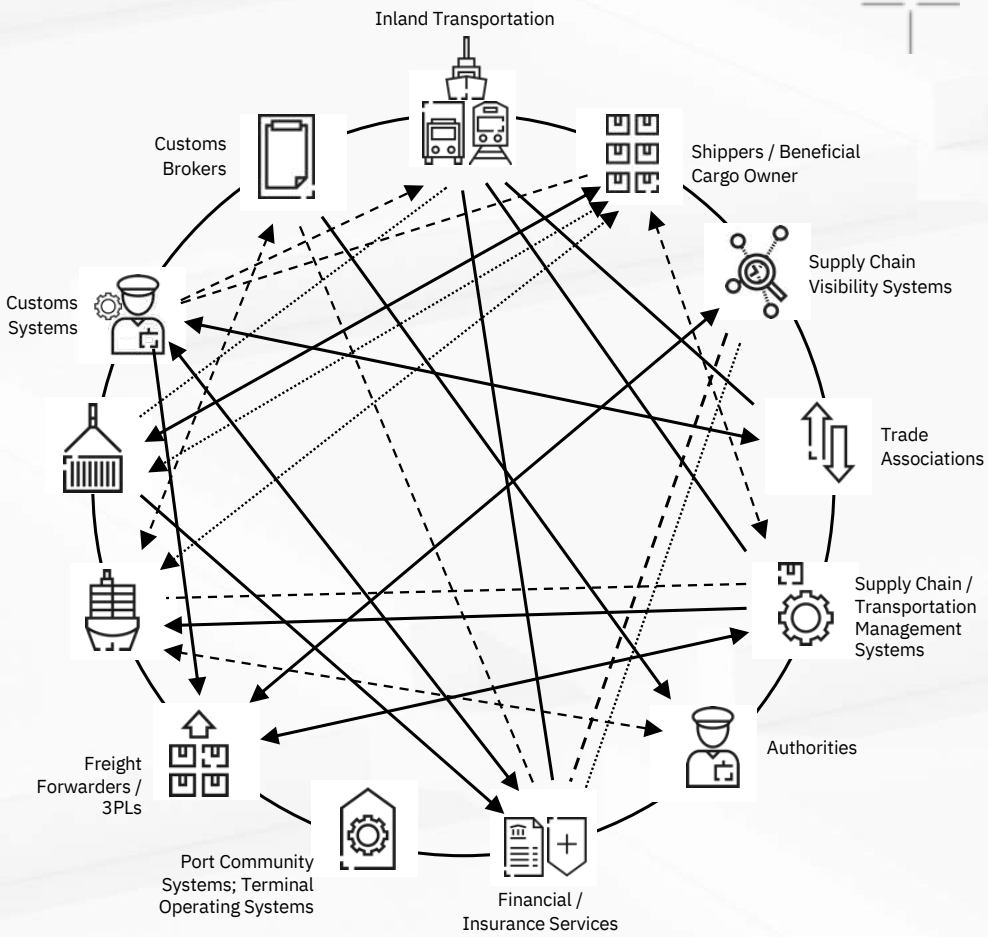


TradeLens improves **global trade efficiency**

- TradeLens is an open, extensible platform for sharing shipping events, messages, and documents across all the actors and systems in the supply chain ecosystem.
- It provides shared visibility and shared state for container shipments

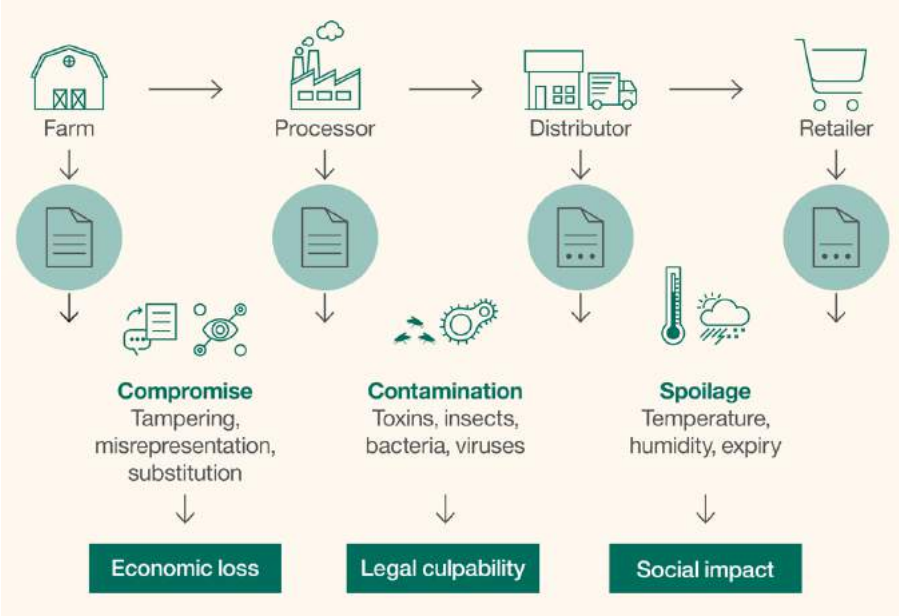
Benefits

- Increase speed and transparency for cross border transactions through real time access to container events.
- Reduced cost and increased efficiency through paperless trade



IBM Food Trust for **supply chain transparency**

- IBM Food Trust is a set of modules 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.

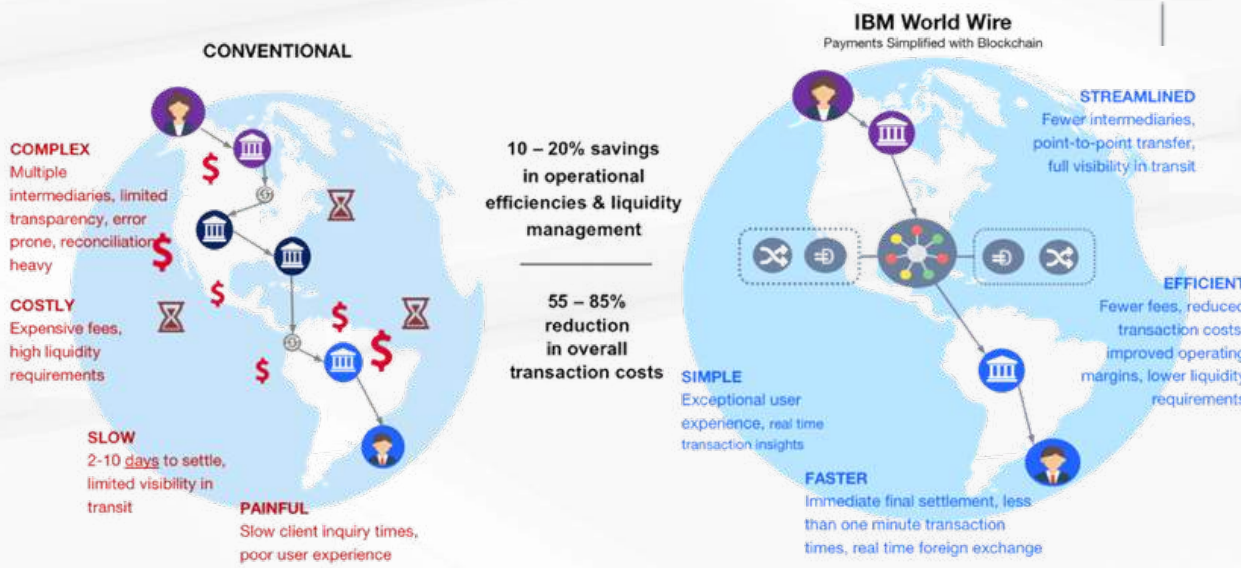


Benefits

- Reduce impact of food recalls through instant access to end-to-end traceability data to verify history in the food network and supply chain.
- Help to address the 1 in 10 people sickened and 400,000 fatalities world wide which occur every year from food-born illnesses.

World Wire is **revolutionizing global payments**

- IBM Blockchain World Wire is an integrated network for real-time clearing and settlement.
- Allows banks and financial institutions to send and settle payments around the globe with finality in a matter of seconds
- Eliminates enduring challenges that have long hampered the cross-border payments industry.



Benefits

- Payment support regardless of size, origination, destination or asset type
- Higher visibility for streamlined transactions with reduced disputes and reconciliation needs
- Enhanced regulatory compliance through improved transparency
- Secure network with interaction and eligibility criteria as well as robust access controls

Decentralized **trusted identity**

- Sovrin pushes identity to the edge of the network
- Cryptographic, point to point exchange of identity
- Based on Hyperledger Indy technology

Benefits

- A decentralized approach that establishes trust and puts the end user in control
- Every person, organization, and thing has a digital wallet to control the flow of their identity
- No PII is stored on the public ledger!

sovrin
identity for all

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

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

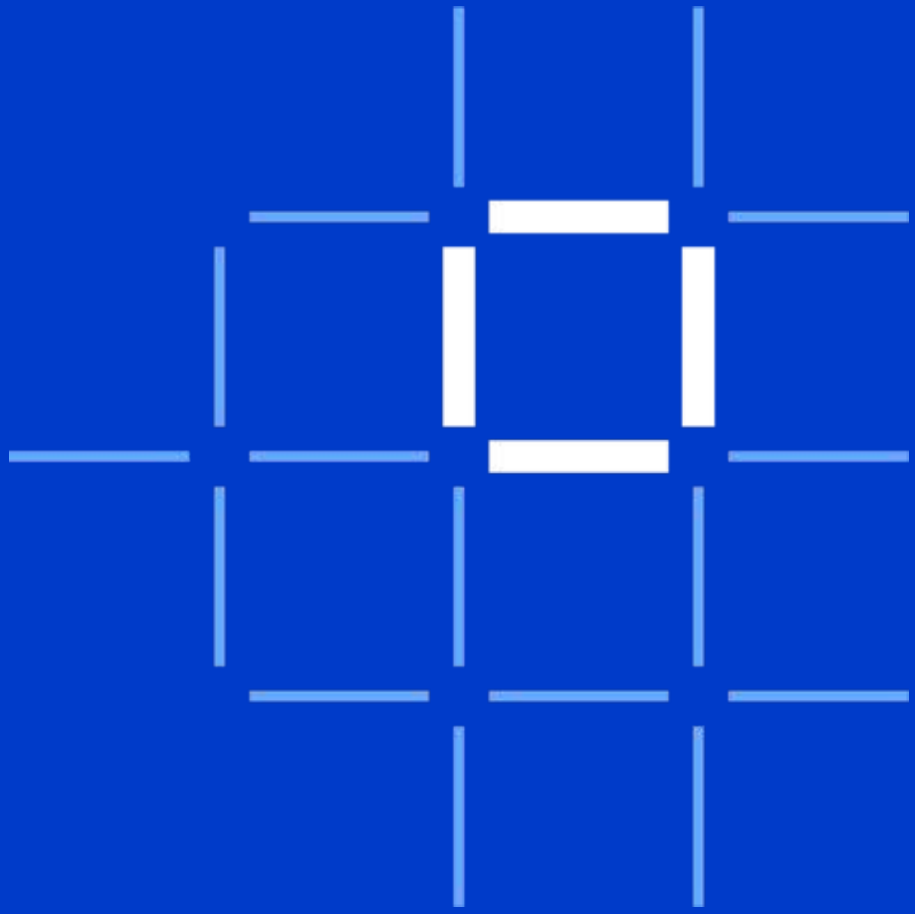
Market Maker

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

What is Blockchain?

Example networks

How can IBM 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

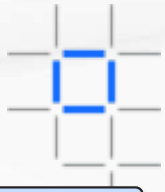
Trusted Expertise

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'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**

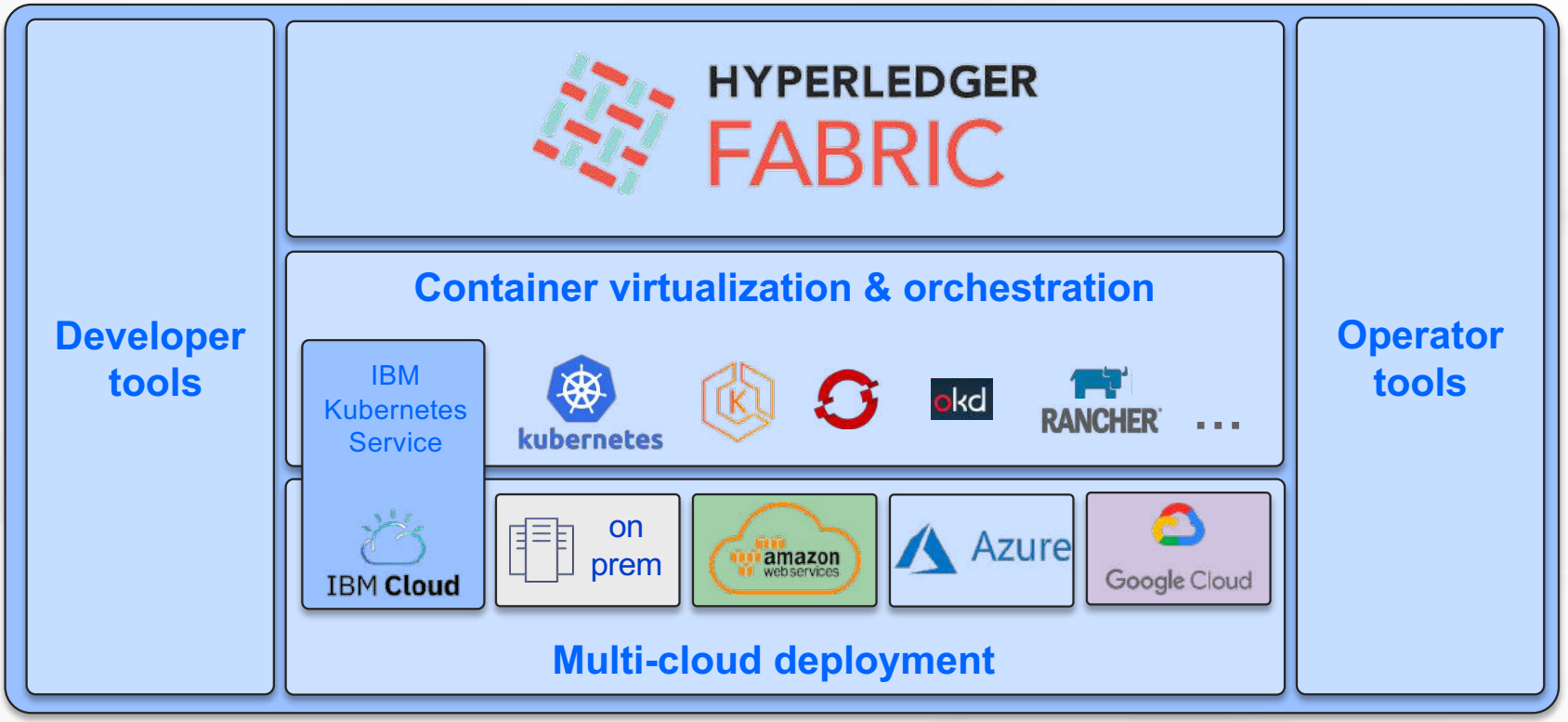
Build and operate blockchain networks in heterogeneous environments

HYPERLEDGER

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

Introducing **IBM Blockchain Platform**

Build and operate Hyperledger Fabric networks



Advanced tooling
Create & manage smart contracts, applications & networks

Open technology
Hyperledger Fabric, Containers, Kubernetes

Deploy anywhere
Comprehensive cloud & on-premises options

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 and has since gathered significant cross-industry momentum
- Open source
  Open standards
  Open governance model

Premier

Associate

General

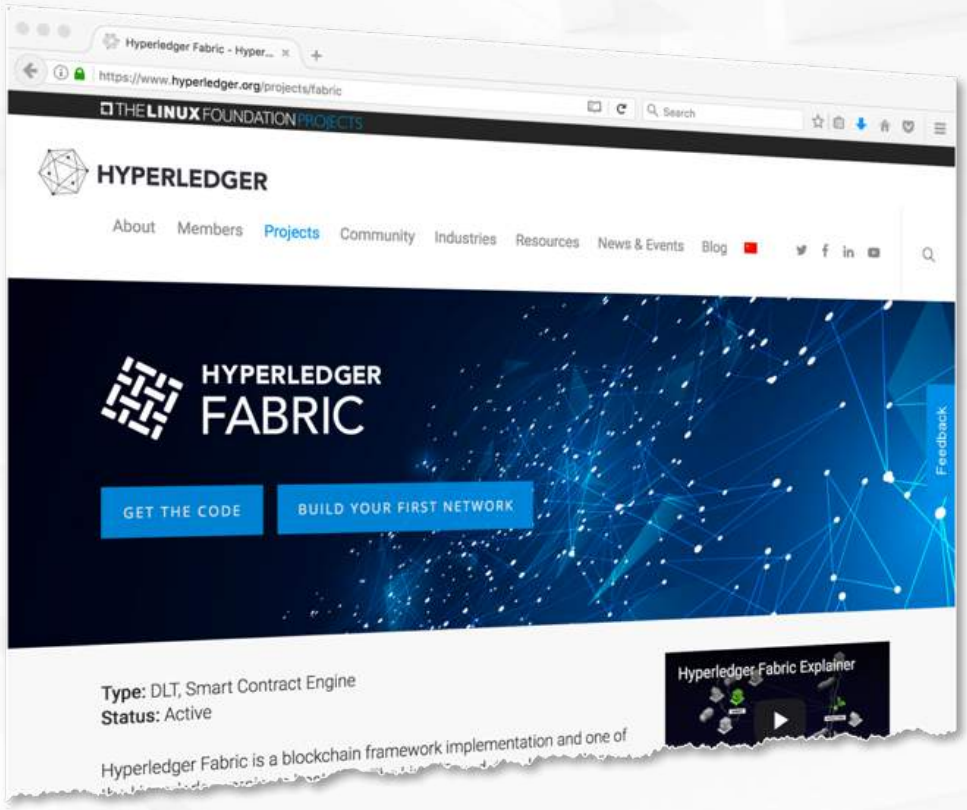
General

Academia Associate

Source: https://www.hyperledger.org/members
Updated: 24 January 2020

HYPERLEDGER FABRIC

Distributed ledger



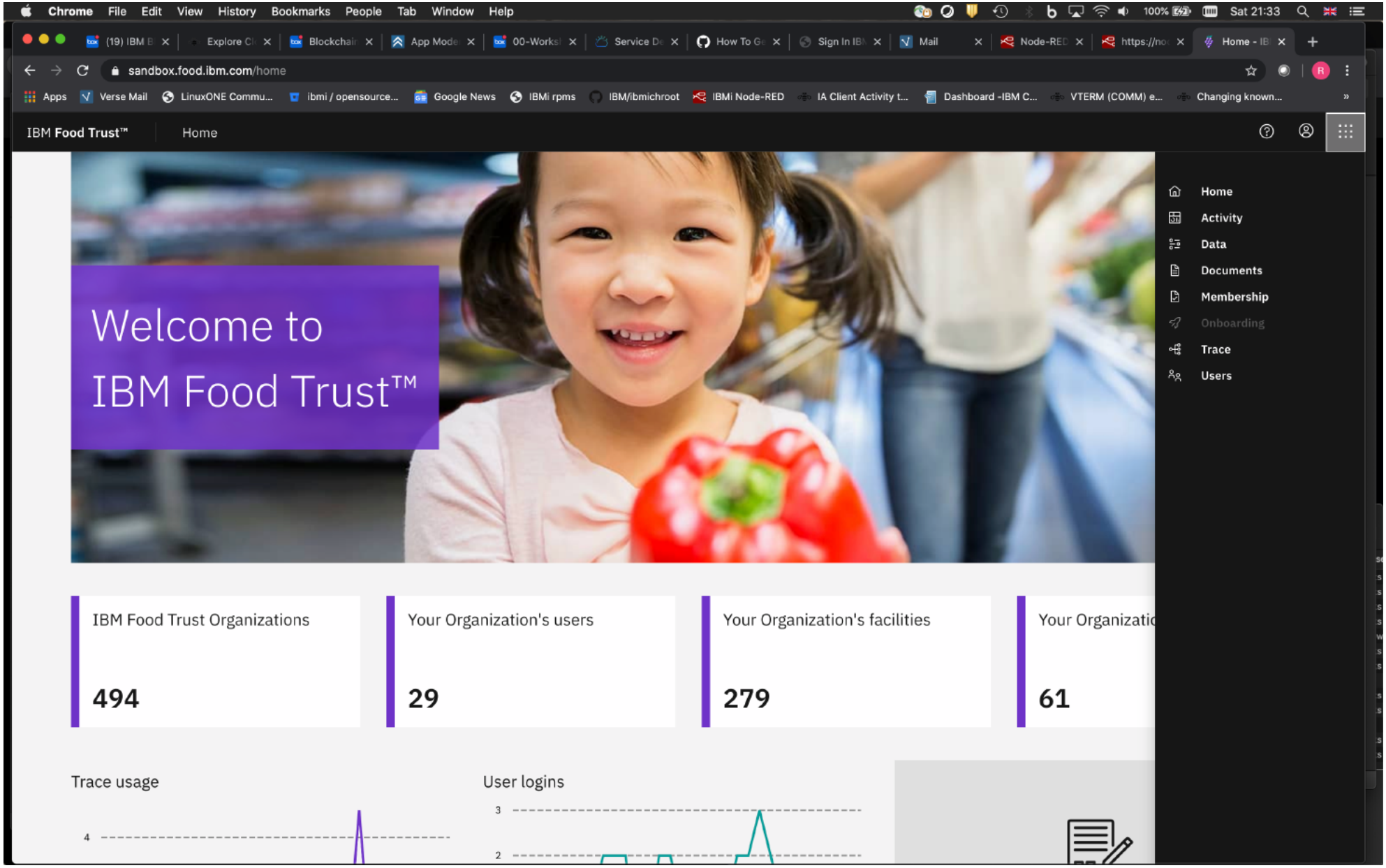
- An implementation of blockchain technology that is a foundation for developing blockchain applications
- Emphasis on ledger, smart contracts, consensus, confidentiality, resiliency and scalability.
- V2.0 released January 2020
  - V1.4 Long Term Service production release with emphasis on operational and serviceability enhancements; new programming model abstractions for ease of development
  - V2.0 stream rolling out significant new features
- IBM is one of the many contributing organizations

