

Get Ready for the Next Big Thing

Hyperledger Fabric Blockchain

Arjan ten Hoopen



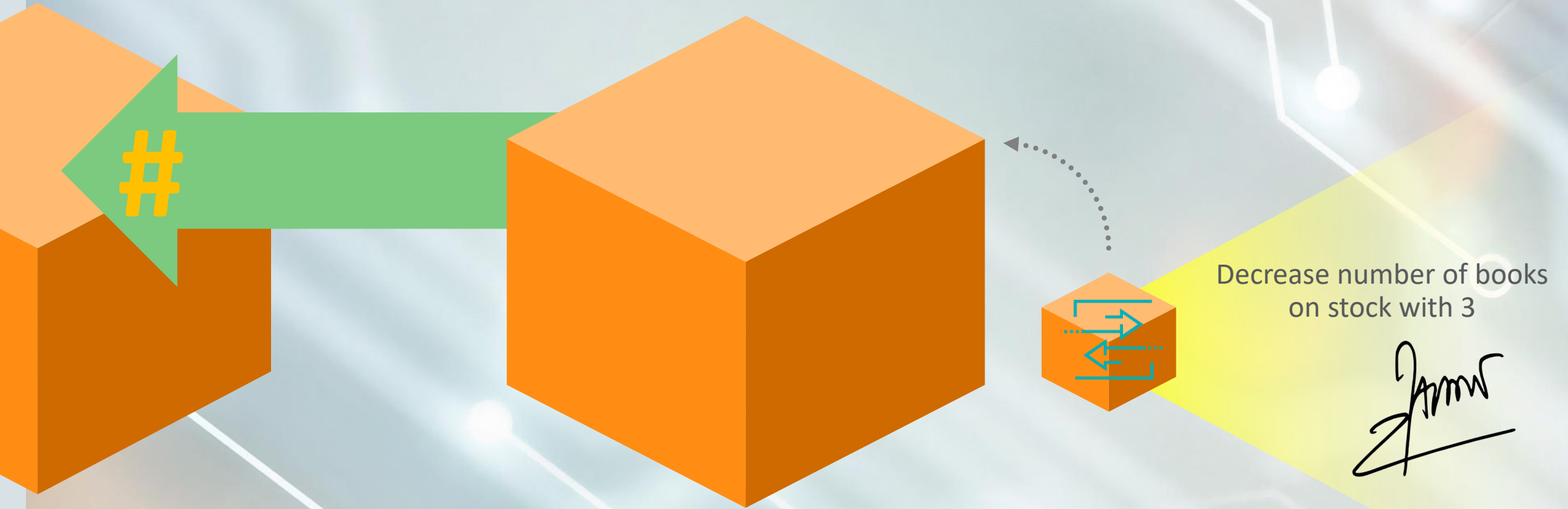


BLOCKCHAIN

What is a Blockchain

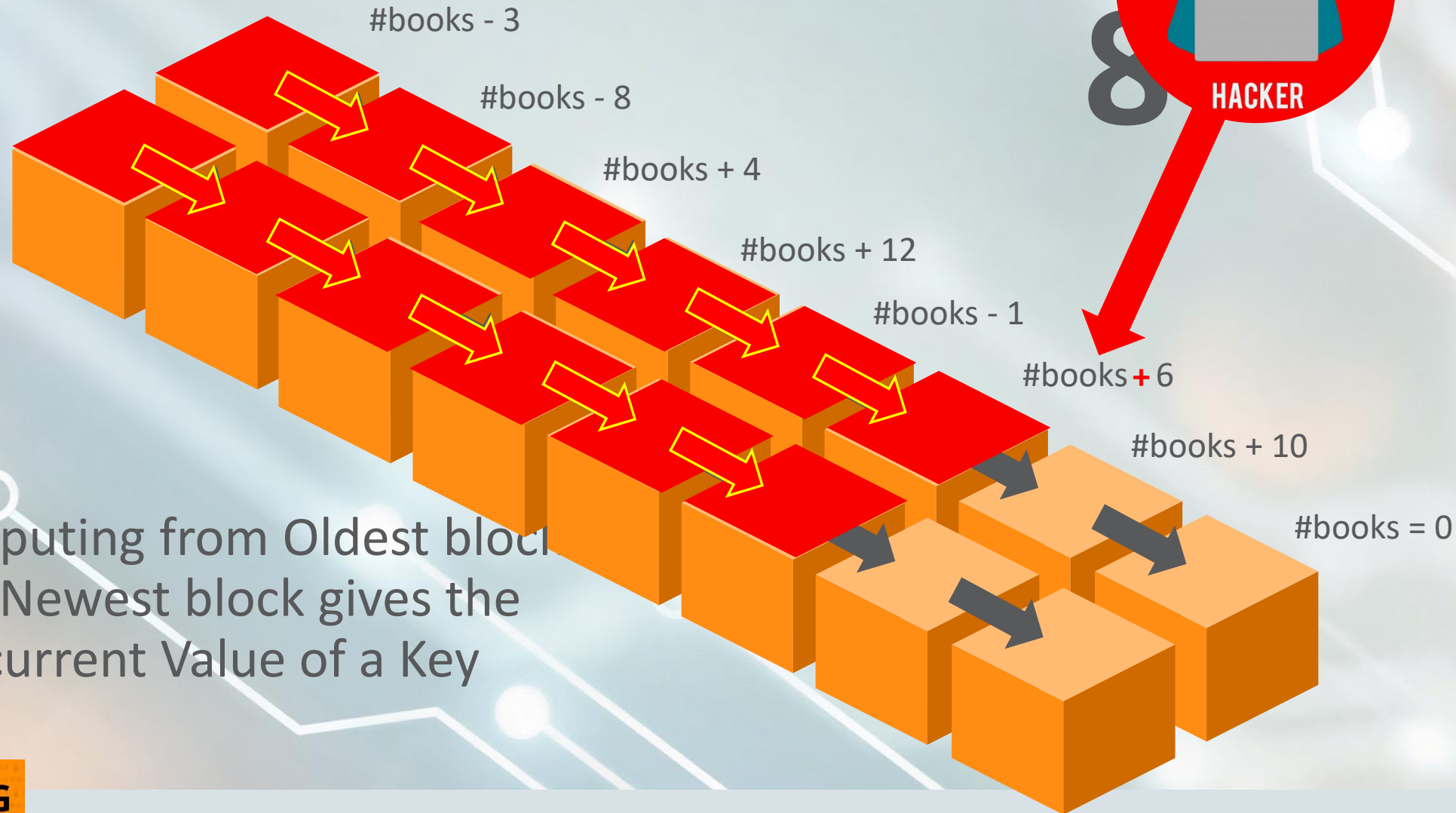
Block ...Blocks ... Blockchain

A Block



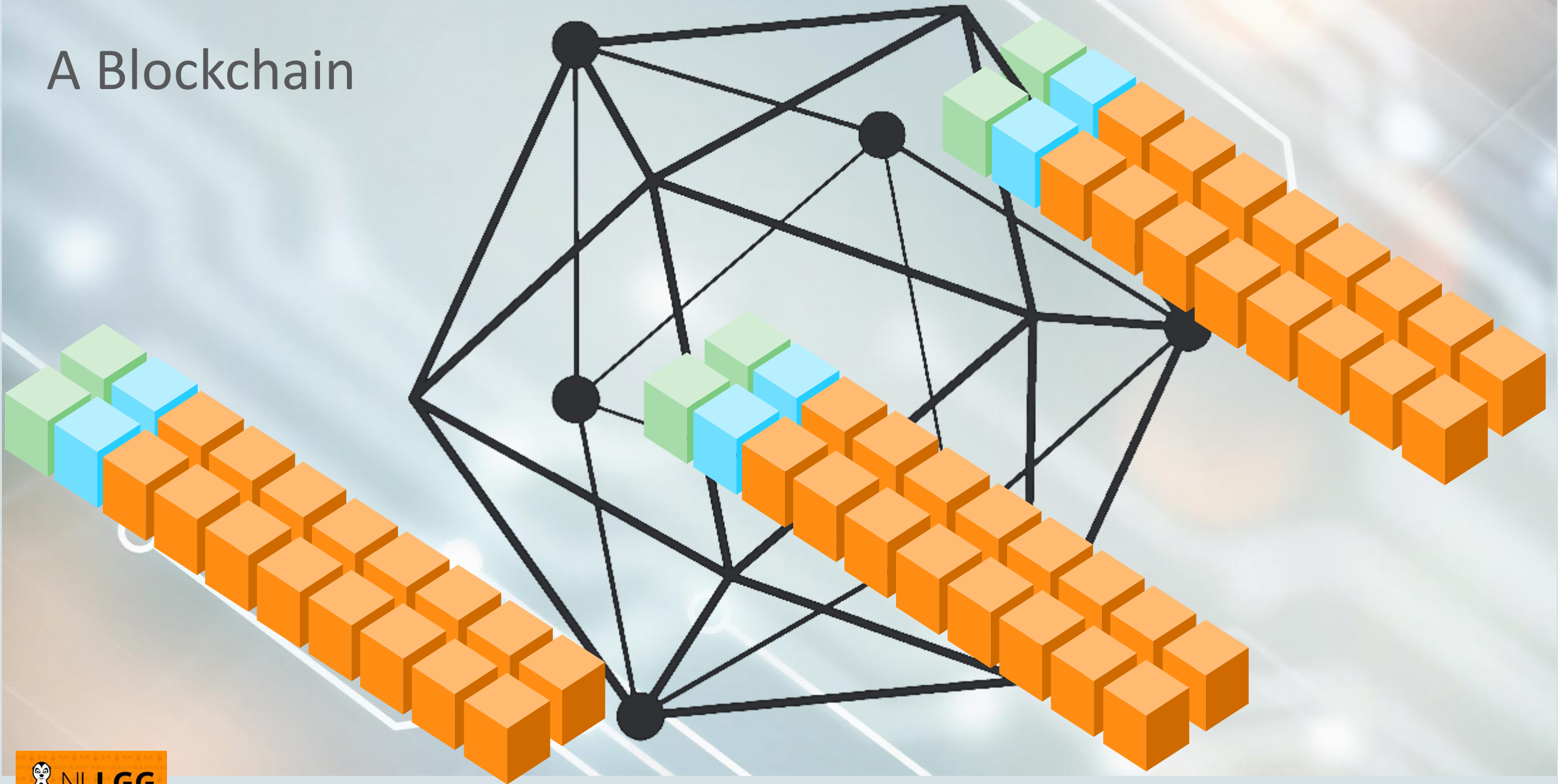
A Blockchain

$$\#books = 0 + 10 - 6 + 4 - 8 - 3$$

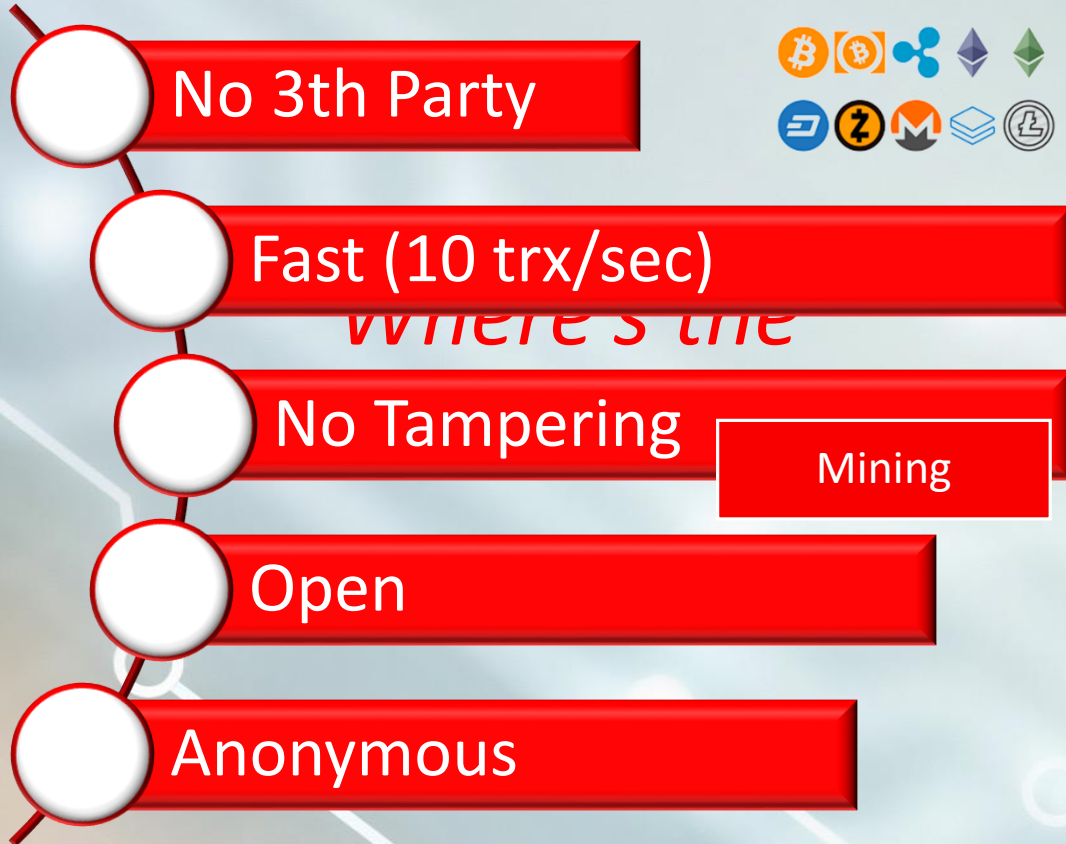


Computing from Oldest block to Newest block gives the current Value of a Key

A Blockchain



Is a Blockchain a Blockchain ?