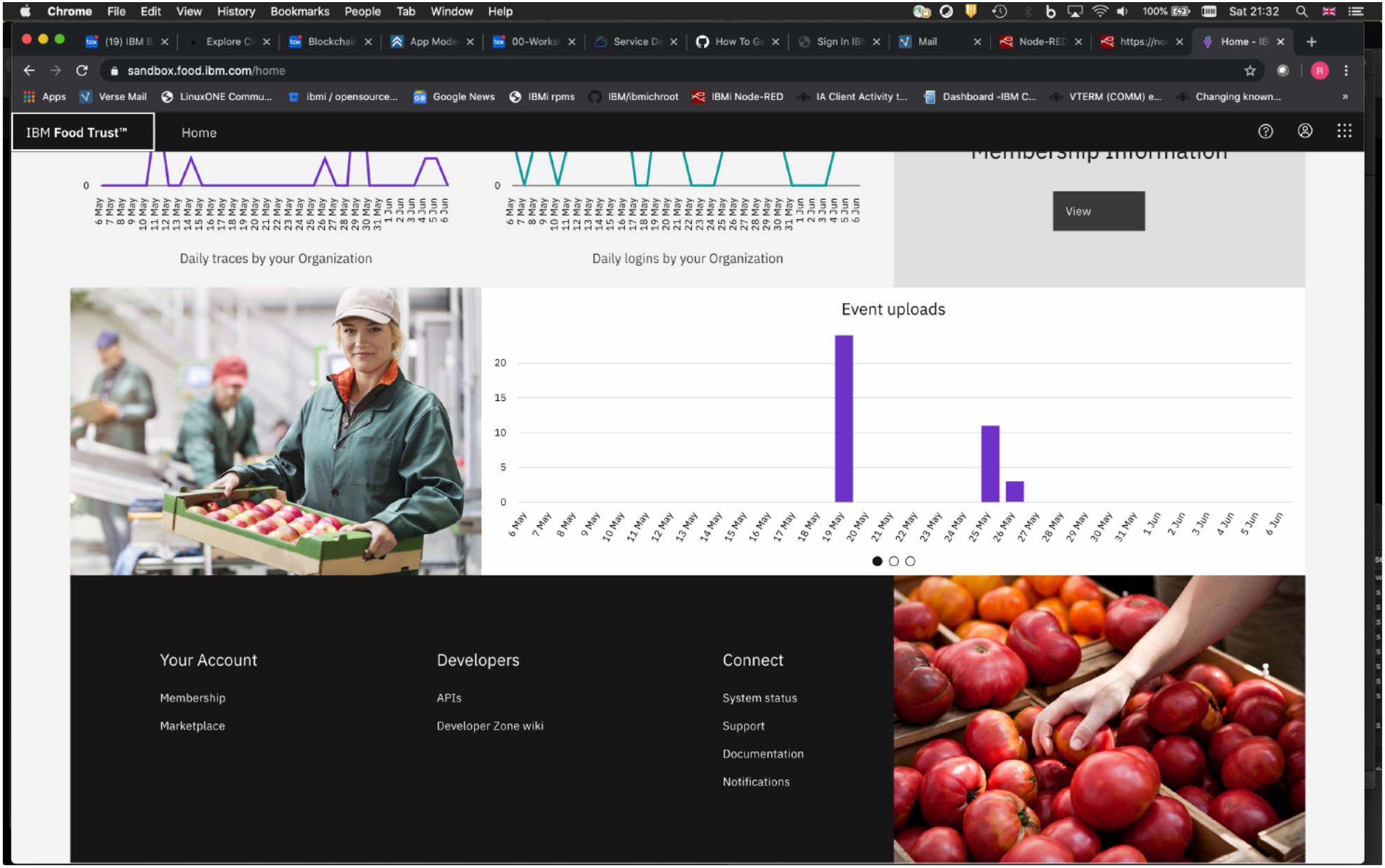
Blockchain introduction

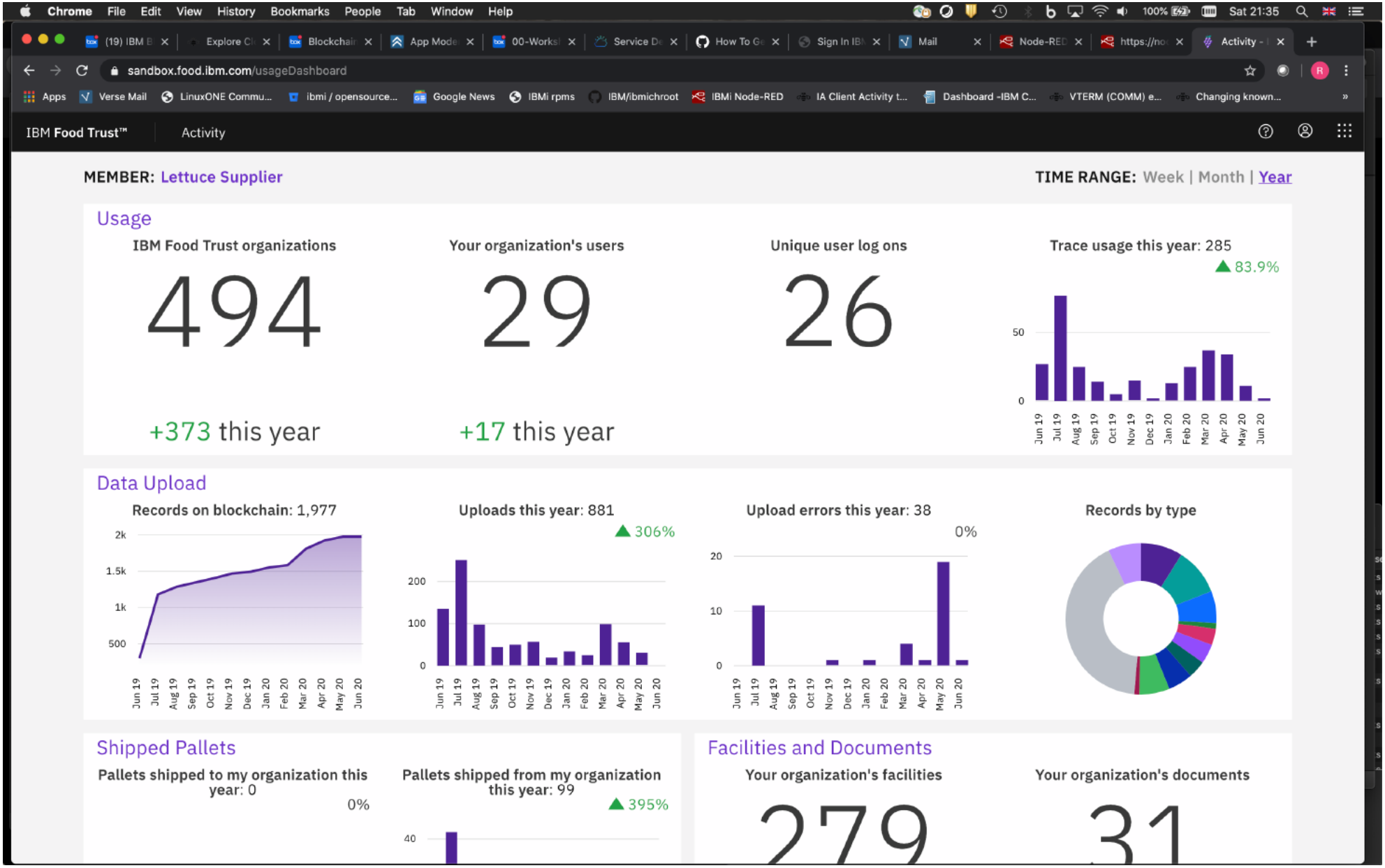
Solutions Overview

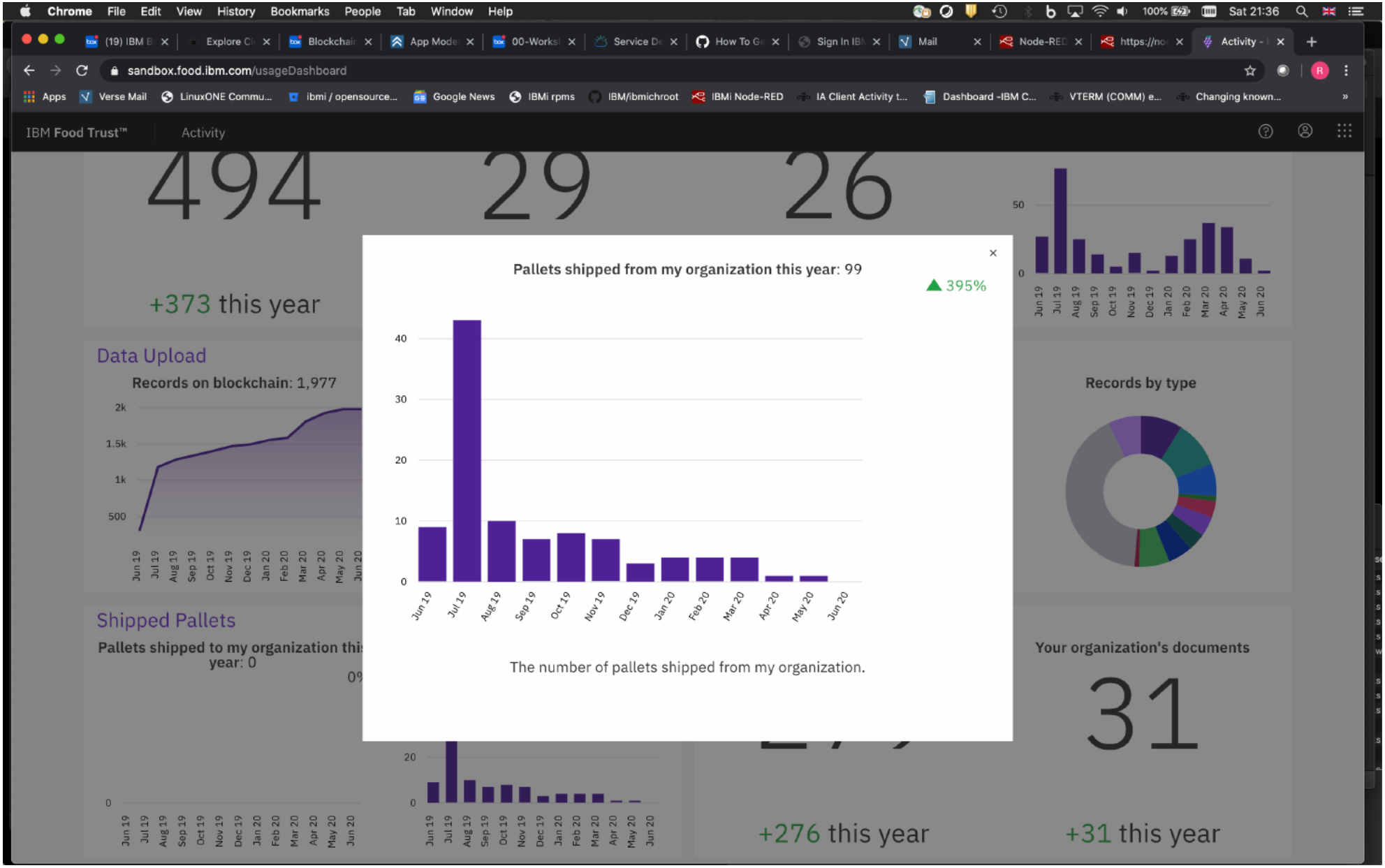
IBMi and Blockchain

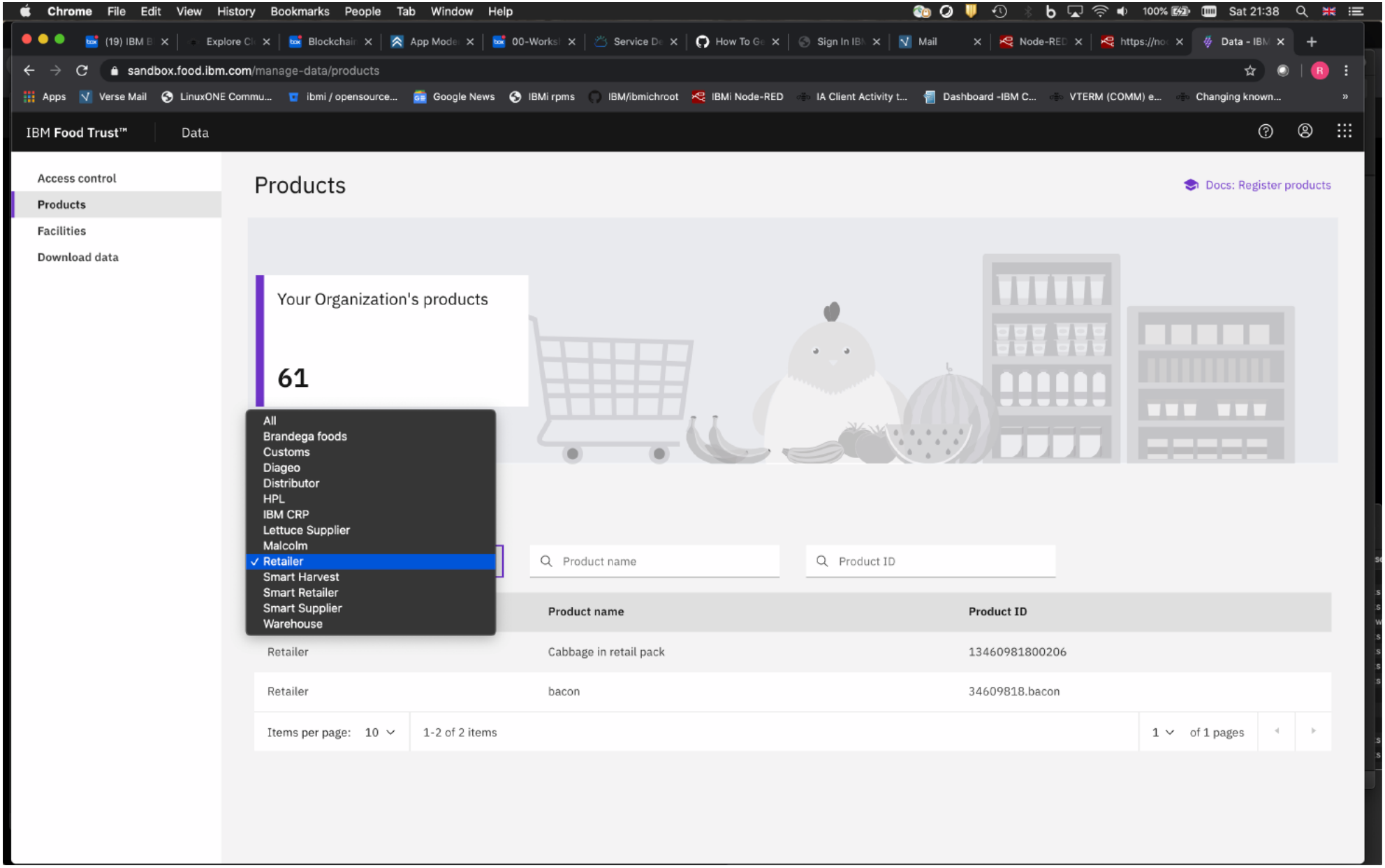
Demo: **IBM Food Trust**

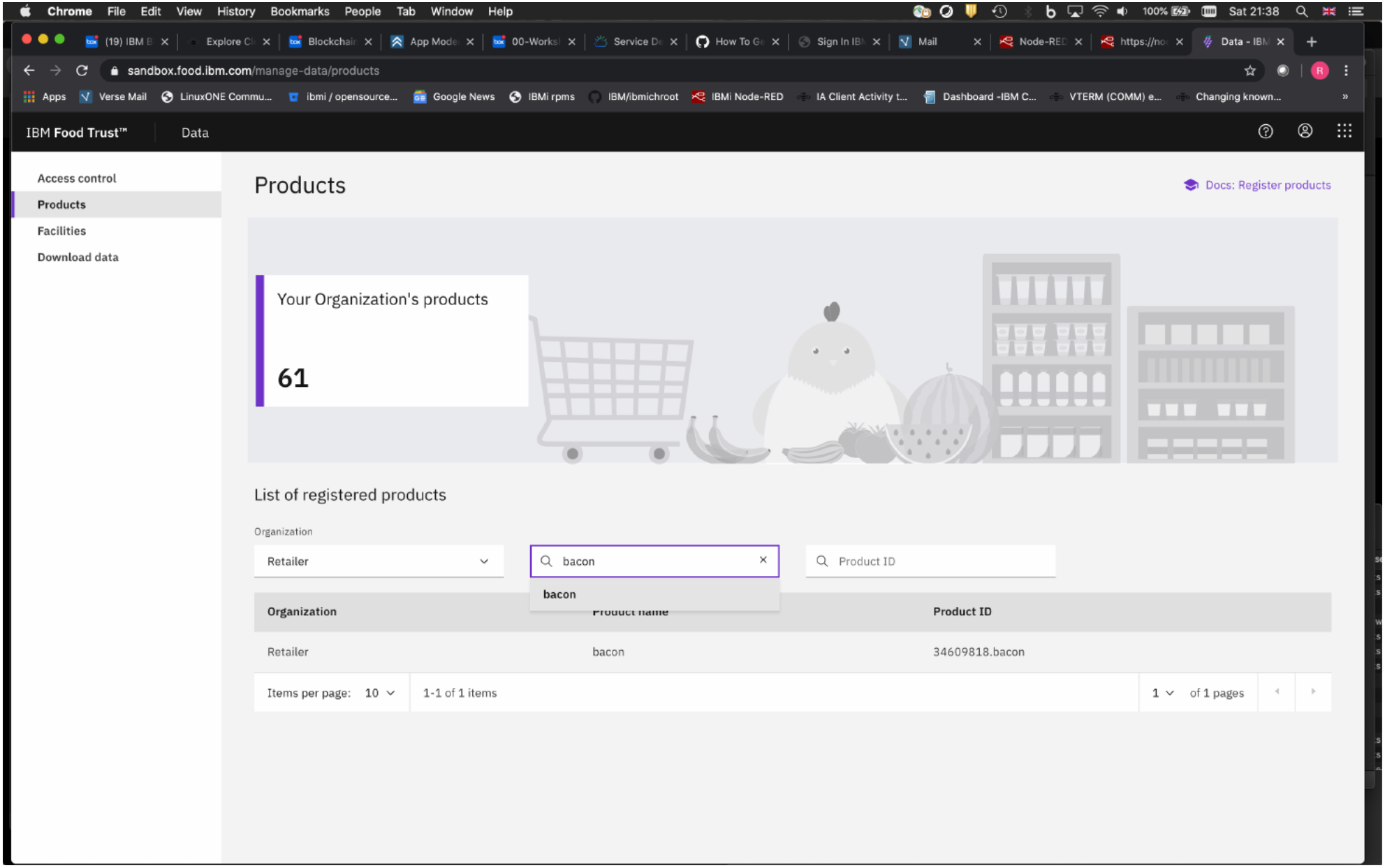

Chrome File Edit View History Bookmarks People Tab Window Help
sandbox.food.ibm.com/home
IBM Food Trust™
Home
Welcome to IBM Food Trust™
Home
Activity
Data
Documents
Membership
Onboarding
Trace
Users
IBM Food Trust Organizations
494
Your Organization's users
29
Your Organization's facilities
279
61
Trace usage
User logins

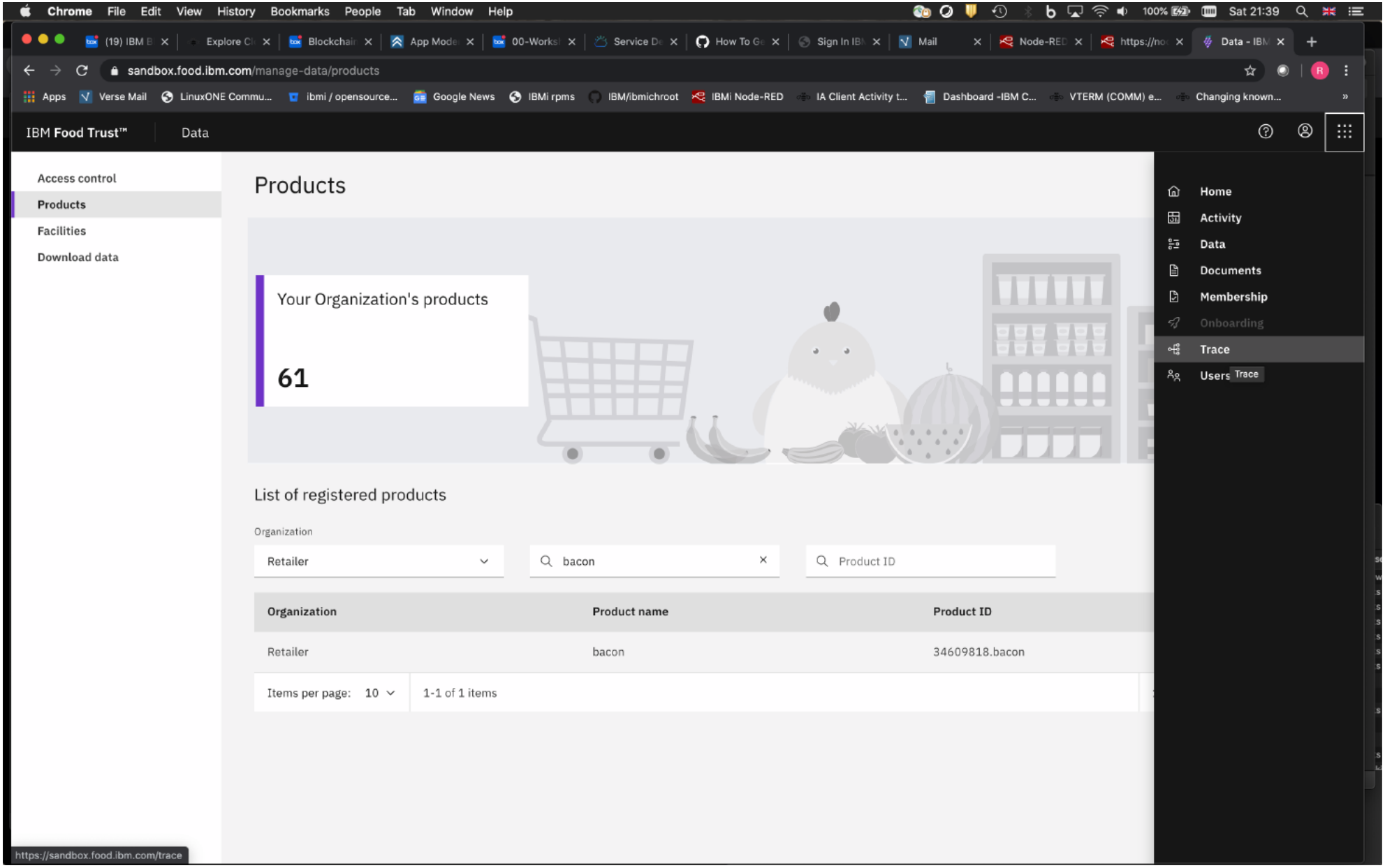

Chrome File Edit View History Bookmarks People Tab Window Help
sandbox.food.ibm.com/home
IBM Food Trust™
Home
Daily traces by your Organization
Daily logins by your Organization
View
Event uploads
Your Account
Membership
Marketplace
Developers
APIs
Developer Zone wiki
Connect
System status
Support
Documentation
Notifications

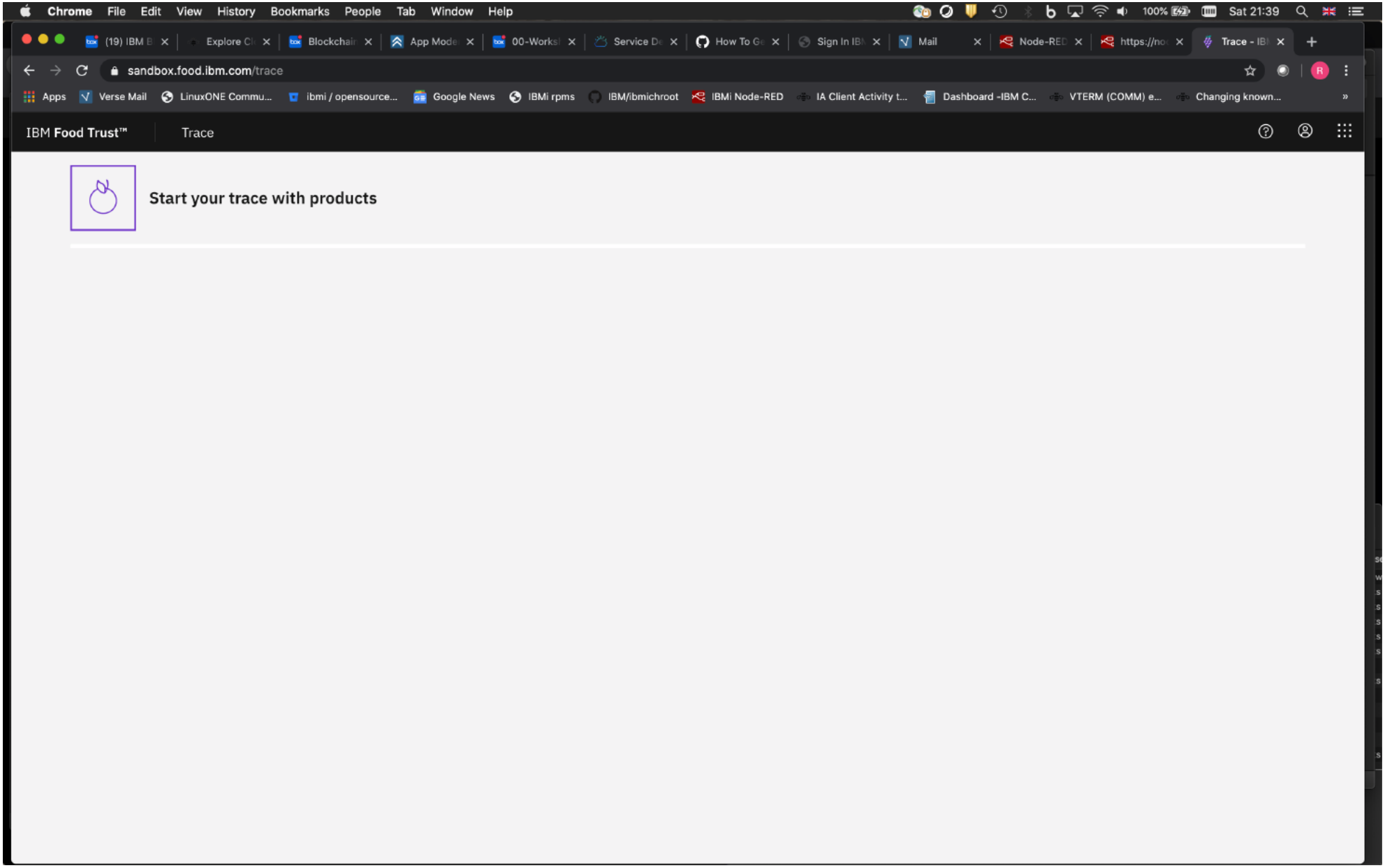

Chrome File Edit View History Bookmarks People Tab Window Help
Sat 21:35
sandbox.food.ibm.com/usageDashboard
IBM Food Trust™
Activity
MEMBER: Lettuce Supplier
TIME RANGE: Week | Month | Year
Usage
IBM Food Trust organizations
494
+373 this year
Your organization's users
29
+17 this year
Unique user log ons
26
Trace usage this year: 285
▲ 83.9%
Data Upload
Records on blockchain: 1,977
Uploads this year: 881
▲ 306%
Upload errors this year: 38
0%
Records by type
Shipped Pallets
Pallets shipped to my organization this year: 0
0%
Pallets shipped from my organization this year: 99
▲ 395%
Facilities and Documents
Your organization's facilities
279
Your organization's documents
31