Permissionless Blockchain



Permissioned Blockchain

Chaincode

Implements *Smart Contracts*

<Chaincode>

It adds “Conditions” to the Blockchain

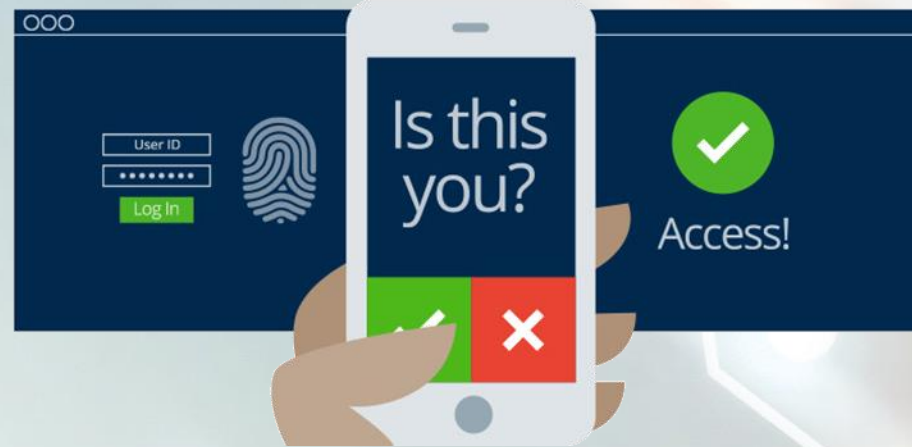
The Business needs to define the Logic

Developers will Implement the Chaincode

Chaincode is actually a “program”

Java, Node.js or Golang

Authentication & Privacy



How do I know that you are the one you say you are

Enable Privacy

How do I know that you are the one you say your are ..