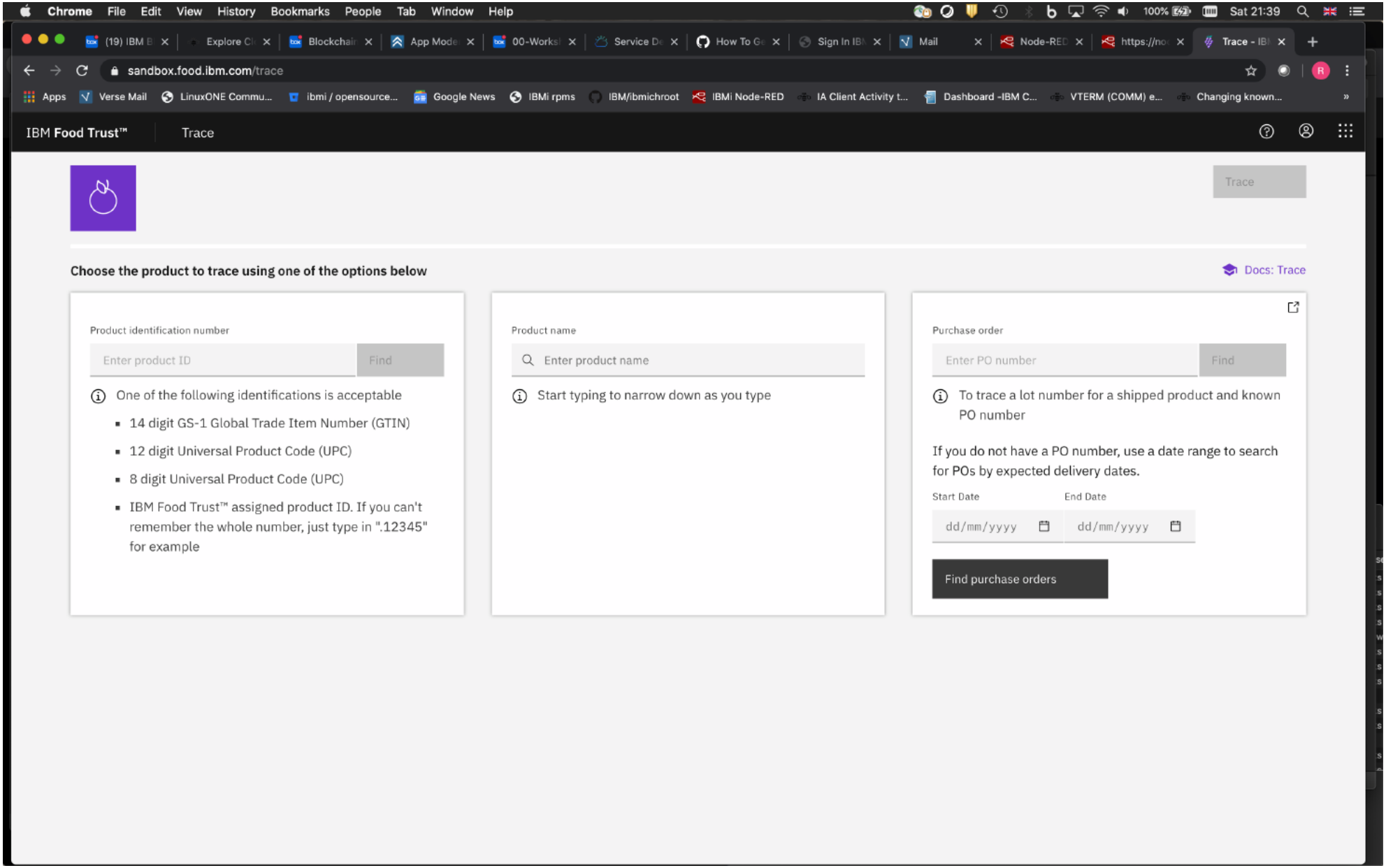

Chrome File Edit View History Bookmarks People Tab Window Help
Sat 21:36
sandbox.food.ibm.com/usageDashboard
IBM Food Trust™
Activity
494
29
26
+373 this year
Data Upload
Records on blockchain: 1,977
Records by type
Shipped Pallets
Pallets shipped to my organization this year: 0
Pallets shipped from my organization this year: 99
▲ 395%
The number of pallets shipped from my organization.
Your organization's documents
31
+276 this year
+31 this year

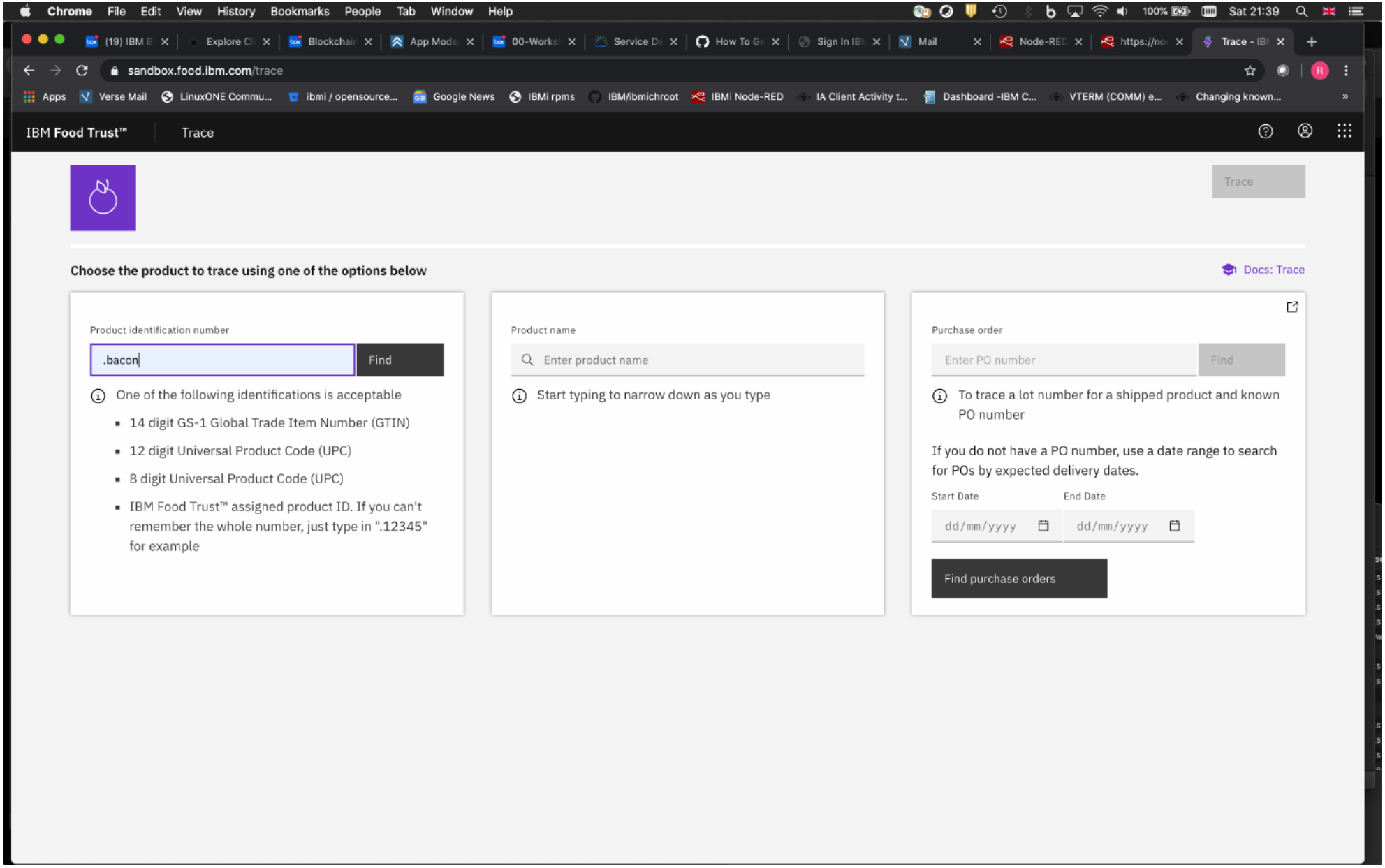

Chrome File Edit View History Bookmarks People Tab Window Help
sandbox.food.ibm.com/manage-data/products
IBM Food Trust™
Data
Access control
Products
Facilities
Download data
Products
Docs: Register products
Your Organization's products
61
All
Brandega foods
Customs
Diageo
Distributor
HPL
IBM CRP
Lettuce Supplier
Malcolm
Retailer
Smart Harvest
Smart Retailer
Smart Supplier
Warehouse
Product name
Product ID
Product name
Product ID
Retailer
Cabbage in retail pack
13460981800206
Retailer
bacon
34609818.bacon
Items per page: 10
1-2 of 2 items
1
of 1 pages

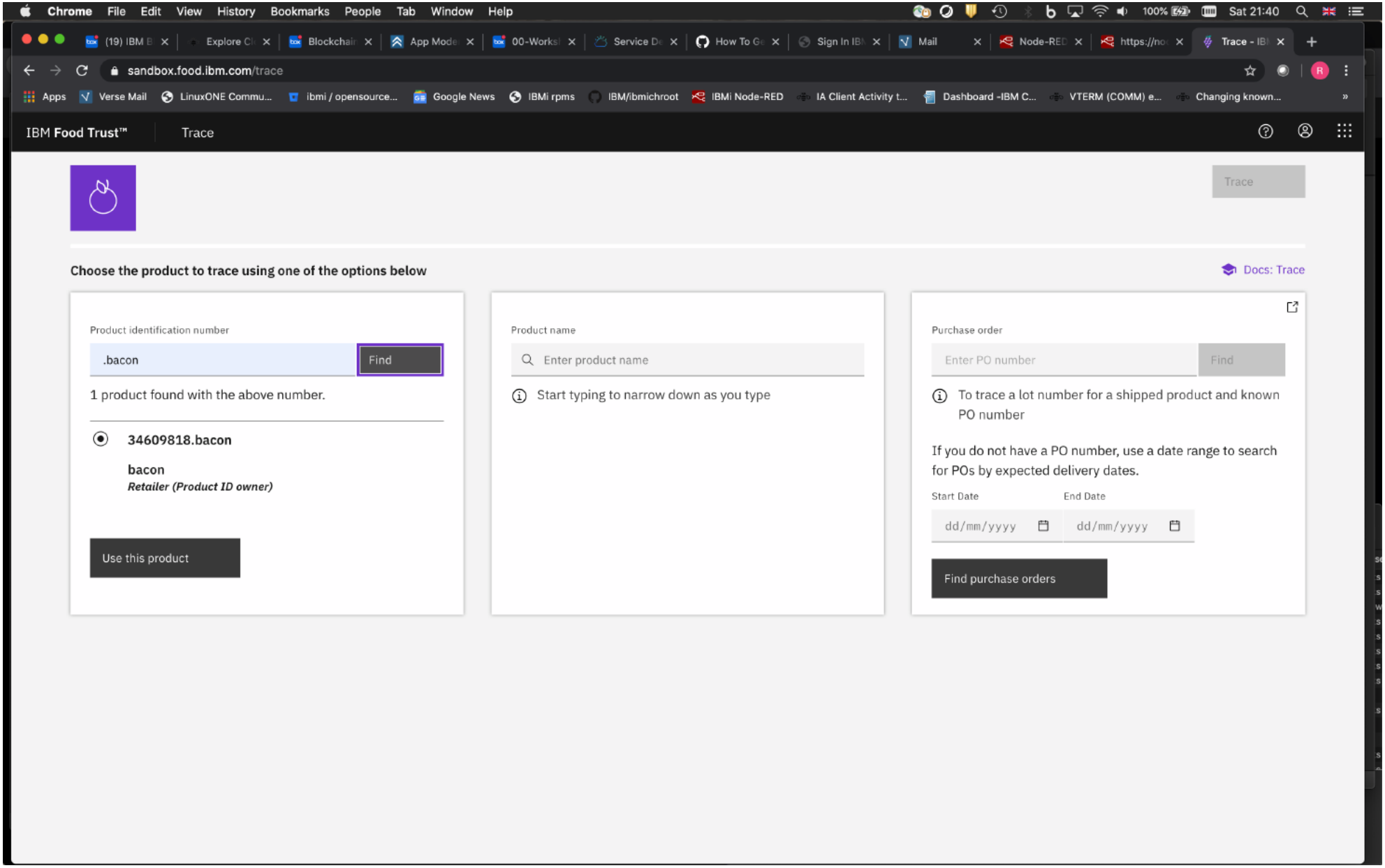

Chrome File Edit View History Bookmarks People Tab Window Help
Sat 21:38
sandbox.food.ibm.com/manage-data/products
IBM Food Trust™
Data
Access control
Products
Facilities
Download data
Products
Docs: Register products
Your Organization's products
61
List of registered products
Organization
Retailer
bacon
Product ID
bacon
Organization
Product name
Product ID
Retailer
bacon
34609818.bacon
Items per page: 10
1-1 of 1 items
1 of 1 pages

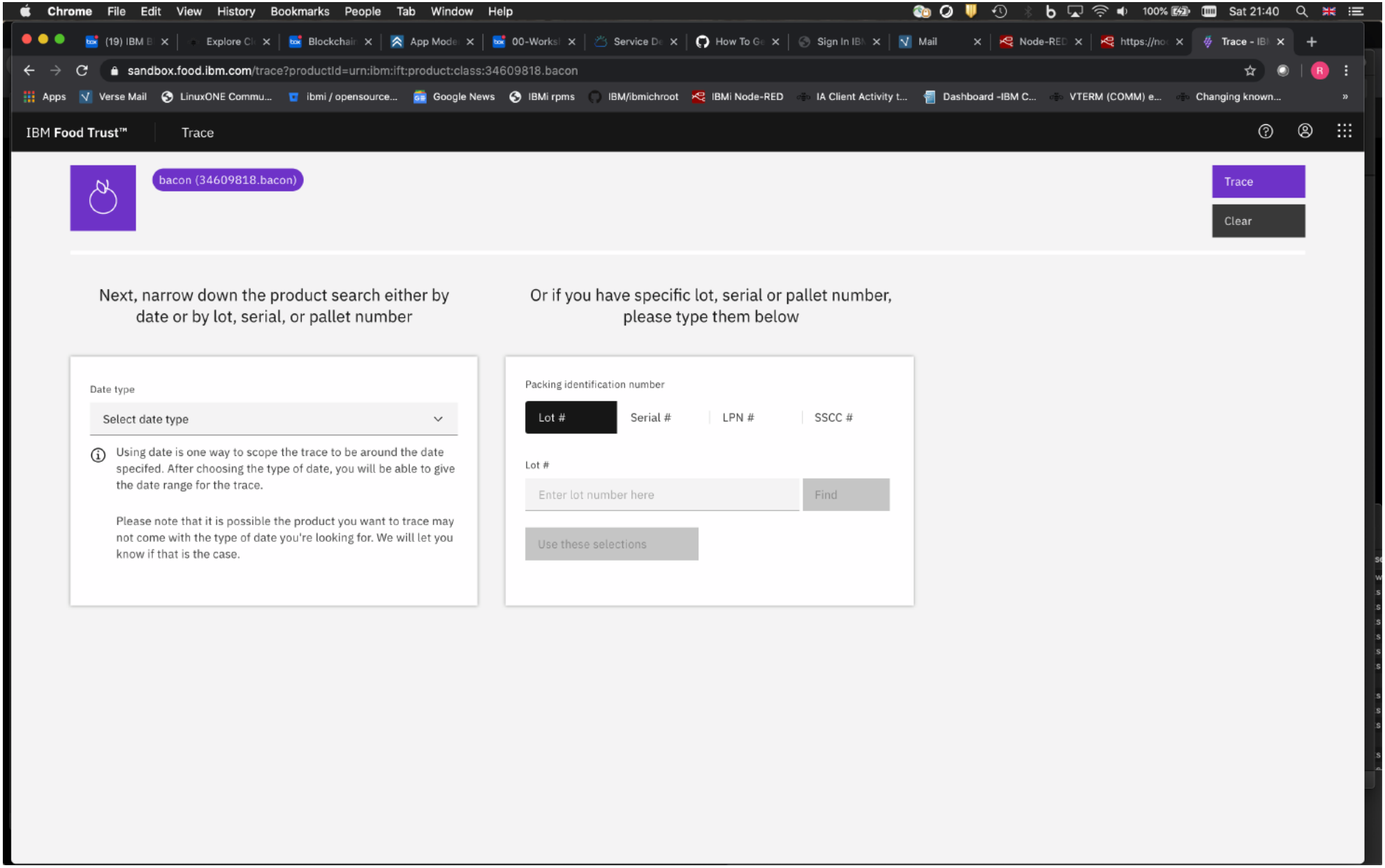

Chrome File Edit View History Bookmarks People Tab Window Help
sandbox.food.ibm.com/manage-data/products
IBM Food Trust™
Data
Access control
Products
Facilities
Download data
Products
Your Organization's products
61
List of registered products
Organization
Retailer
bacon
Product ID
Organization
Product name
Product ID
Retailer
bacon
34609818.bacon
Items per page: 10
1-1 of 1 items
Home
Activity
Data
Documents
Membership
Onboarding
Trace
Users
Trace
https://sandbox.food.ibm.com/trace

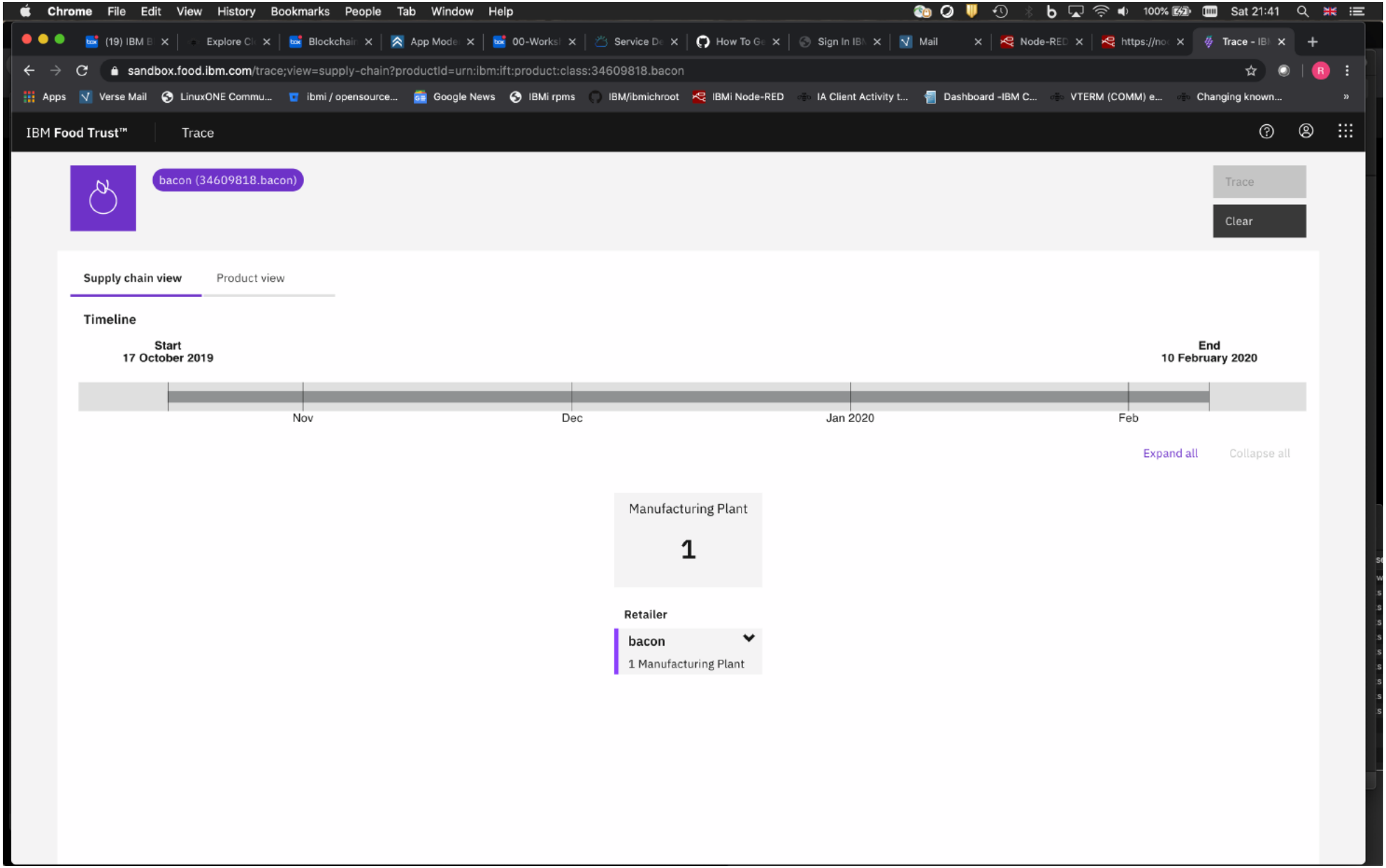

Chrome File Edit View History Bookmarks People Tab Window Help
Sat 21:39
sandbox.food.ibm.com/trace
Apps
Verse Mail
LinuxONE Commu...
ibmi / opensource...
Google News
IBMi rpms
IBM/ibmichroot
IBMi Node-RED
IA Client Activity t...
Dashboard -IBM C...
VTERM (COMM) e...
Changing known...
IBM Food Trust™
Trace
Start your trace with products

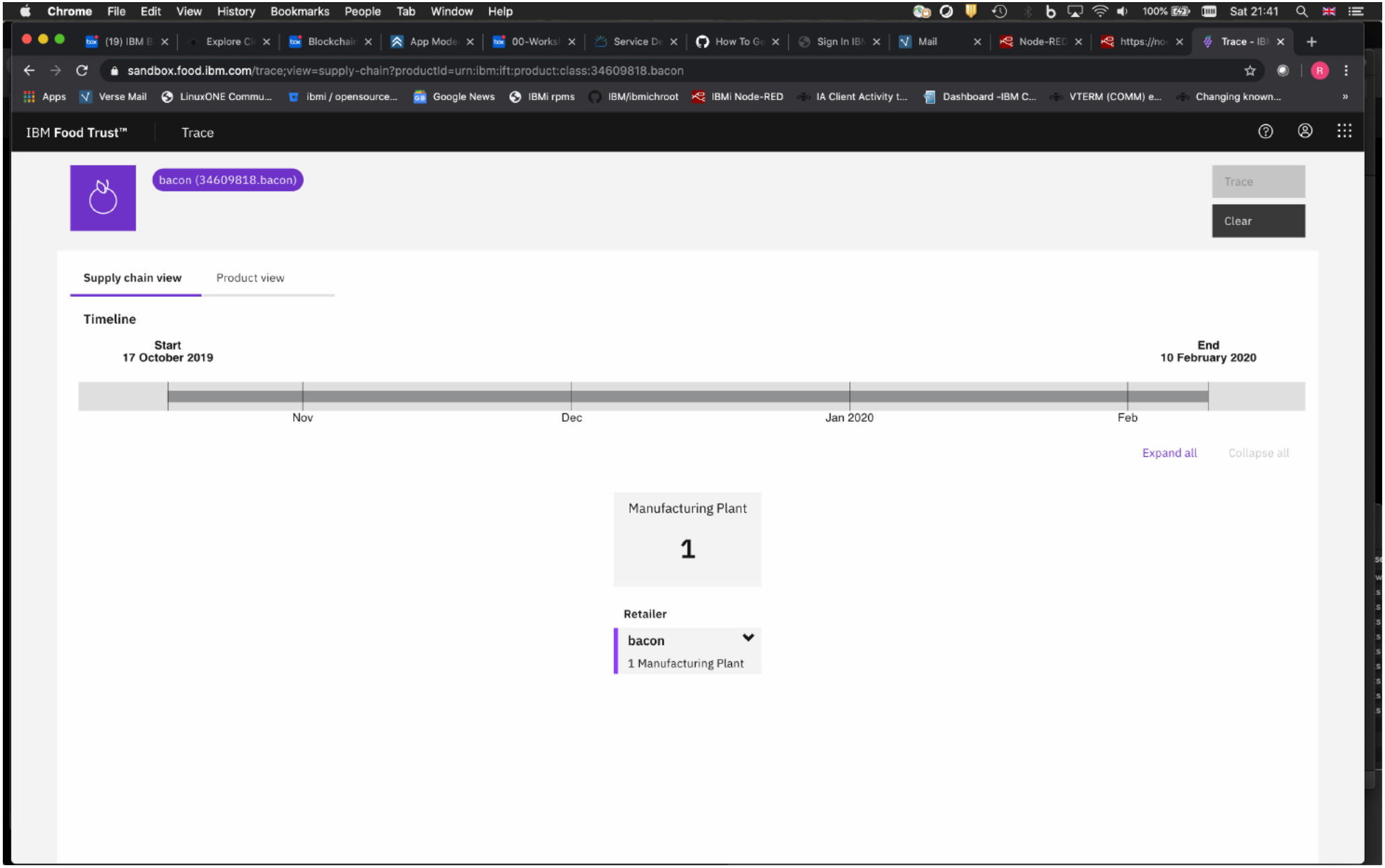

Chrome File Edit View History Bookmarks People Tab Window Help
Sat 21:39
sandbox.food.ibm.com/trace
IBM Food Trust™
Trace
Trace
Choose the product to trace using one of the options below
Docs: Trace
Product identification number
Enter product ID
Find
One of the following identifications is acceptable
14 digit GS-1 Global Trade Item Number (GTIN)
12 digit Universal Product Code (UPC)
8 digit Universal Product Code (UPC)
IBM Food Trust™ assigned product ID. If you can't remember the whole number, just type in ".12345" for example
Product name
Enter product name
Start typing to narrow down as you type
Purchase order
Enter PO number
Find
To trace a lot number for a shipped product and known PO number
If you do not have a PO number, use a date range to search for POs by expected delivery dates.
Start Date
End Date
dd/mm/yyyy
dd/mm/yyyy
Find purchase orders

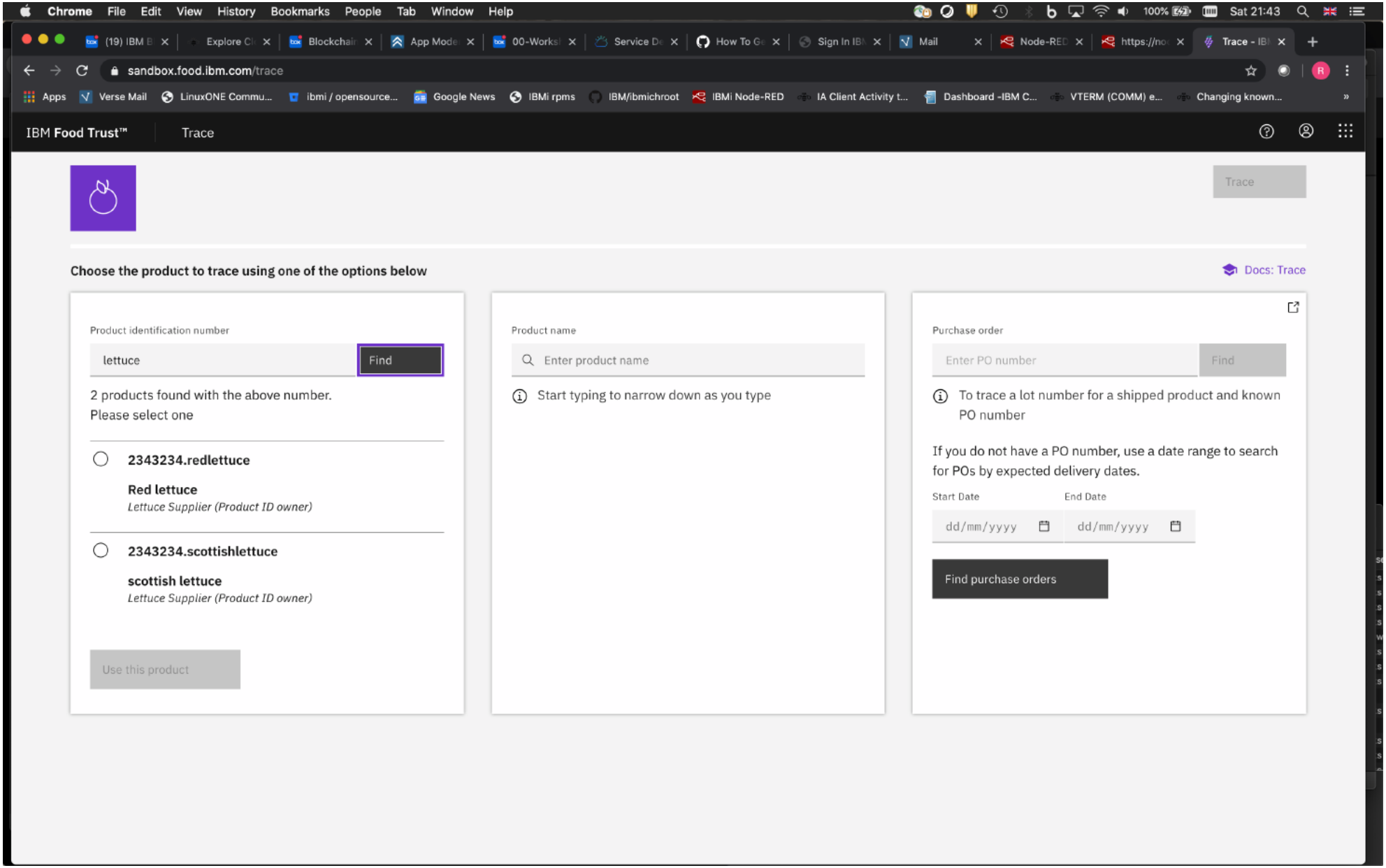

Chrome File Edit View History Bookmarks People Tab Window Help
Sat 21:39
sandbox.food.ibm.com/trace
IBM Food Trust™
Trace
Trace
Choose the product to trace using one of the options below
Docs: Trace
Product identification number
.bacon
Find
One of the following identifications is acceptable
14 digit GS-1 Global Trade Item Number (GTIN)
12 digit Universal Product Code (UPC)
8 digit Universal Product Code (UPC)
IBM Food Trust™ assigned product ID. If you can't remember the whole number, just type in ".12345" for example
Product name
Enter product name
Start typing to narrow down as you type
Purchase order
Enter PO number
Find
To trace a lot number for a shipped product and known PO number
If you do not have a PO number, use a date range to search for POs by expected delivery dates.
Start Date
End Date
dd/mm/yyyy
dd/mm/yyyy
Find purchase orders

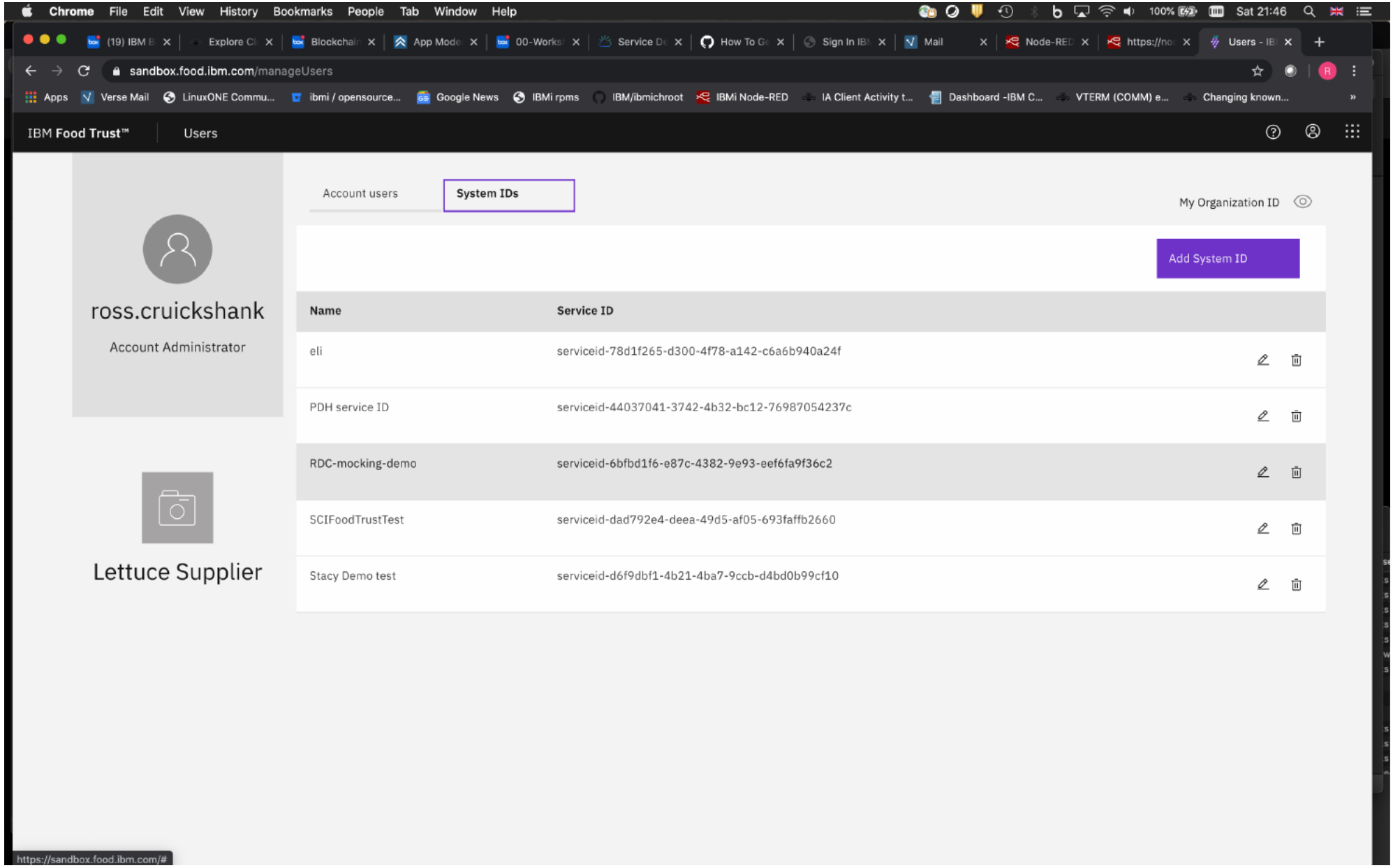

Chrome File Edit View History Bookmarks People Tab Window Help
Sat 21:40
sandbox.food.ibm.com/trace
IBM Food Trust™
Trace
Trace
Choose the product to trace using one of the options below
Docs: Trace
Product identification number
.bacon
Find
1 product found with the above number.
34609818.bacon
bacon
Retailer (Product ID owner)
Use this product
Product name
Enter product name
Start typing to narrow down as you type
Purchase order
Enter PO number
Find
To trace a lot number for a shipped product and known PO number
If you do not have a PO number, use a date range to search for POs by expected delivery dates.
Start Date
End Date
dd/mm/yyyy
dd/mm/yyyy
Find purchase orders

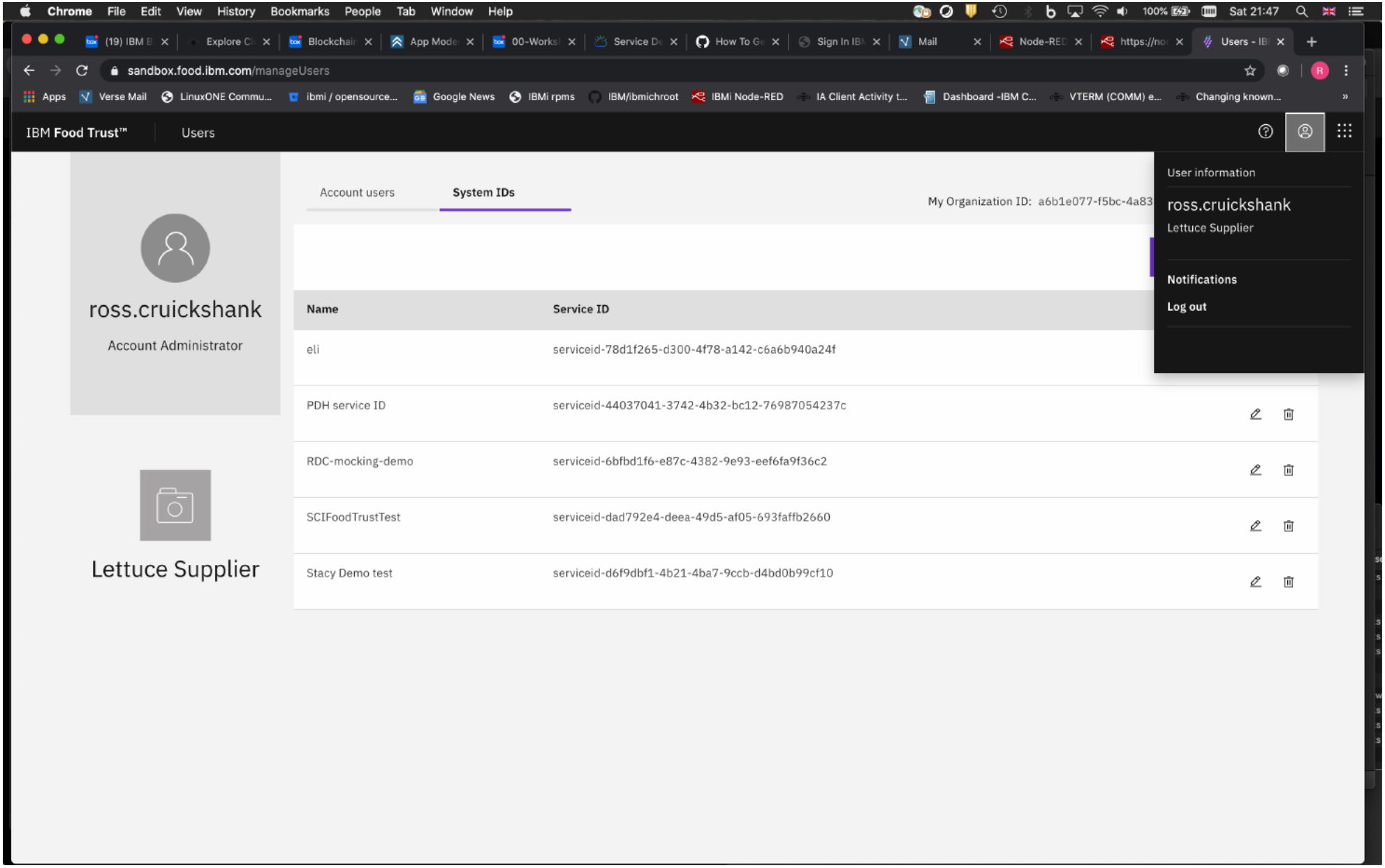

Chrome File Edit View History Bookmarks People Tab Window Help
sandbox.food.ibm.com/trace?productId=urn:ibm:ift:product:class:34609818.bacon
IBM Food Trust™
Trace
bacon (34609818.bacon)
Trace
Clear
Next, narrow down the product search either by date or by lot, serial, or pallet number
Or if you have specific lot, serial or pallet number, please type them below
Date type
Select date type
Using date is one way to scope the trace to be around the date specifed. After choosing the type of date, you will be able to give the date range for the trace.
Please note that it is possible the product you want to trace may not come with the type of date you're looking for. We will let you know if that is the case.
Packing identification number
Lot #
Serial #
LPN #
SSCC #
Lot #
Enter lot number here
Find
Use these selections

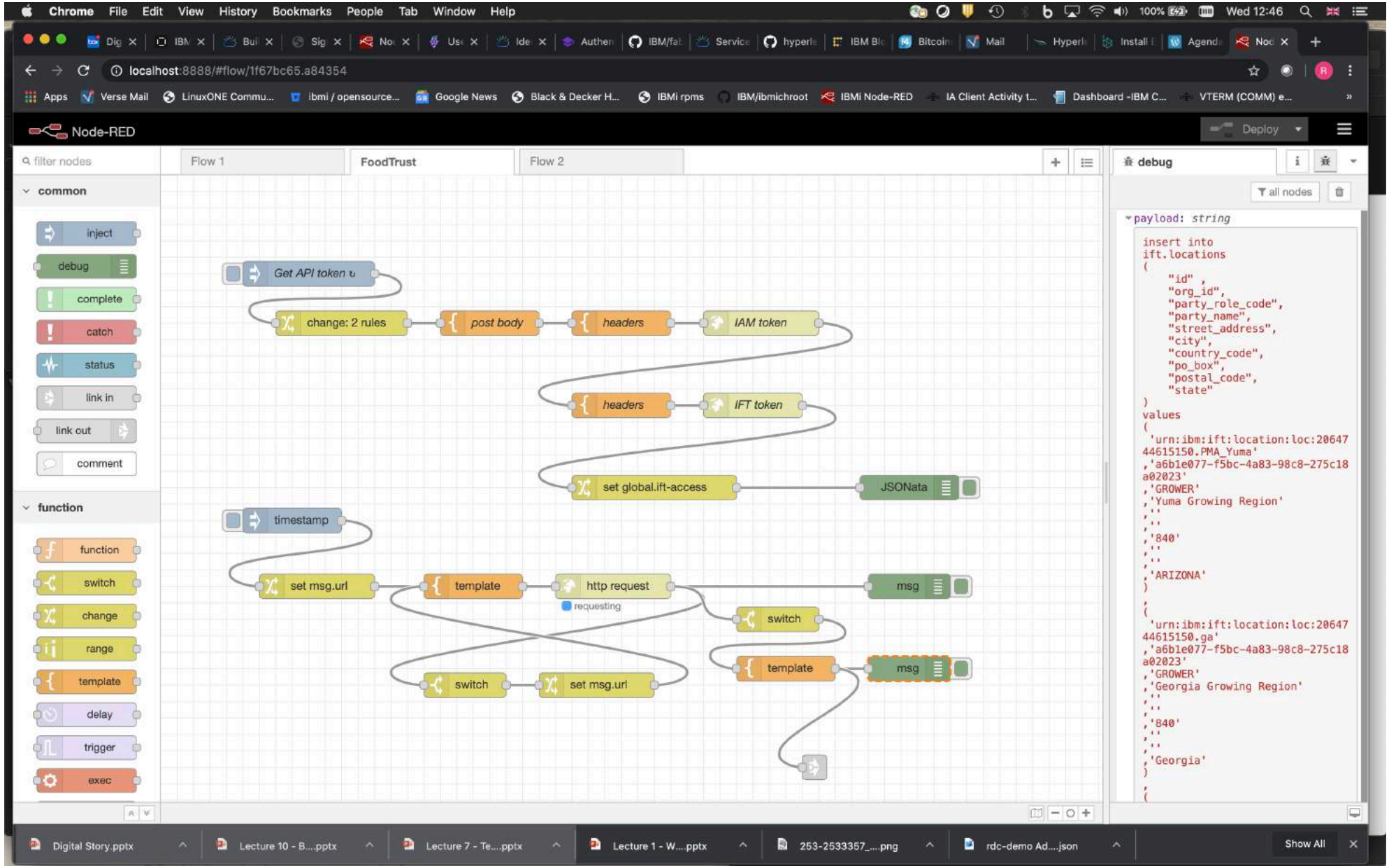

Chrome File Edit View History Bookmarks People Tab Window Help
Sat 21:41
sandbox.food.ibm.com/trace;view=supply-chain?productId=urn:ibm:ift:product:class:34609818.bacon
IBM Food Trust™
Trace
bacon (34609818.bacon)
Trace
Clear
Supply chain view
Product view
Timeline
Start
17 October 2019
End
10 February 2020
Nov
Dec
Jan 2020
Feb
Expand all
Collapse all
Manufacturing Plant
1
Retailer
bacon
1 Manufacturing Plant


Chrome File Edit View History Bookmarks People Tab Window Help
Sat 21:41
sandbox.food.ibm.com/trace;view=supply-chain?productId=urn:ibm:ift:product:class:34609818.bacon
IBM Food Trust™
Trace
bacon (34609818.bacon)
Trace
Clear
Supply chain view
Product view
Timeline
Start
17 October 2019
End
10 February 2020
Nov
Dec
Jan 2020
Feb
Expand all
Collapse all
Manufacturing Plant
1
Retailer
bacon
1 Manufacturing Plant


Chrome File Edit View History Bookmarks People Tab Window Help
Sat 21:43
sandbox.food.ibm.com/trace
IBM Food Trust™
Trace
Trace
Choose the product to trace using one of the options below
Docs: Trace
Product identification number
lettuce
Find
2 products found with the above number.
Please select one
2343234.redlettuce
Red lettuce
Lettuce Supplier (Product ID owner)
2343234.scottishlettuce
scottish lettuce
Lettuce Supplier (Product ID owner)
Use this product
Product name
Enter product name
Start typing to narrow down as you type
Purchase order
Enter PO number
Find
To trace a lot number for a shipped product and known PO number
If you do not have a PO number, use a date range to search for POs by expected delivery dates.
Start Date
End Date
dd/mm/yyyy
dd/mm/yyyy
Find purchase orders


Chrome File Edit View History Bookmarks People Tab Window Help
sandbox.food.ibm.com/manageUsers
IBM Food Trust™
Users
Account users
System IDs
My Organization ID
Add System ID
ross.cruickshank
Account Administrator
Lettuce Supplier
Name
Service ID
eli
serviceid-78d1f265-d300-4f78-a142-c6a6b940a24f
PDH service ID
serviceid-44037041-3742-4b32-bc12-76987054237c
RDC-mocking-demo
serviceid-6bfbd1f6-e87c-4382-9e93-eef6fa9f36c2
SCIFoodTrustTest
serviceid-dad792e4-deea-49d5-af05-693faffb2660
Stacy Demo test
serviceid-d6f9dbf1-4b21-4ba7-9ccb-d4bd0b99cf10
https://sandbox.food.ibm.com/#