Key Pair



Private Key



Public Key

This Key-Pair allows "Anyone" to Check if it was You

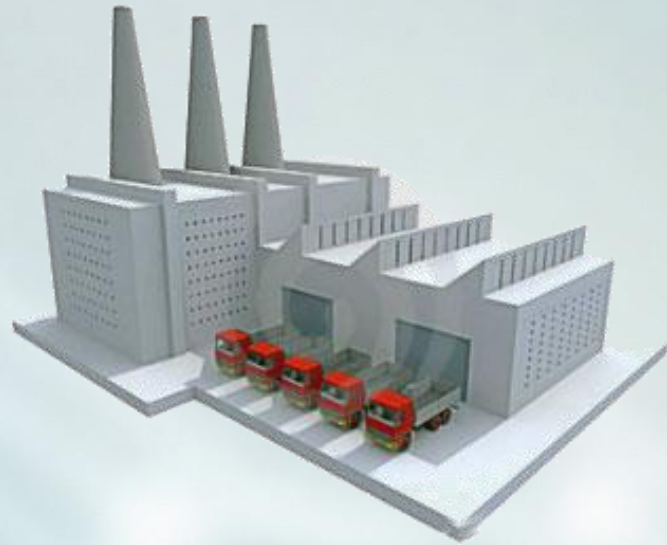
... "Anyone" only needs the Public Key ...



Sounds like Magic ...

Keys

Everything you never wanted to know...