Chrome File Edit View History Bookmarks People Tab Window Help
Sat 21:47
sandbox.food.ibm.com/manageUsers
IBM Food Trust™
Users
Account users
System IDs
My Organization ID: a6b1e077-f5bc-4a83
User information
ross.cruickshank
Lettuce Supplier
Notifications
Log out
ross.cruickshank
Account Administrator
Lettuce Supplier
Name
Service ID
eli
serviceid-78d1f265-d300-4f78-a142-c6a6b940a24f
PDH service ID
serviceid-44037041-3742-4b32-bc12-76987054237c
RDC-mocking-demo
serviceid-6bfbd1f6-e87c-4382-9e93-eef6fa9f36c2
SCIFoodTrustTest
serviceid-dad792e4-deea-49d5-af05-693faffb2660
Stacy Demo test
serviceid-d6f9dbf1-4b21-4ba7-9ccb-d4bd0b99cf10


Chrome File Edit View History Bookmarks People Tab Window Help
Wed 12:46
localhost:8888/#flow/1f67bc65.a84354
Node-RED
Deploy
filter nodes
Flow 1
FoodTrust
Flow 2
common
inject
debug
complete
catch
status
link in
link out
comment
function
function
switch
change
range
template
delay
trigger
exec
Get API token
change: 2 rules
post body
headers
IAM token
headers
IFT token
set global.ift-access
JSONata
timestamp
set msg.url
template
http request
requesting
msg
switch
template
msg
switch
set msg.url
debug
all nodes
payload: string
insert into
ift.locations
(
"id" ,
"org_id",
"party_role_code",
"party_name",
"street_address",
"city",
"country_code",
"po_box",
"postal_code",
"state"
)
values
(
'urn:ibm:ift:location:loc:20647
44615150.PMA_Yuma'
,'a6b1e077-f5bc-4a83-98c8-275c18
a02023'
,'GROWER'
,'Yuma Growing Region'
,''
,''
,'840'
,''
,''
,'ARIZONA'
)
,
(
'urn:ibm:ift:location:loc:20647
44615150.ga'
,'a6b1e077-f5bc-4a83-98c8-275c18
a02023'
,'GROWER'
,'Georgia Growing Region'
,''
,''
,'840'
,''
,''
,'Georgia'
)
,
(
Digital Story.pptx
Lecture 10 - B....pptx
Lecture 7 - Te....pptx
Lecture 1 - W....pptx
253-2533357_....png
rdc-demo Ad....json
Show All

IBM Solutions

- Food Trust
- TradeLens
- World Wire
- Trust Your Supplier
- Digital Identity

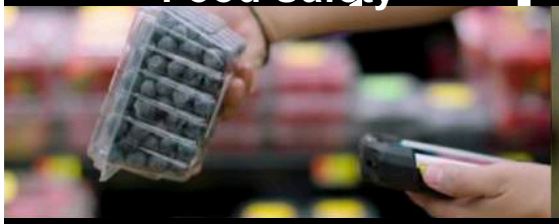
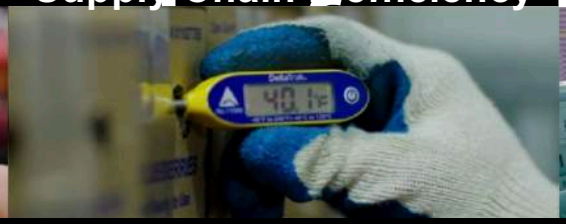
Your Solution

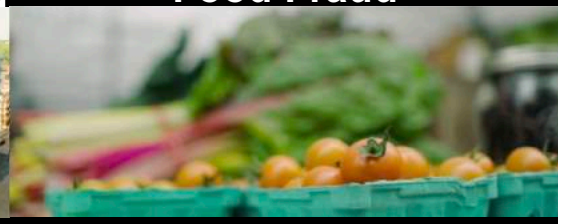
IBM Food Trust

- Overview

Only 1 in 4 consumers trust

Food Safety | **Supply Chain Inefficiency** | **Food Waste** | **Food Fraud**



1 out of 10
people get sick each year, and 420,000 die from foodborne illness

80%
of CPGs business are partially or entirely paper-based

1 / 3
of fresh food is thrown out because it is considered unacceptable

1 in 5
seafood samples is mislabeled worldwide

(43% mislabeled in NYC)

The root of these issues, and many others, are the lack of trust and transparency

IBM
ibm.com/food

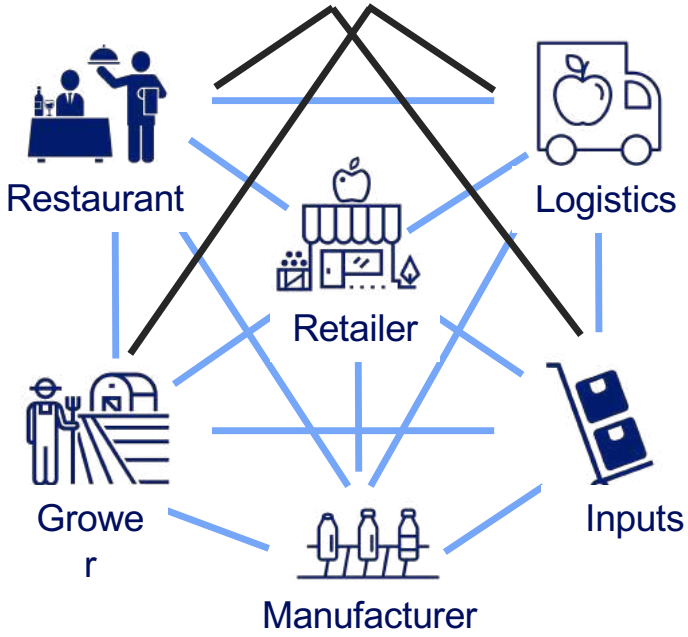
Sources: World Health Organization, Gravitas Study, FAO of UN, Oceana

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

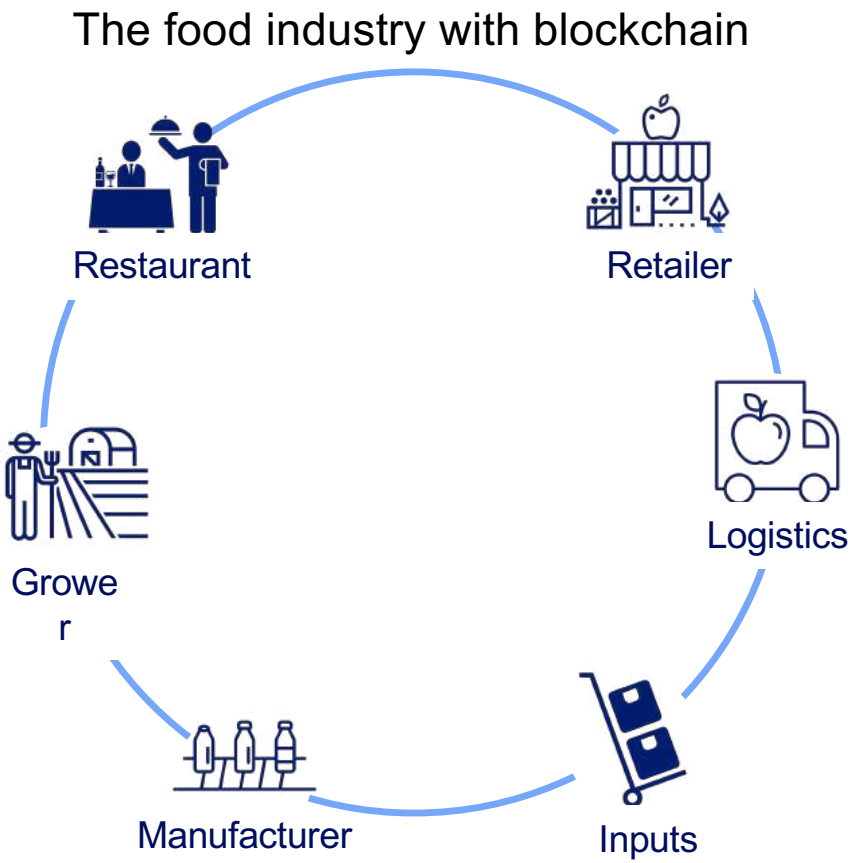
The food industry today



Blockchain transforms systems with trust and transparency

The Solution:

- Because blockchain provides an independent data-sharing platform, participants trust it
- 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



An open, distributed blockchain model

Distributed Nodes & Smart Contracts
Clients using IBM Food Trust data to express unique business logic

Open APIs
Open data to enable ecosystem clients and partners to build customization with IBM Food Trust

Nodes anywhere
Flexibility with nodes in hybrid cloud environments for running Smart Contracts

Interoperability
Supported through Smart Contracts, integrate and connect data across networks and other infrastructure

Trust Anchors
IBM Food Trust participants that are endorsing, validating, and securing the network

Building a blockchain-enabled business solution requires more than blockchain

Blockchain-Enabled Business Solution

Business Value

Designed so every participant can see a positive ROI

Ecosystem

Walmart
Save money. Live better.

Nestlé

Driscoll's
Only the Finest Berries

gsf

Carrefour

Open to all participants in the food ecosystem

Governance Model

Built and maintained with the collaboration of industry thought leaders

- Data Ownership
- Membership
- Trust Model
- Interoperability
- 3rd Parties
- And more

Standards & Interoperability

GS1

EDI

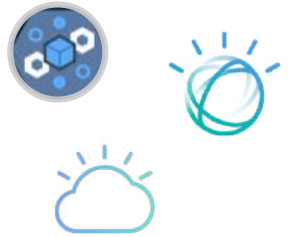
HYPERLEDGER

- Industry standards
- Data management systems
- Open APIs
- Cloud agnostic
- Current and future blockchain solutions

Technology

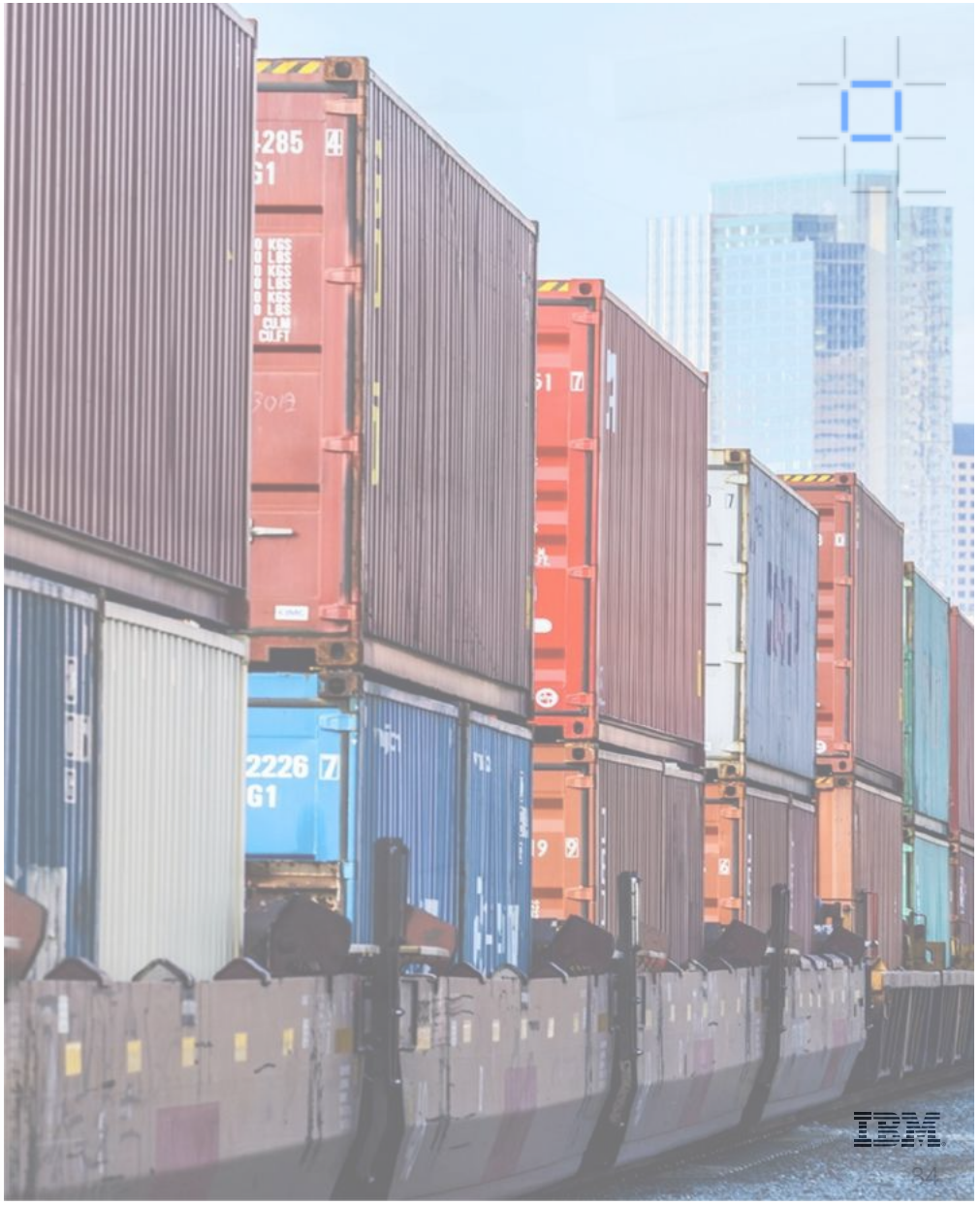
Innovative enterprise-class technology:

- Security / Privacy
- Reliability
- Scalability
- Resilience
- Auditability



TRADELENS

IBM **Blockchain**



TRADE MADE EASY

TradeLens is ushering in a new era in global supply chains—one where all parties can collaborate, share data, and realize the benefits of digitization.

TradeLens is fundamentally improving the most frustrating parts of container logistics – document handling, consignment visibility and shipment workflows within and across the supply chain.

GLOBAL TRADE IN NUMBERS

$16+ TRILLION IN GOODS

Are shipped across international borders each year

80% OF THE GOODS

Consumers use daily are carried by the ocean shipping industry

GLOBAL TRADE INCREASE OF 15%

If barriers within the international supply chain were reduced

WTO estimates suggest that improvements in data and document-handling could unlock more than

$4 TRILLION OF GLOBAL ECONOMIC GROWTH

GLOBAL TRADE IS HIGHLY INEFFICIENT AND BURDENED BY PAPER-BASED PROCESSES

+ **Data trapped in organizational silos**

  Information is held in paper and various digital formats across dozens of service providers along the supply chain, requiring complex, cumbersome, and costly peer-to-peer messaging. The result is inconsistent information across organizational boundaries, latency in obtaining shipment visibility, and blind spots that hinder the efficient flow of goods.

+ **Manual, time-consuming, paper-based processes**

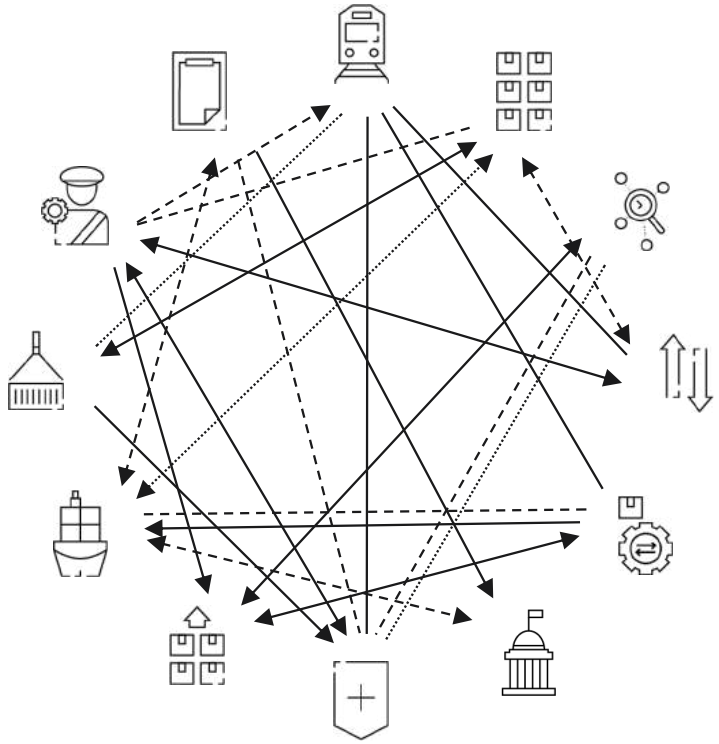
  The collection and processing of up-to-date data, as well as inefficient trade document exchange, requires manual checks and frequent follow-ups and results in errors, delays and high compliance costs. Late filings are common due to missing information.

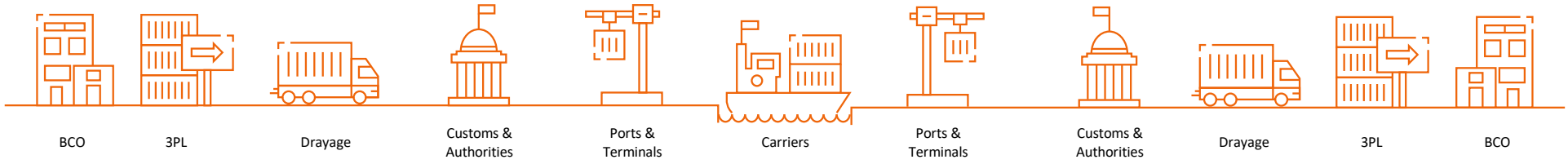
+ **Clearance takes too long and is often subject to fraud**

  Risk assessments by customs authorities lack sufficient and trusted information resulting in high inspection rates, added prevention measures against fraud and forgery, and delayed customs clearance.

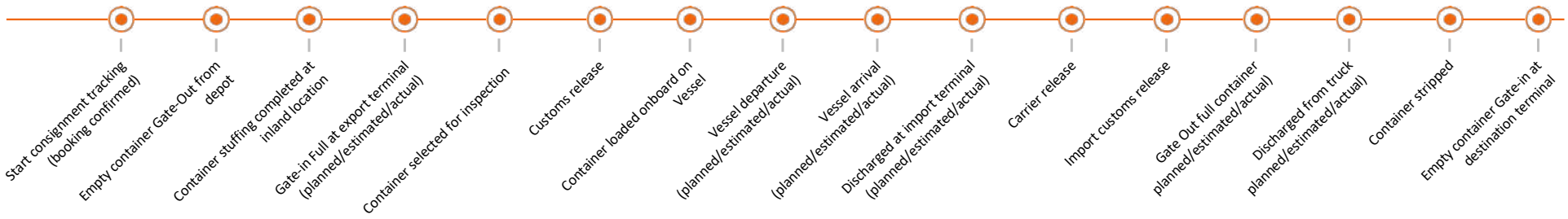
+ **High costs and poor customer service**

  These challenges have significant downstream repercussions. The inability to forecast and plan effectively, address supply chain disruptions in near real-time, and share trusted information across the supply chain leads to excessive safety stock inventory, high administrative costs, operational challenges, and ultimately poor customer service.





SHIPPING MILESTONES AND SHIPMENT DATA*

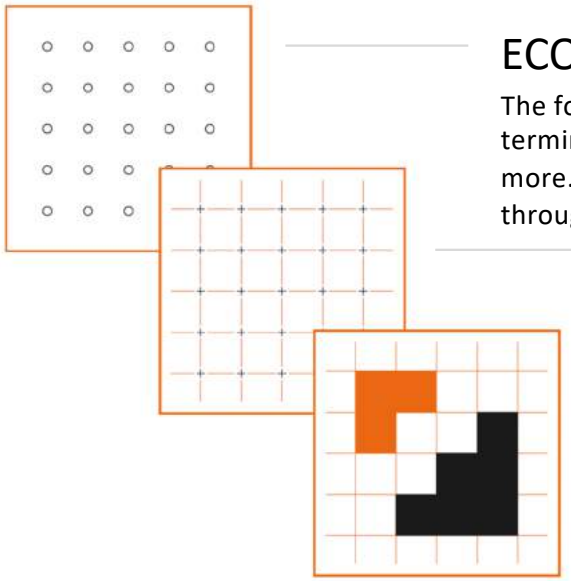


STRUCTURED AND UNSTRUCTURED DOCUMENTS*

TRADELENS BLOCKCHAIN BUSINESS NETWORK

* Note: representative sample only of the data on the platform

THE TRADELENS SOLUTION



ECOSYSTEM

The foundation of TradeLens is its business network — shippers, freight forwarders, ports and terminals, ocean carriers, intermodal operators, government authorities, customs brokers and more. Each entity shares information that can be tracked, stored and actioned across the platform throughout a shipment's journey.

PLATFORM

The TradeLens Platform is accessible via an open API and brings together the ecosystem through a set of open standards. Powered by Hyperledger Fabric blockchain technology and IBM Cloud, the platform enables the industry to share information and collaborate securely.

MARKETPLACE

An open Applications and Services Marketplace allows both TradeLens and third parties to publish fit-for-purpose services atop the TradeLens platform, fostering supply chain innovation and value creation.

THE IMPORTANCE OF DATA TRANSFORMATION

Few would disagree that the data in today's supply chains are too often of poor quality, inconsistent, late, incomplete, or unavailable. TradeLens is looking to change that.

Characteristics underpinning data transformation:

1. Data should be accurate and complete and available in near real-time
2. Data should originate directly from the source whenever possible
3. The exchange of data across parties should be simple and standardized
4. Data needs to be secured and protected
5. Non-sensitive data should be shared more readily

What is needed to get there:

1. Adoption of standards is a must
2. Industry-wide standards for data governance and exchange are critical
3. Data governance must be supported by all industry platforms
4. ***Movement away from EDI and towards API is critical***
5. All supply chain partners must acknowledge responsibility and commit to data cleanup (garbage in / garbage out)
6. Dynamic and automated data quality feedback loops needs to be put into place

ECOSYSTEM DATA

Foundational data

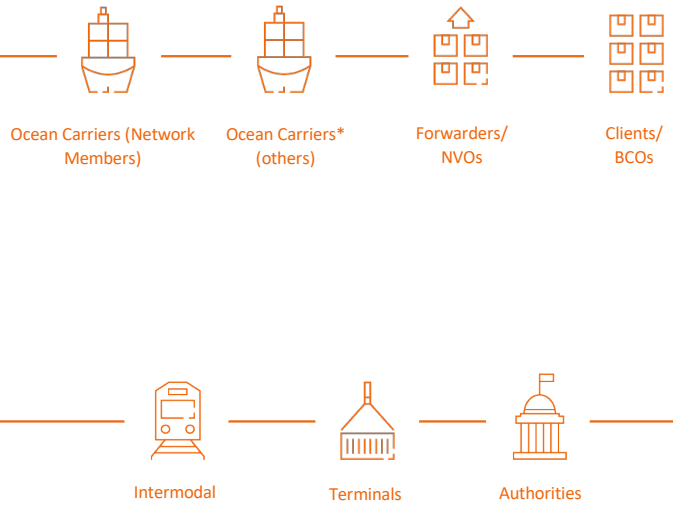
The data and documents to track and manage shipments end-to-end

+ More than half of global container shipping volume committed
+ Vast number of trade lanes covered
+ **20+ Million containers per year today**

Enrichment data

Supplements foundational data, in near real-time and direct from the source

+ Rapidly growing network
+ Extensive port/terminal coverage



TRADELENS

700M Events
per year

5.5M Documents
per year

These figures are estimated to double with the recent addition of major ocean carriers to the ecosystem

* Ocean carriers who are not Network Members can provide data as requested by their customers

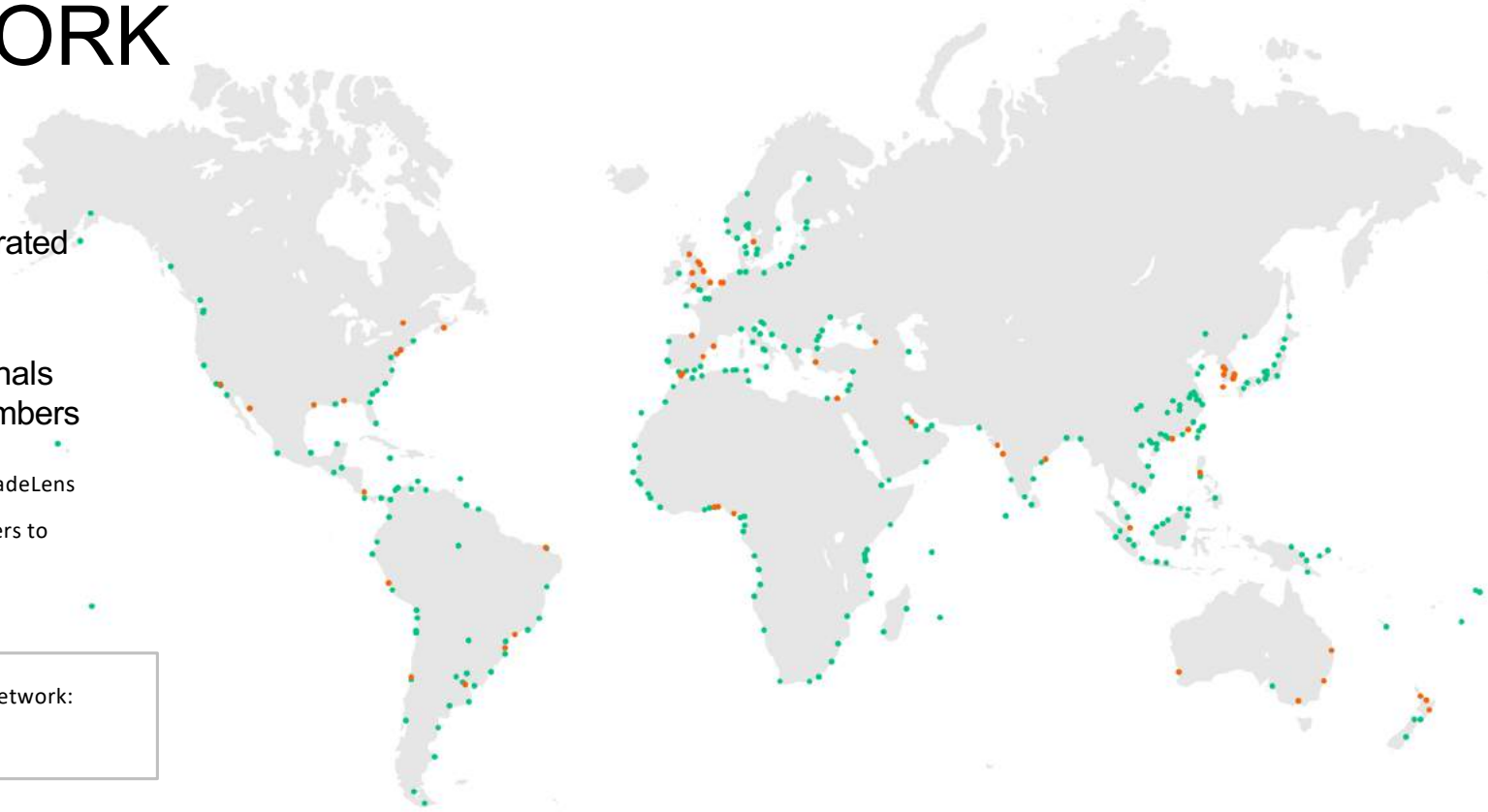
THE TRADELENS PORT AND TERMINAL NETWORK

Coverage across 6 continents

80 ports and terminals directly integrated with TradeLens

Data from up to 600 ports and terminals captured by existing TradeLens members

- Ports and terminals directly integrated with TradeLens
- Ports and terminals contributing data via carriers to TradeLens



Interactive map of TradeLens port and terminal network:

https://www.tradelens.com/ecosystem/

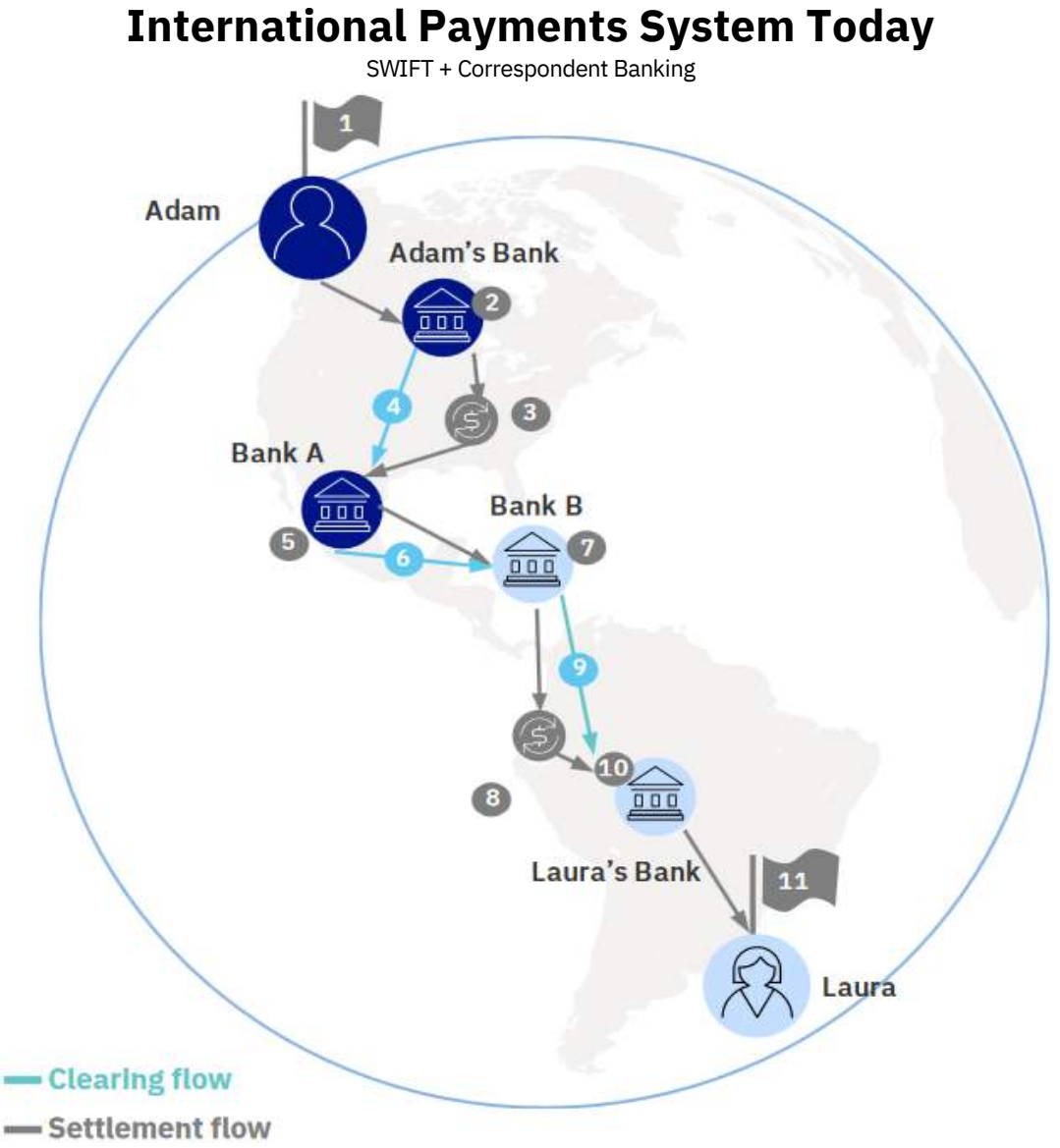

World Wire
Introduced Spring 2019
The new normal in global payments
IBM

Cross-border payments today remain costly, complex and slow

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

The Challenges

- 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.
- 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.
- 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.
- 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.



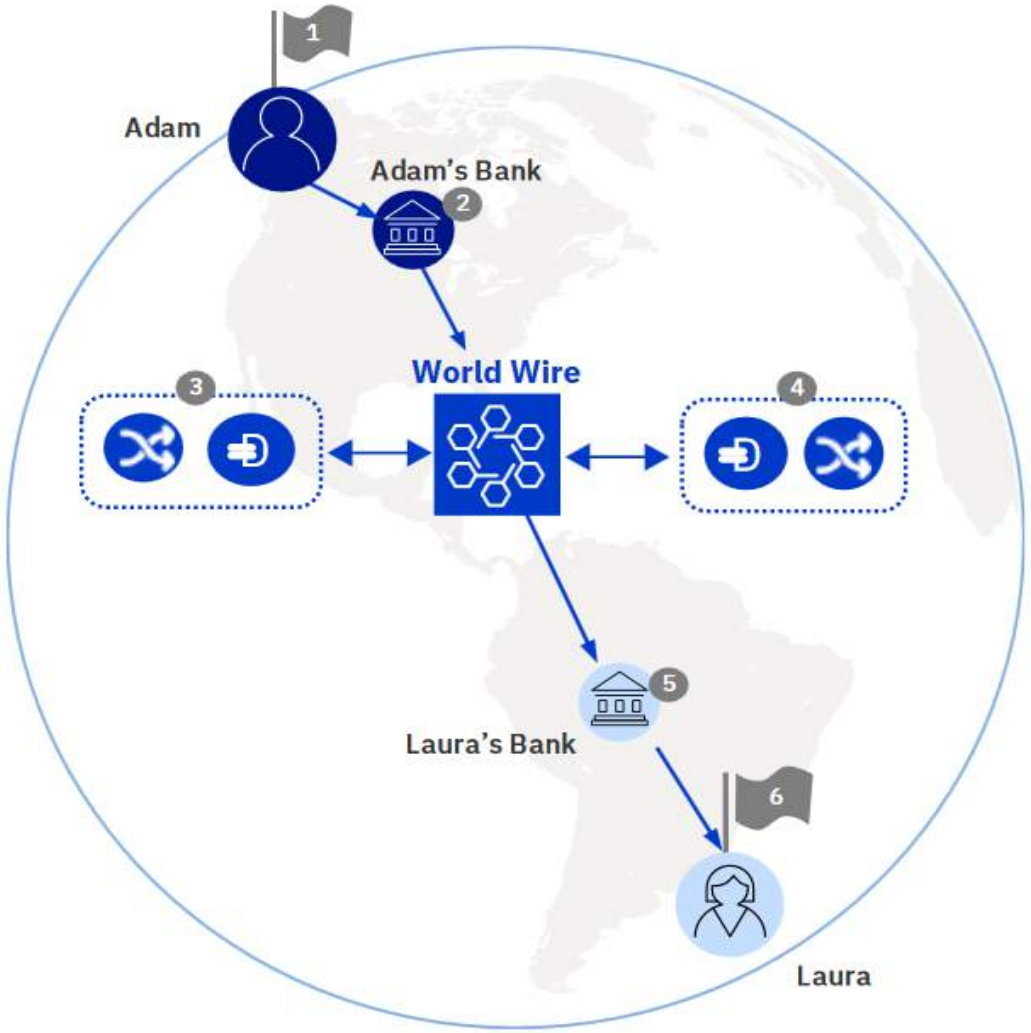
World Wire simplifies clearing & settlement to streamline cross-border payments

Faster, Cheaper & More efficient

World Wire targets industry pain points

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

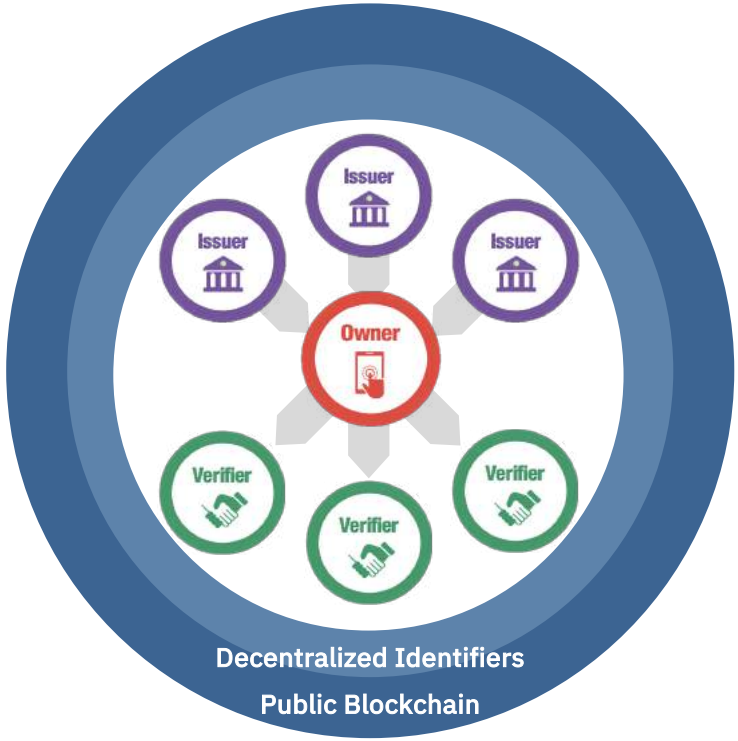
International Payments with World Wire



Clearing and settlement flow

Sovrin is a self-sovereign identity network

- Sovrin pushes identity to the **edge of the network**
- A decentralized approach that establishes trust and puts the **end user** in control
  - Every person, organization, and thing has a digital wallet to control the flow of their identity
  - No PII is stored on the public ledger!
- Cryptographic, point to point exchange of identity
  - Based on **Hyperledger Indy** technology



sovrin
identity for all

Sovrin Identity Concepts

Decentralized Identifier (DIDs)

- User owned and governed
- New type of identifier for verifiable, self sovereign identity
- Fully under the control of person, institution, or thing
- URL to relate an identity for a trusted interaction with a subject
- Standardization for universal identifiers

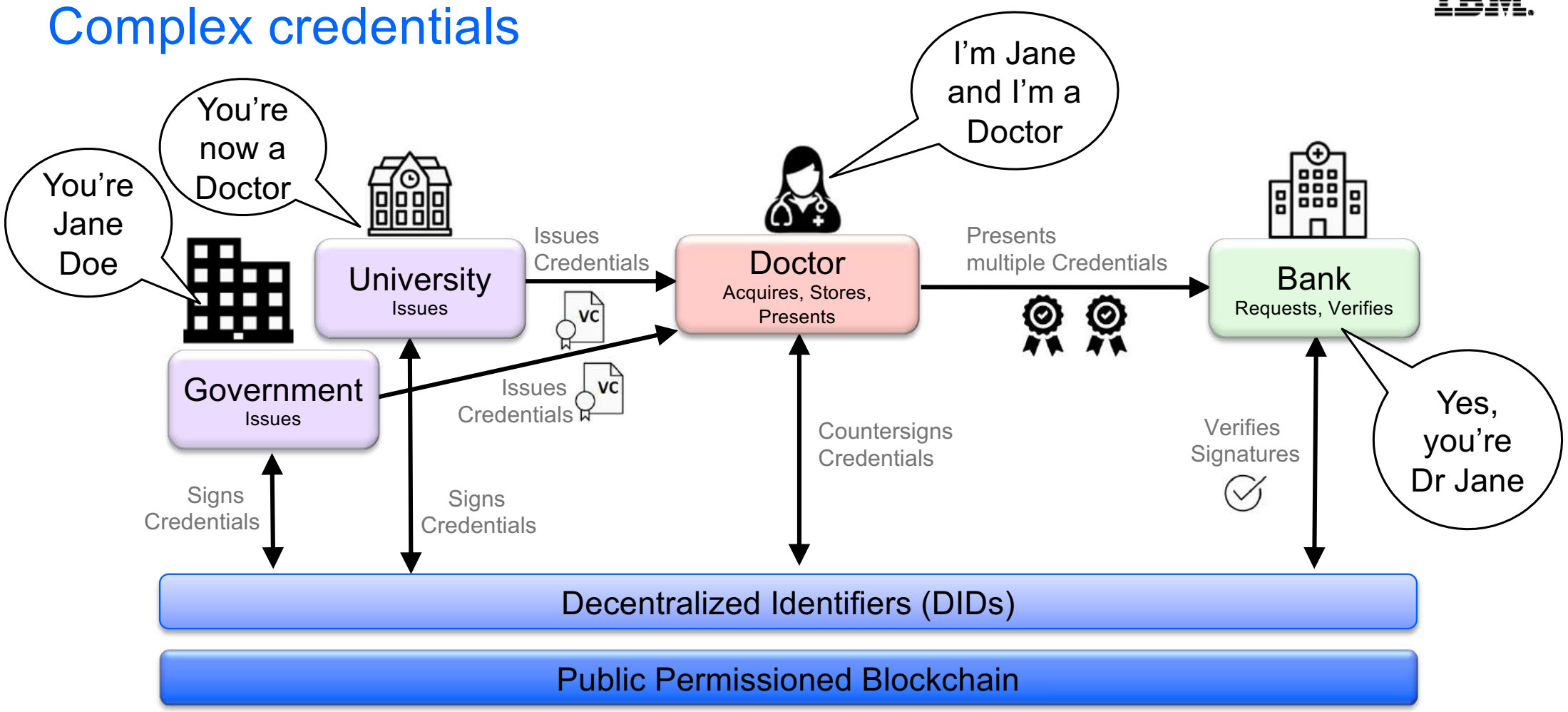
Verifiable Credentials

- Cryptographically backed statements of truth
- Standard way of defining, exchanging, and verifying digital information
- Ecosystem of issuers, verifiers, and owners

Decentralized Key Management

- User permissioning
- Entities own their own keys and have a “public key” ring for those they interact with
- “Public key” rings are used to resolve and verify interactions through DIDs

Complex credentials



IBM Solutions

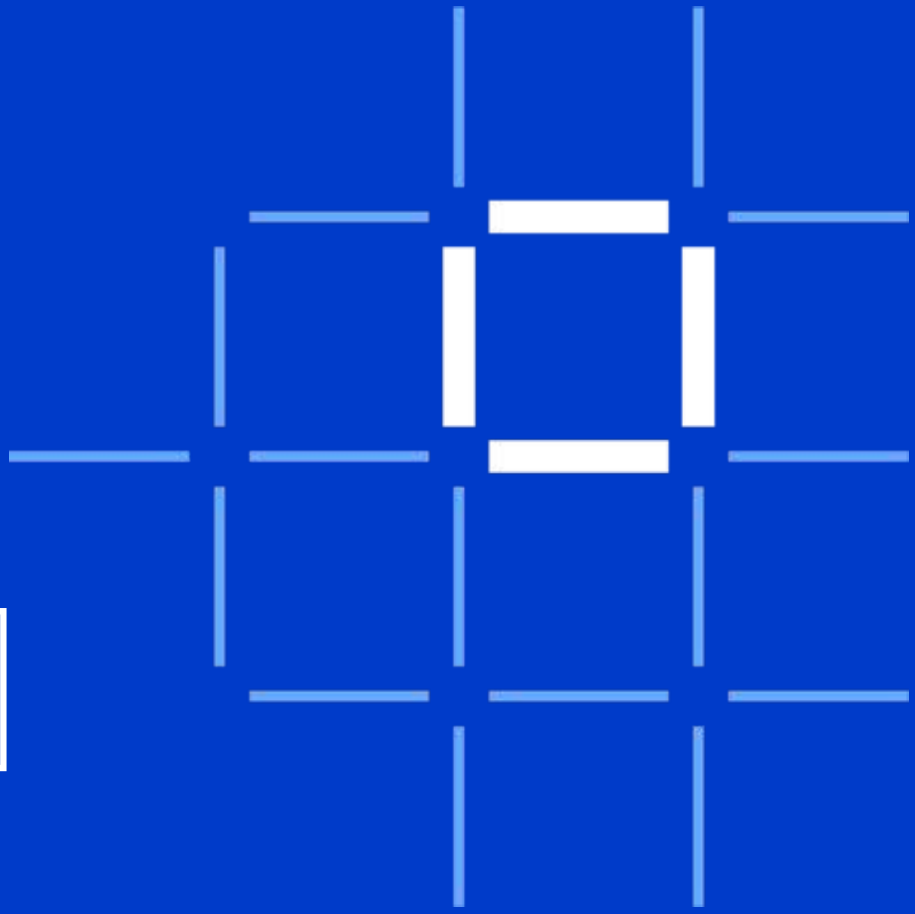
- Food Trust
- TradeLens
- World Wire
- Digital Identity

Your Solution

Blockchain introduction

Solutions Overview

IBMi and Blockchain



Good blockchain use-case or bad?

Food Provenance

Holiday Tracking Tool

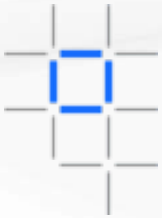
Know Your Customer

Secure Document Store

Track Your Child

Electronic Medical Records

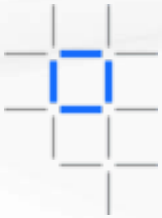
What makes a good business blockchain use case?



- Identifying a good blockchain use-case is not always easy!
  - However there should always be:

1. A business problem to be solved
   - That cannot be more efficiently solved with other technologies
2. An identifiable business network
   - With Participants, Assets and Transactions
3. A need for trust
   - Consensus, Immutability, Finality or Provenance

What makes a good first blockchain use case?

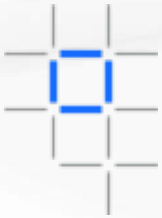


– First use-cases are even more difficult to identify!

1. A limited scope, but still solves a real business problem
   - Minimum Viable Product in a few weeks of effort
2. A smaller business network
   - Usually without requiring regulators and consortia
3. Allows for scaling with more participants and scenarios
   - Consider shadow chains to mitigate risks

Start small, succeed and grow fast!

Sample questions to ask for the selected use case:



1. What is the specific business problem / challenge that the first project will address?
2. What is the current way of solving this business problem?
3. Assuming the business problem is large, what specific aspects of this business problem will be addressed?
4. Who are the business network participants (organizations) involved and what are their roles?
5. Who are the specific people within the organization and what are their job roles?
6. What assets are involved and what is the key information associated with the assets?
7. What are the transactions involved, between whom, and what assets are associated with transactions?
8. What are the main steps in the current workflow and how are these executed by the business network participants?
9. What is the expected benefit of applying blockchain technology to the business problem for each of the network participants?
10. What legacy systems are involved? What degree of integration with the legacy systems is needed?