Private Key

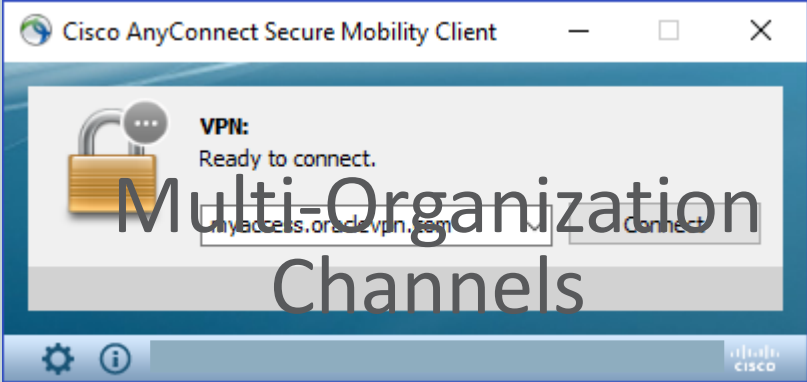
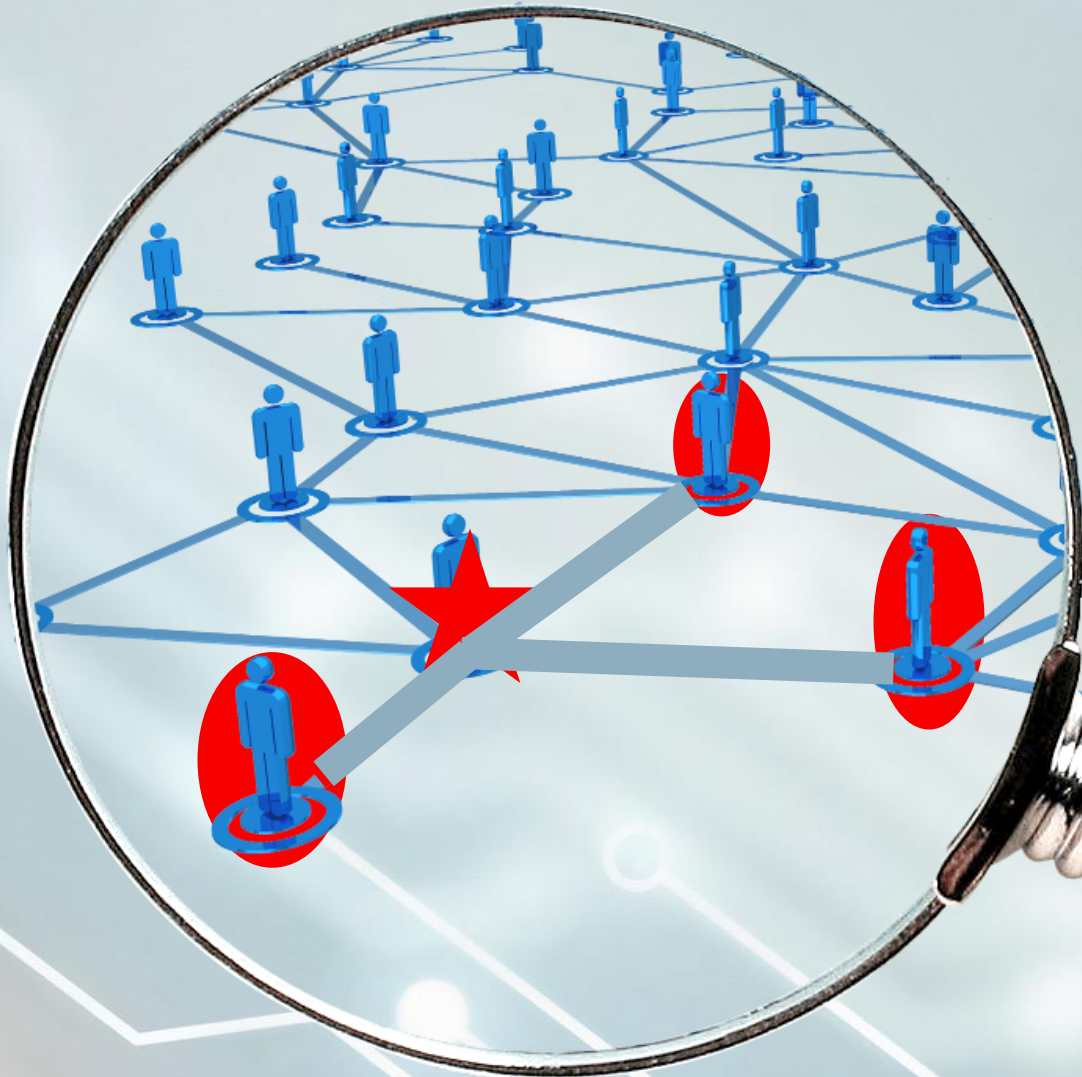
Public Key