Off the shelf blockchain – things to remember

Hyperledger Fabric

- Open source platform/peer capability
- Based on Go lang
- No current support for golang in PASE

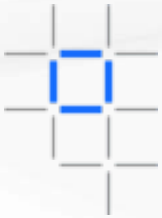
Hyperledger Besu

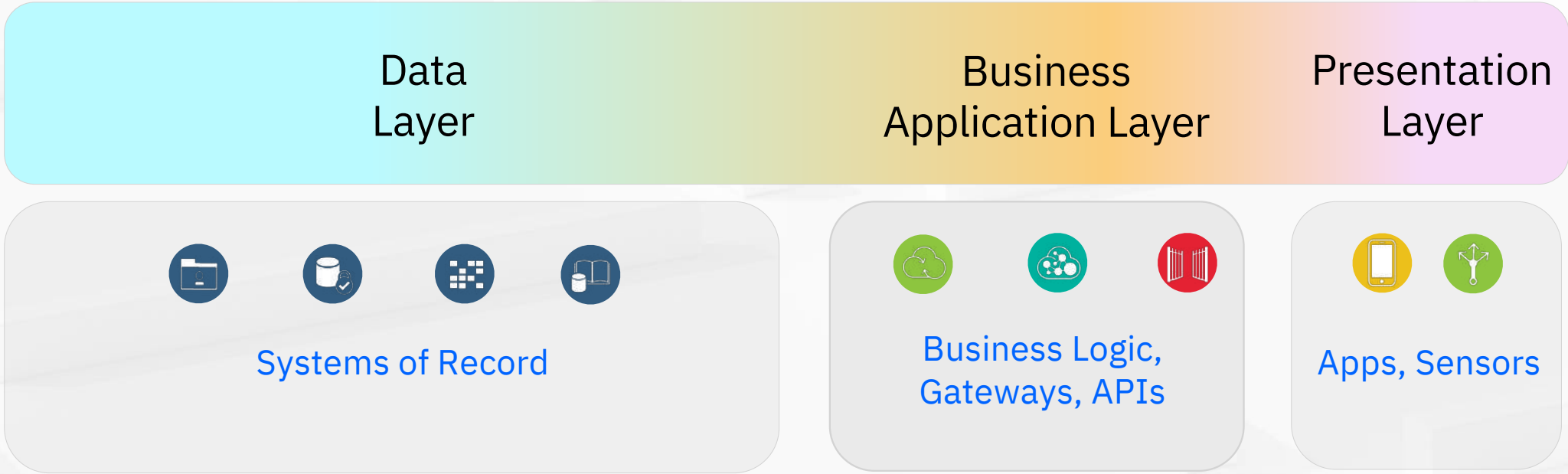
- Node.js client for Ethereum networks
- Requires JDK 1.11
- No current support > 1.8
- Rocksdb binary not available for PASE

Proof of Work

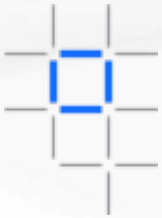
- CPU intensive
- GPU offload
- Neither great for IBMi

A typical enterprise systems architecture





Typical roles in an enterprise systems architecture



Data Layer | Business Application Layer | Presentation Layer

Governor

Deployer
Operator

Developer

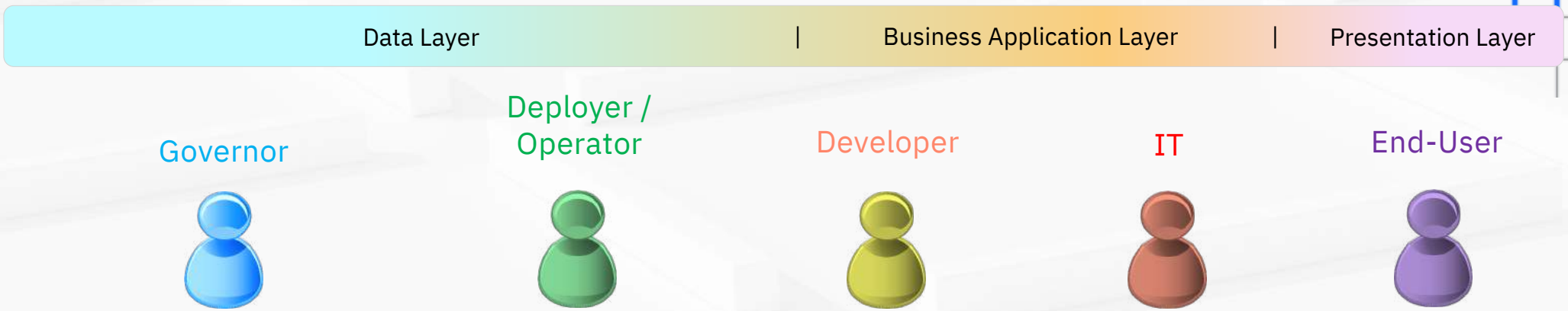
IT

End-User

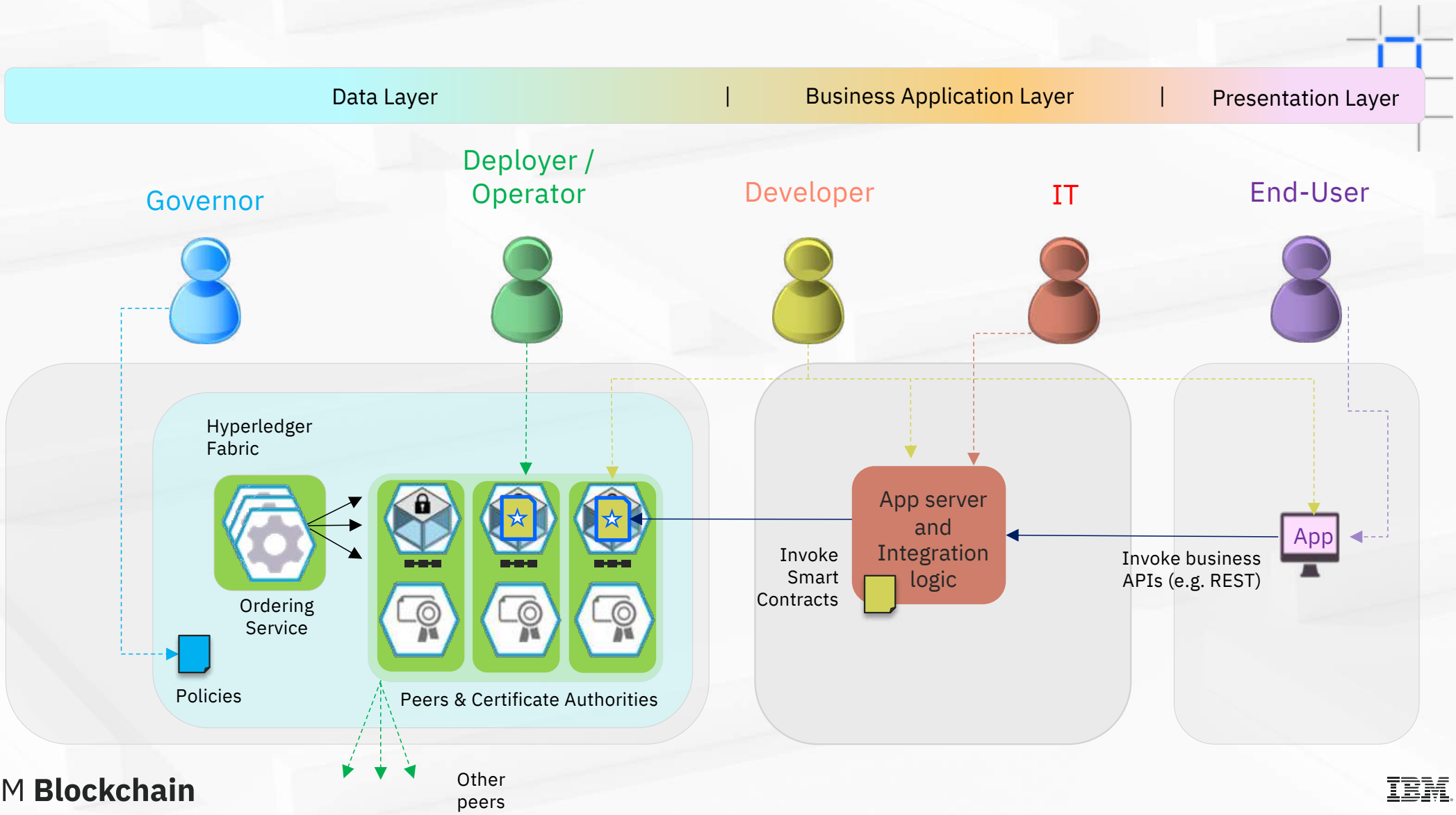
Systems of Record

Business Logic,
Gateways, APIs

Apps, Sensors

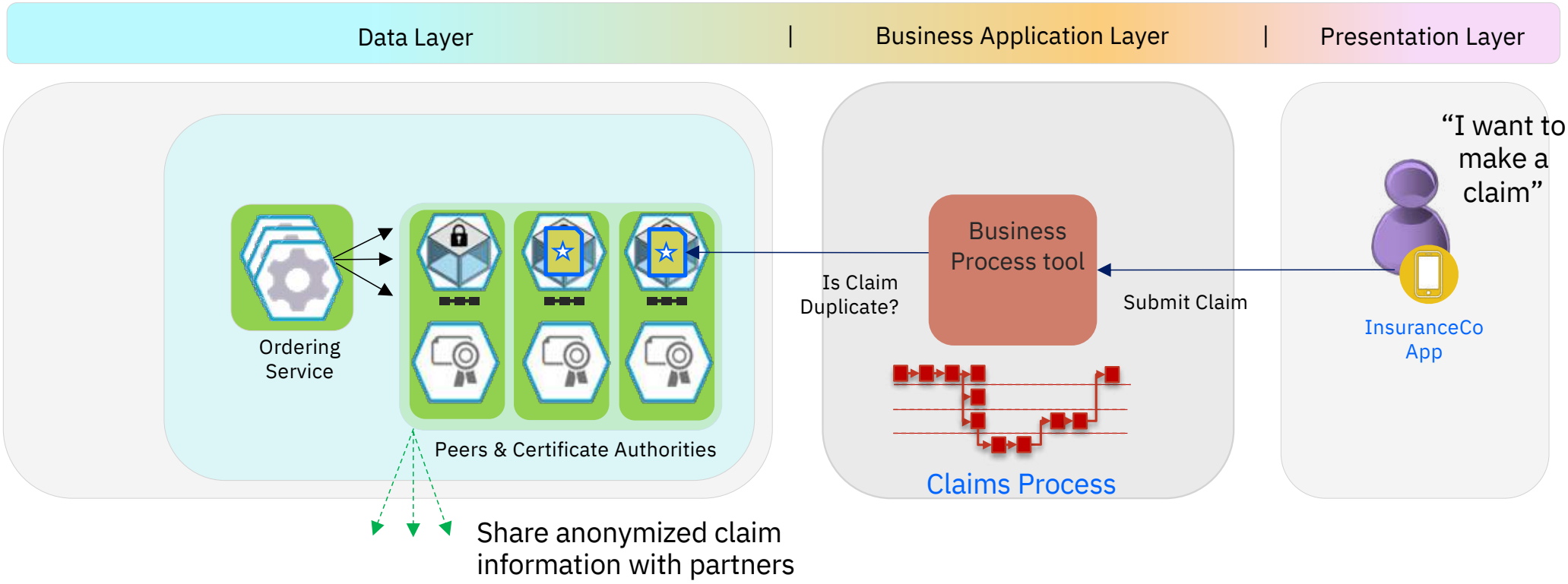


Where would a blockchain solution fit in this architecture?


Data Layer
Business Application Layer
Presentation Layer
Governor
Deployer / Operator
Developer
IT
End-User
Hyperledger Fabric
Ordering Service
Policies
Peers & Certificate Authorities
Other peers
App server and Integration logic
Invoke Smart Contracts
App
Invoke business APIs (e.g. REST)

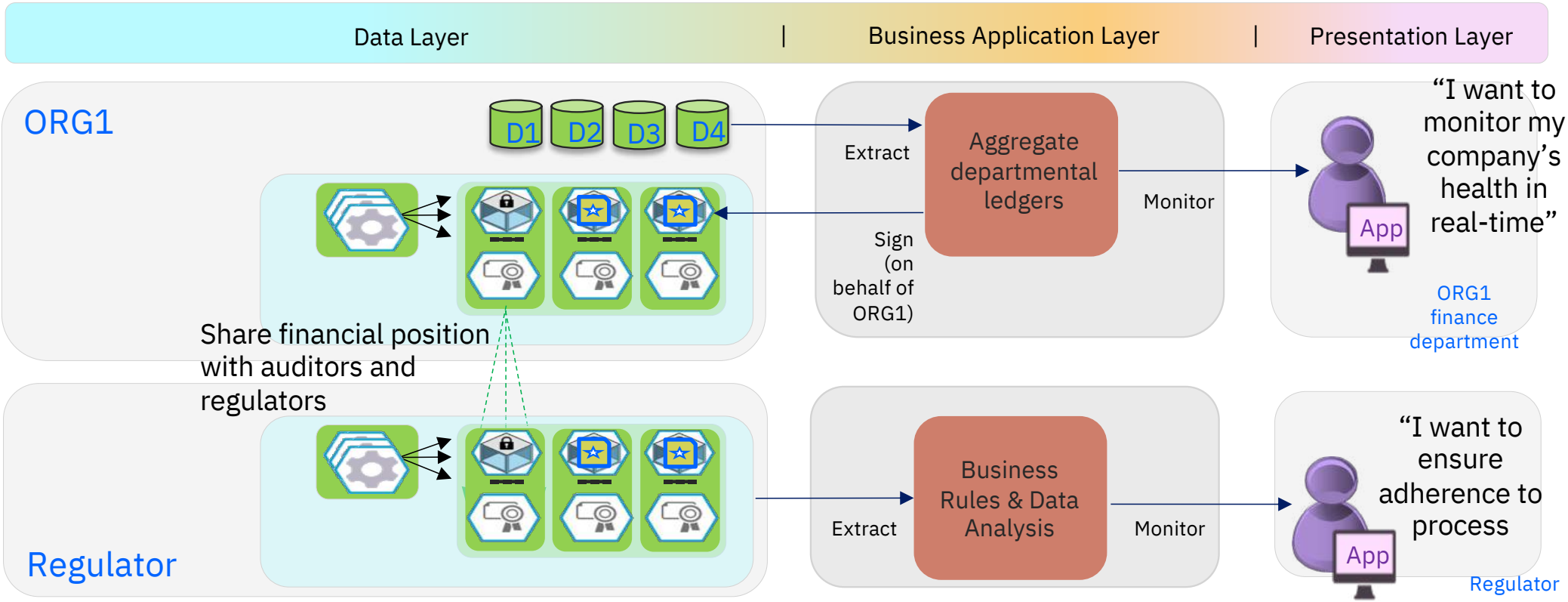
Extending business process to include partners

Business Process Management tools are typically deployed within a single organization or business unit, with B2B interactions managed point-to-point, often using a variety of technologies. Sharing business process can **lower costs** and **improve the reliability of data**.



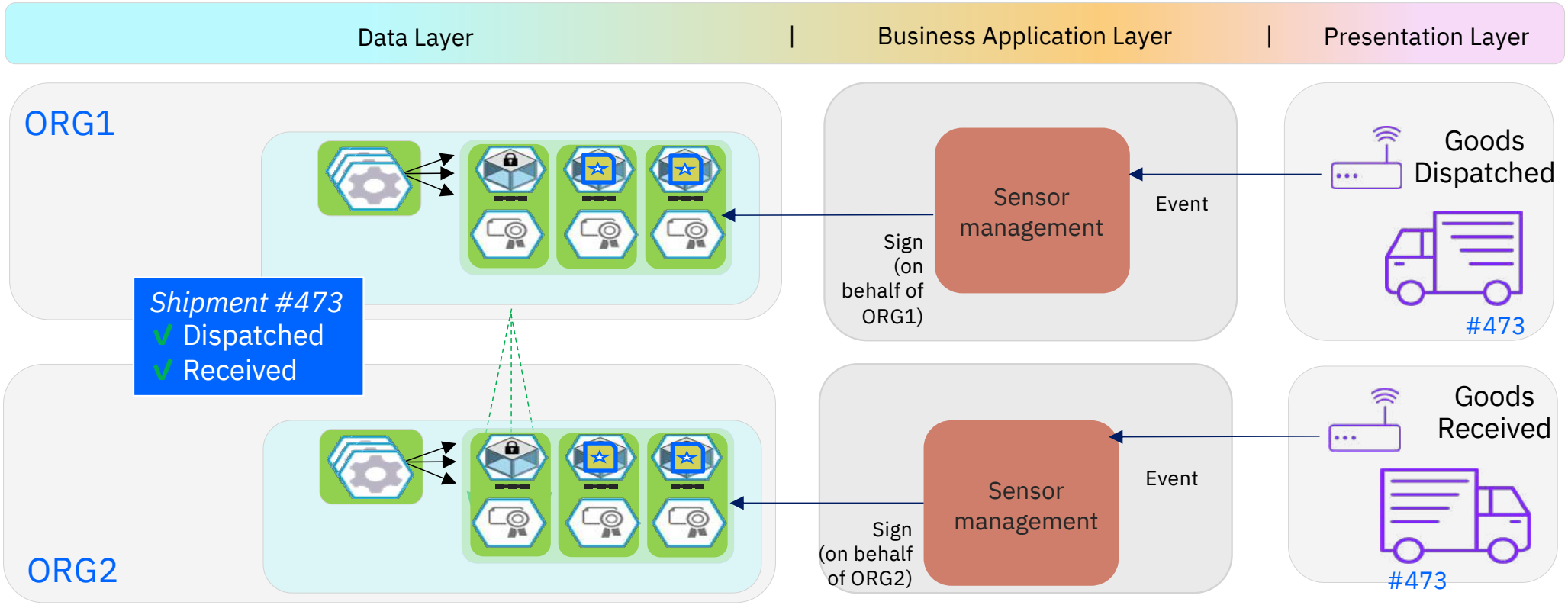
Lowering the costs of audit and compliance

Financial and compliance data in a large organization is spread through many divisions and geographies. Auditors and regulators need indelible proof of key transactions and adherence to process. Collating this proof can be costly and time consuming. Blockchain shows **provably signed and tamper-resistant data**.



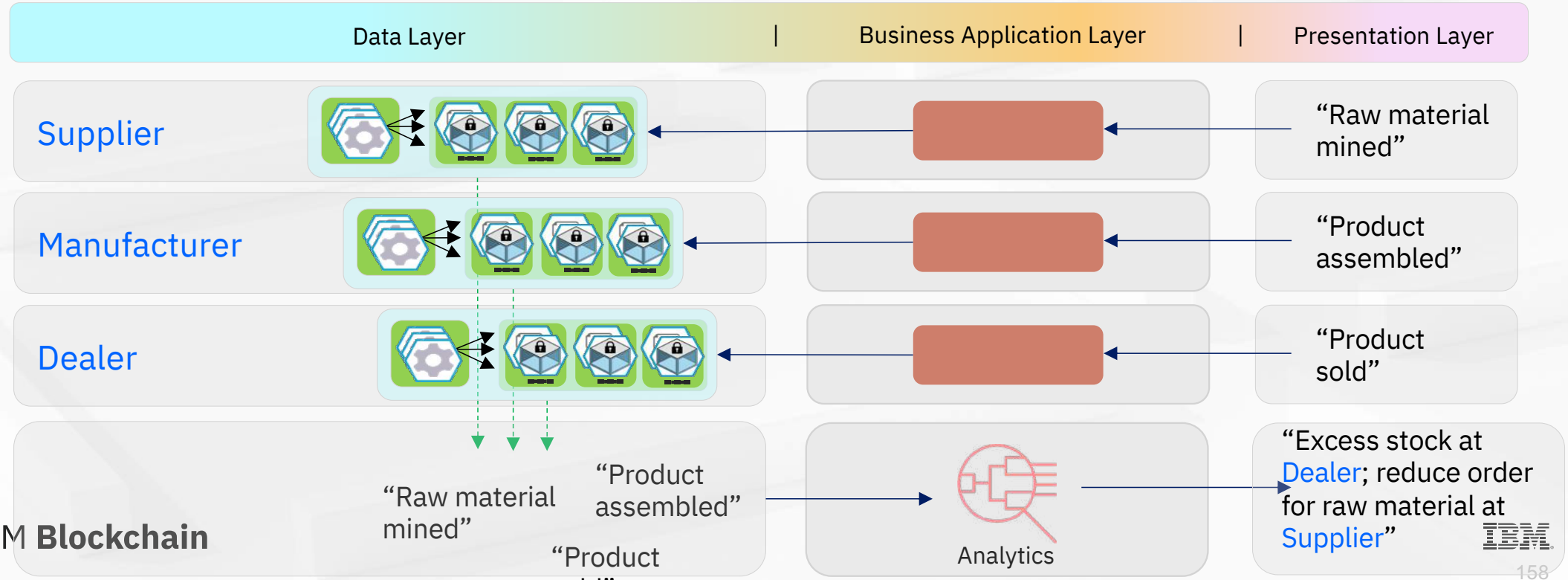
Verification of receipt with device integration

Events from devices can **trace provenance** of goods and components through a supply chain. Make contracts that harness sensor information, perform evidence-based dispute resolution, provide and verify reliable receipt of goods, prevent disposed components from entering black market, and more.



Insights and action over a supply chain

Blockchain provides a corpus of data that spans the entire business network. Blockchain information is more reliable and complete than any single organisation's source of truth. Analytics scenarios are therefore a good fit for blockchain. Gain insight into the effectiveness of end-to-end business process, and turn those insights into operational improvements, leading to **more efficient supply chains and lower costs**.

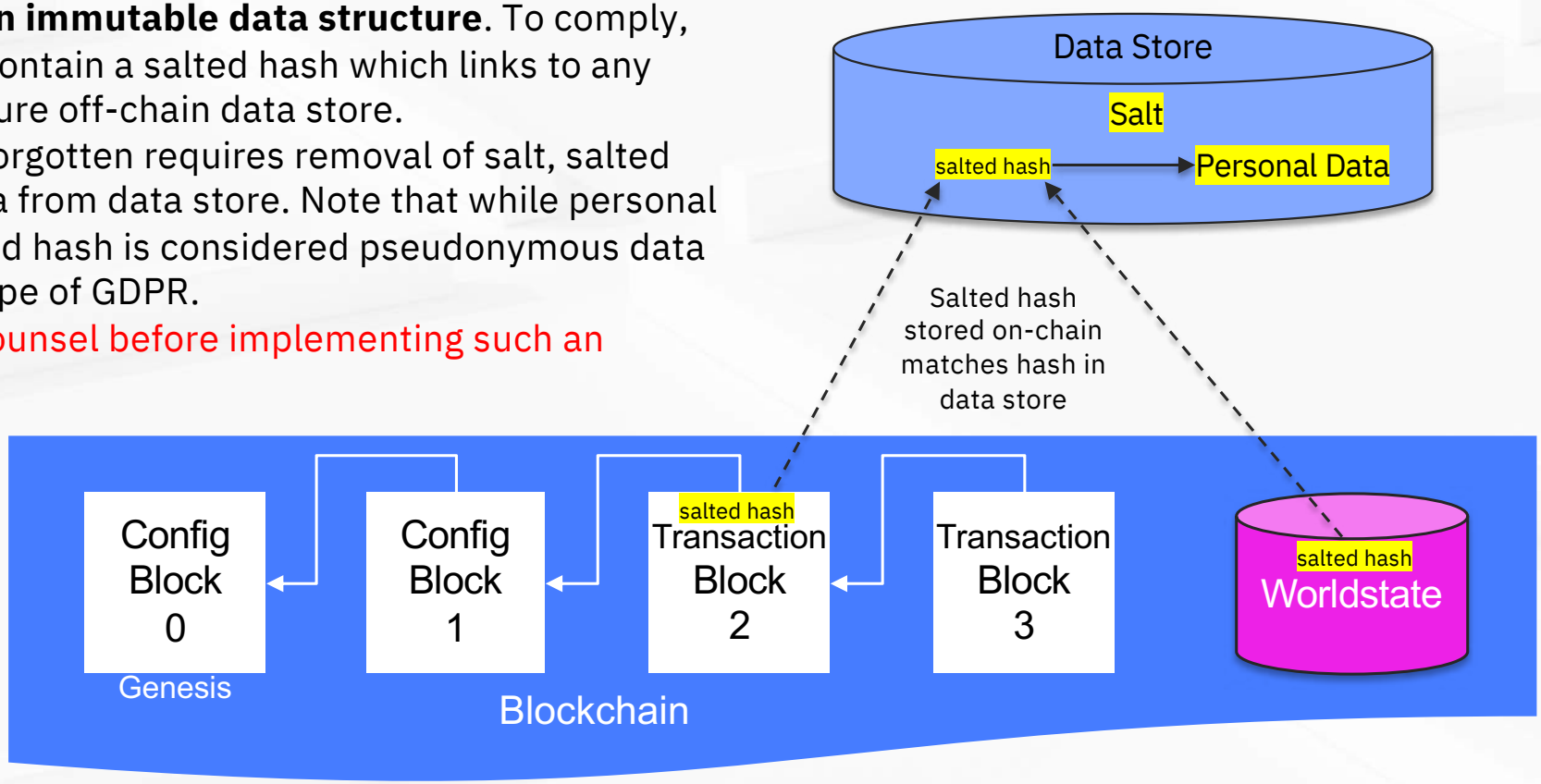


Storing personal data with privacy in mind

GDPR regulation enables EU citizens to exercise their right to be forgotten, which means that **personal data of EU citizens cannot be stored on an immutable data structure**. To comply, on-chain data should contain a salted hash which links to any personal data on a secure off-chain data store.

Exercising right to be forgotten requires removal of salt, salted hash and personal data from data store. Note that while personal data remains, the salted hash is considered pseudonymous data and falls under the scope of GDPR.

Always consult legal counsel before implementing such an architecture.



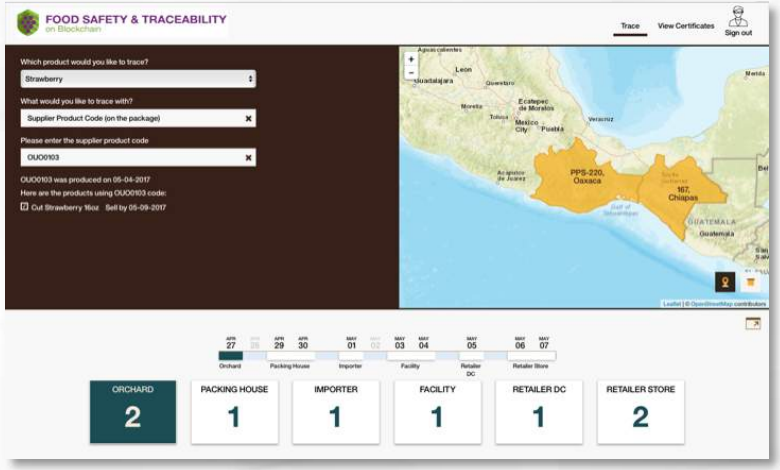
How End-Users interact with the blockchain

Exchanging trustworthy information

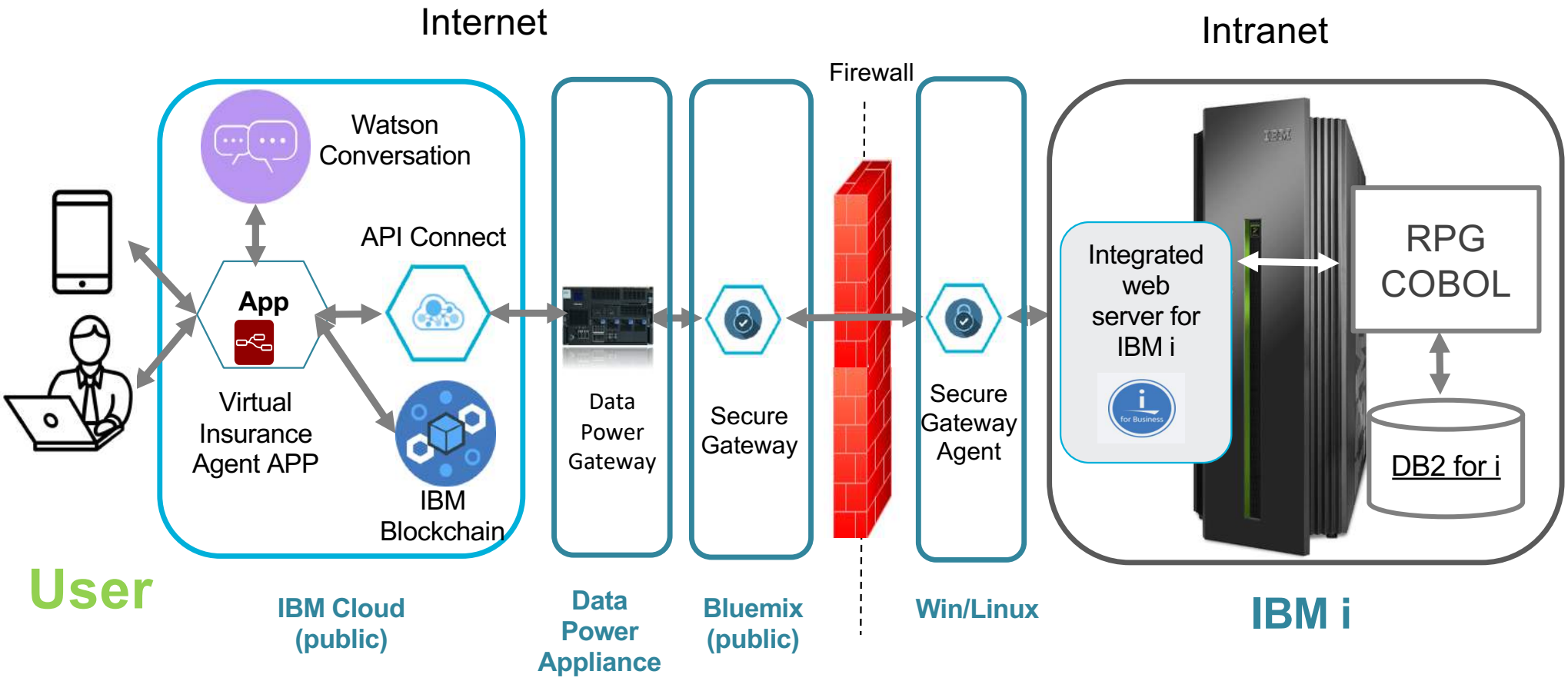
- End-users run presentation logic on an appropriate device
  - For example, mobile application or desktop dashboard
  - There may be multiple end-user applications (often one per organization or user role)

- The value proposition to end-users is that the information they see is trustworthy
  - Will probably be unaware of blockchain back-end
  - Uses an identity managed by the business application layer

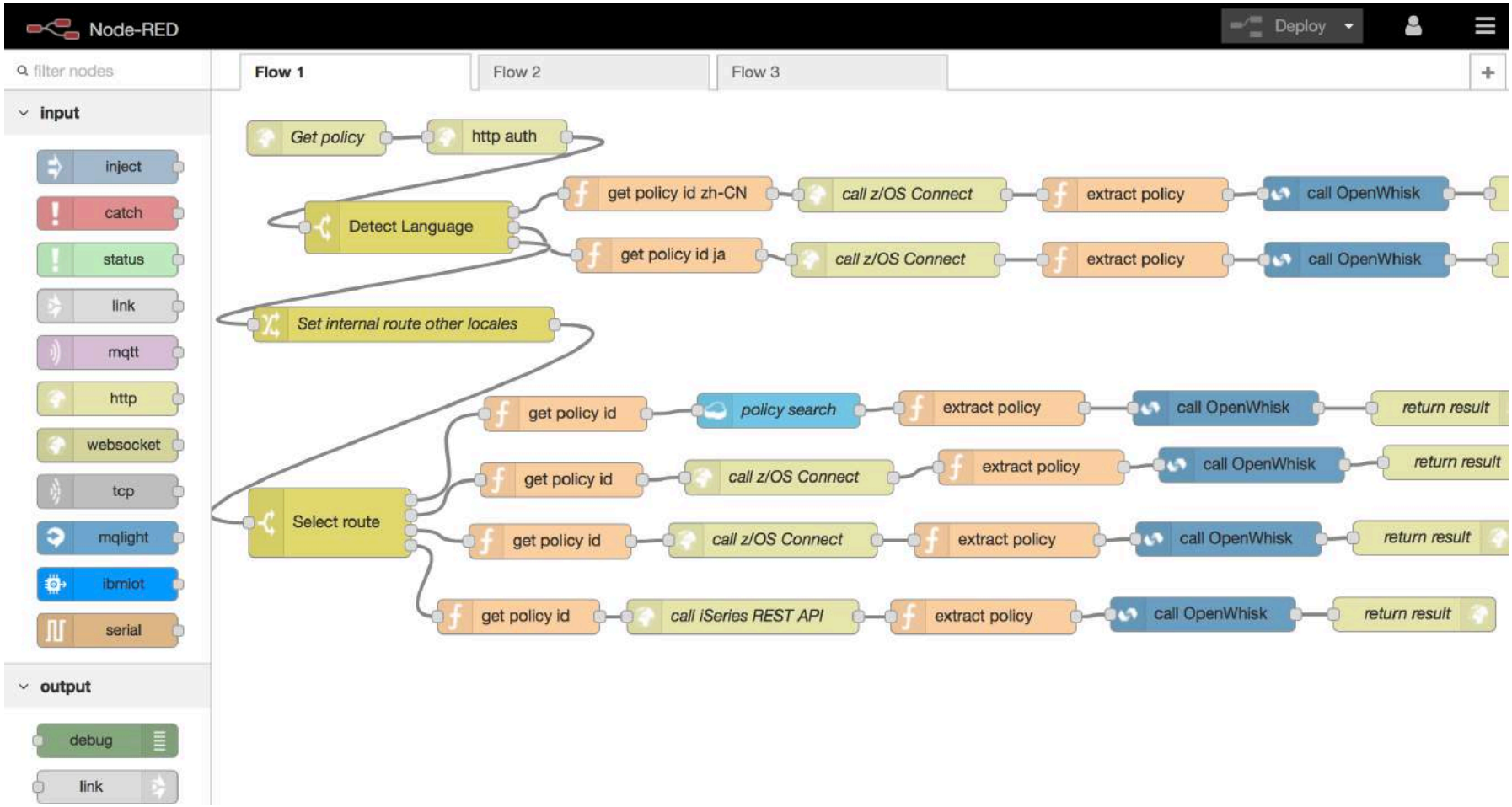
- Many options for presentation logic implementation
  - For example, integrate with end user applications via a REST server built using the Fabric SDK



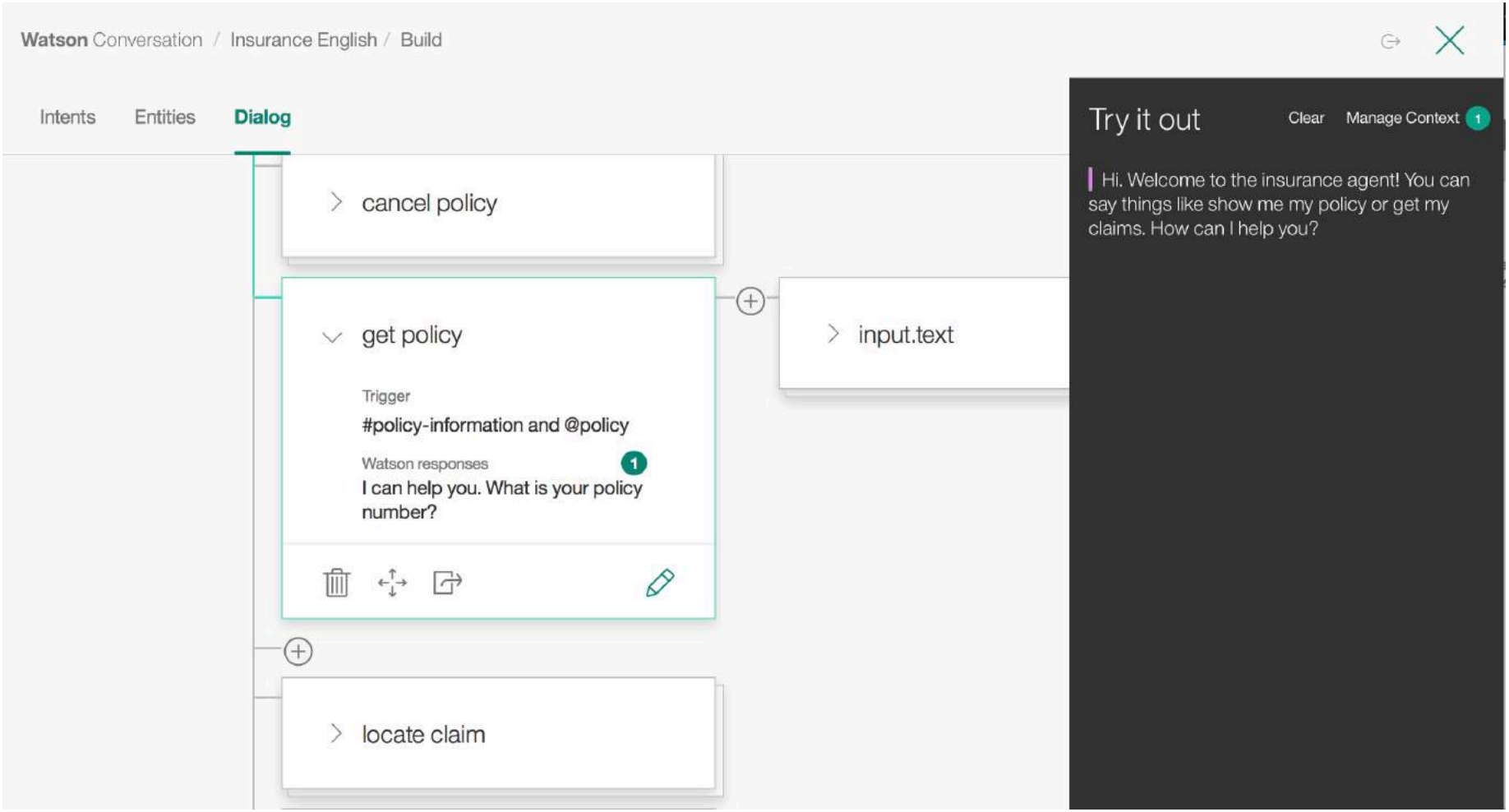
System Architecture With IBM i



Node RED – Business Logic (example)



Watson Conversation – Cognitive Chatbot



High Level Insurance API Architecture

DB2

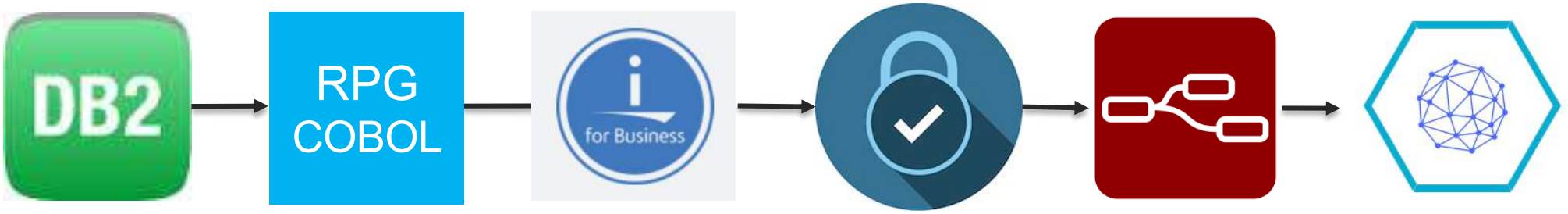
RPG or COBOL

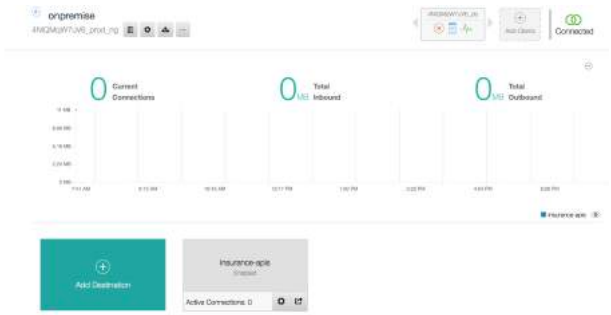
Integrated web server for IBM i

Secure Gateway

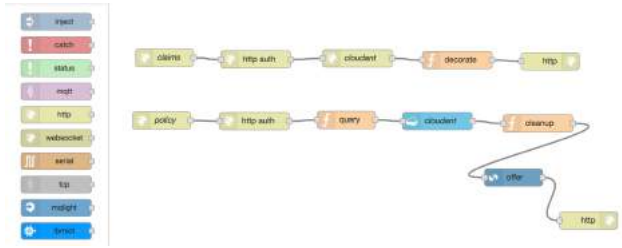
Node Red or Java or Node.js

API Connect





Securely access IBM i applications and data



Build private implementation in a Node Red flow or Java or Node.js

Generate a public secure API

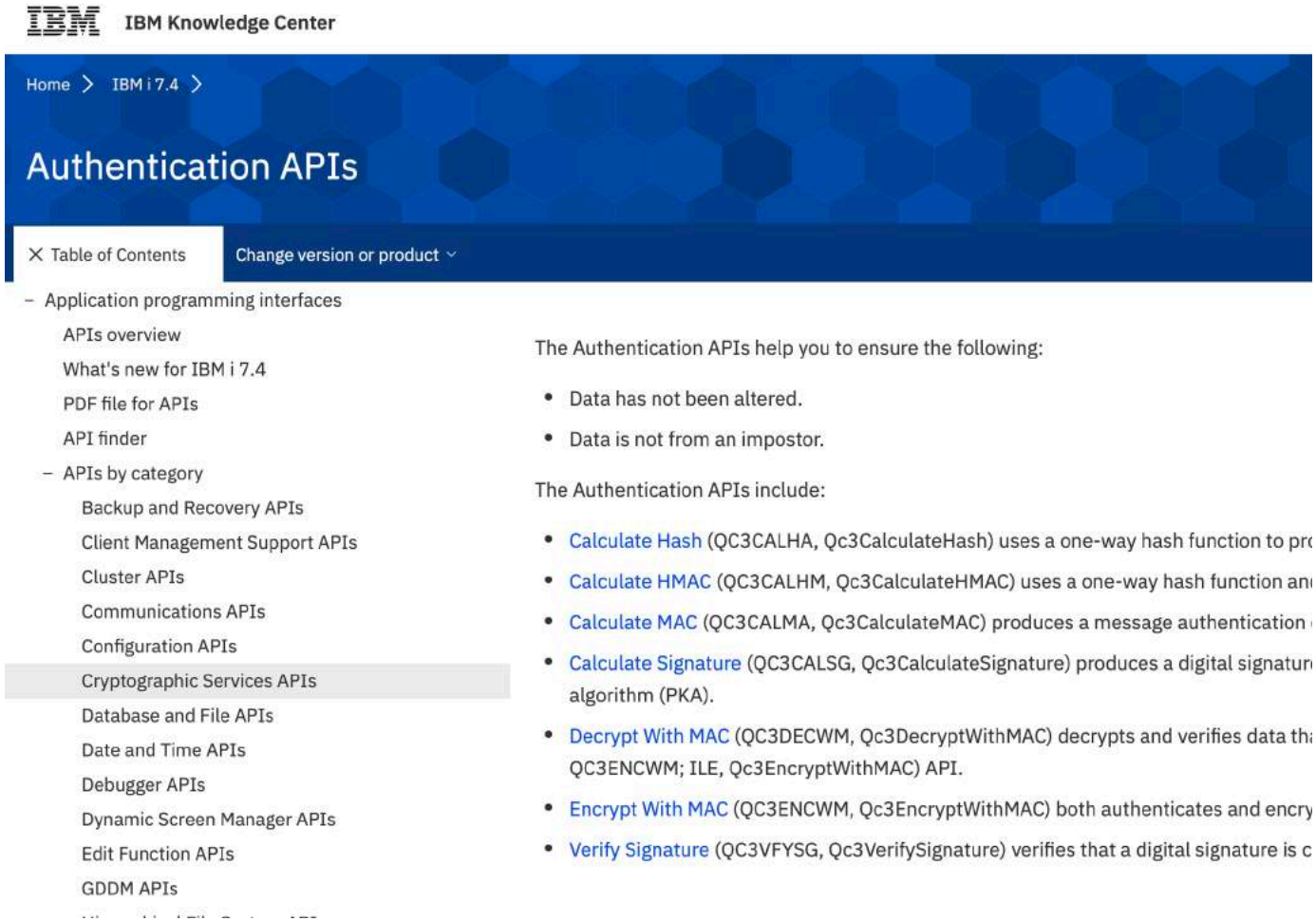
ILE RPG implementation - try this at home

```
// creating a list listPtr = list_create();
// check if the list is empty (it should be)
 if (list_isEmpty(listPtr));
              dsply 'List is empty';
              else;
              dsply 'List is not empty';
endif;
 // create a new list which is populated with
// a subset of data from the original list
sublistPtr = list_sublist(listPtr : 2);
// iterate through the entries of the list
valuePtr = list_iterate(sublistPtr);
dow (valuePtr <> *null);
              value = %str(valuePtr);
               len = %len(%trimr(value));
               //Set the HASH Algorithm you want to use !
              alg.HashAlg = HASH_SHA1;
              //API to calculate the SHA1 hash
              Qc3CalculateHash( %addr(value)  : len   : 'DATA0100'  : alg  : 'ALGD0500'  : '0'  : *OMIT  : bin  : ErrorNull);
              //Convert to HEX
              cvthc( $hex: bin: %len(bin)*2);
              dsply $hex;
              valuePtr = list_iterate(sublistPtr);
enddo;
 // freeing the allocated memory
 list_dispose(listPtr);
```

https://www.mysamplecode.com/2011/05/rpgle-generate-sha-1-hash-use.html
https://bitbucket.org/m1hael/llist/src/master/README.md

ILE RPG implementation

https://www.ibm.com/support/knowledgecenter/ssw_ibm_i_74/apis/catcrypt3.htm



ILE RPG implementation

Required Parameter Group:

1	Input data	Input	Char(*)
2	Length of input data	Input	Binary(4)
3	Input data format name	Input	Char(8)
4	Algorithm description	Input	Char(*)
5	Algorithm description format name	Input	Char(8)
6	Cryptographic service provider	Input	Char(1)
7	Cryptographic device name	Input	Char(10)
8	Hash	Output	Char(*)
9	Error code	I/O	Char(*)

Service Program Name: QC3HASH

Default Public Authority: *USE

Threadsafe: Yes

The Calculate Hash (OPM, QC3CALHA; ILE, Qc3CalculateHash) API uses a one-way hash function to produce a fixed-length output string from a variable-length input string. For all practical purposes, one-way hashes are irreversible. This property makes them useful for authentication purposes.

Information on cryptographic standards can be found in Create Algorithm Context (OPM, QC3CRTAX; ILE, Qc3CreateAlgorithmContext) API.

https://food.ibm.com/
https://www.tradelens.com/

https://cms.ibm.com/case-studies/wijnen-van-maele-systems-software-ibm-i

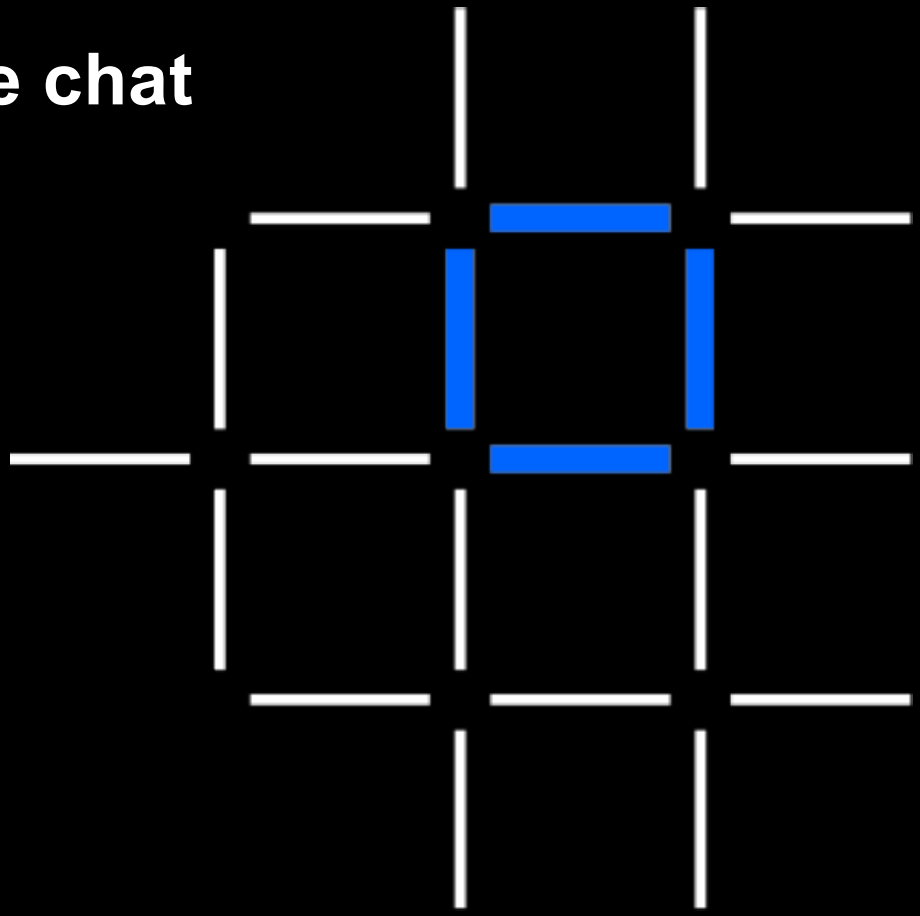
https://www.syncsort.com/en/products/blockchain

https://bitbucket.org/m1hael/llist/src/master/
https://www.mysamplecode.com/2011/05/rpgle-generate-sha-1-hash-use.html

Thank you

Questions? Ideas? Meet me in the chat

Ross Cruickshank
@rcruicks
ross@vnet.ibm.com



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

@IBMBlockchain
IBM Blockchain
IBM Blockchain