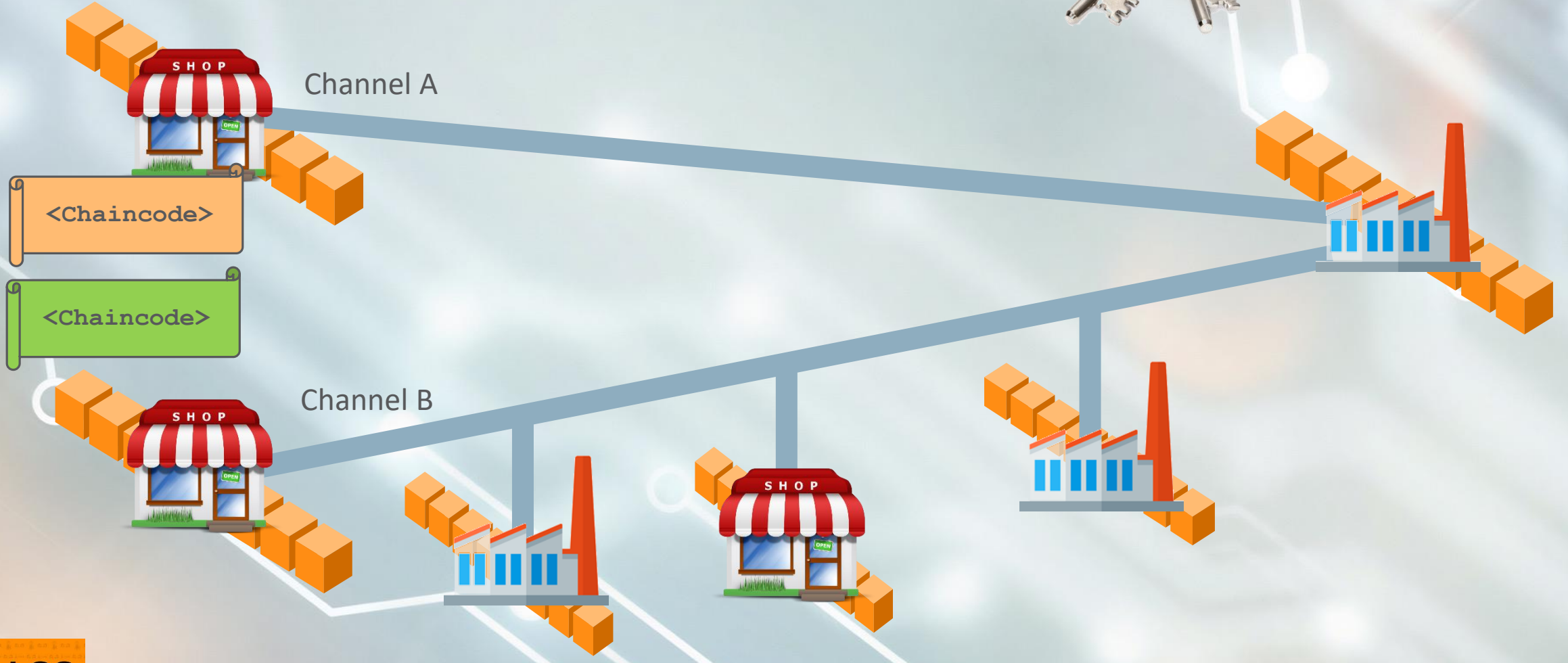
- Marion buys a Marker
 - ... With many many Caps
 - She sends a Cap to “everybody”

If Marion sends you a message written with her Marker; You can use the Cap to check if it's Marion's Marker.

Privacy

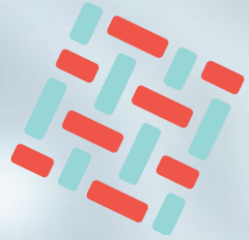


What you need to Remember



Blockchain Technology

Blockchain Technology



HYPERLEDGER FABRIC



- Permissioned
- Modular
- Immutable Transactions

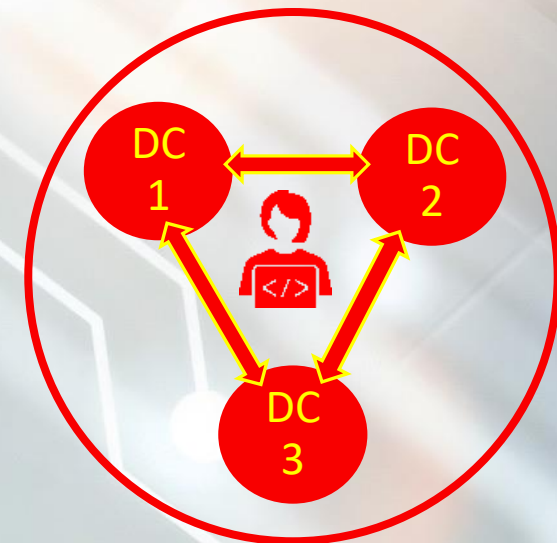
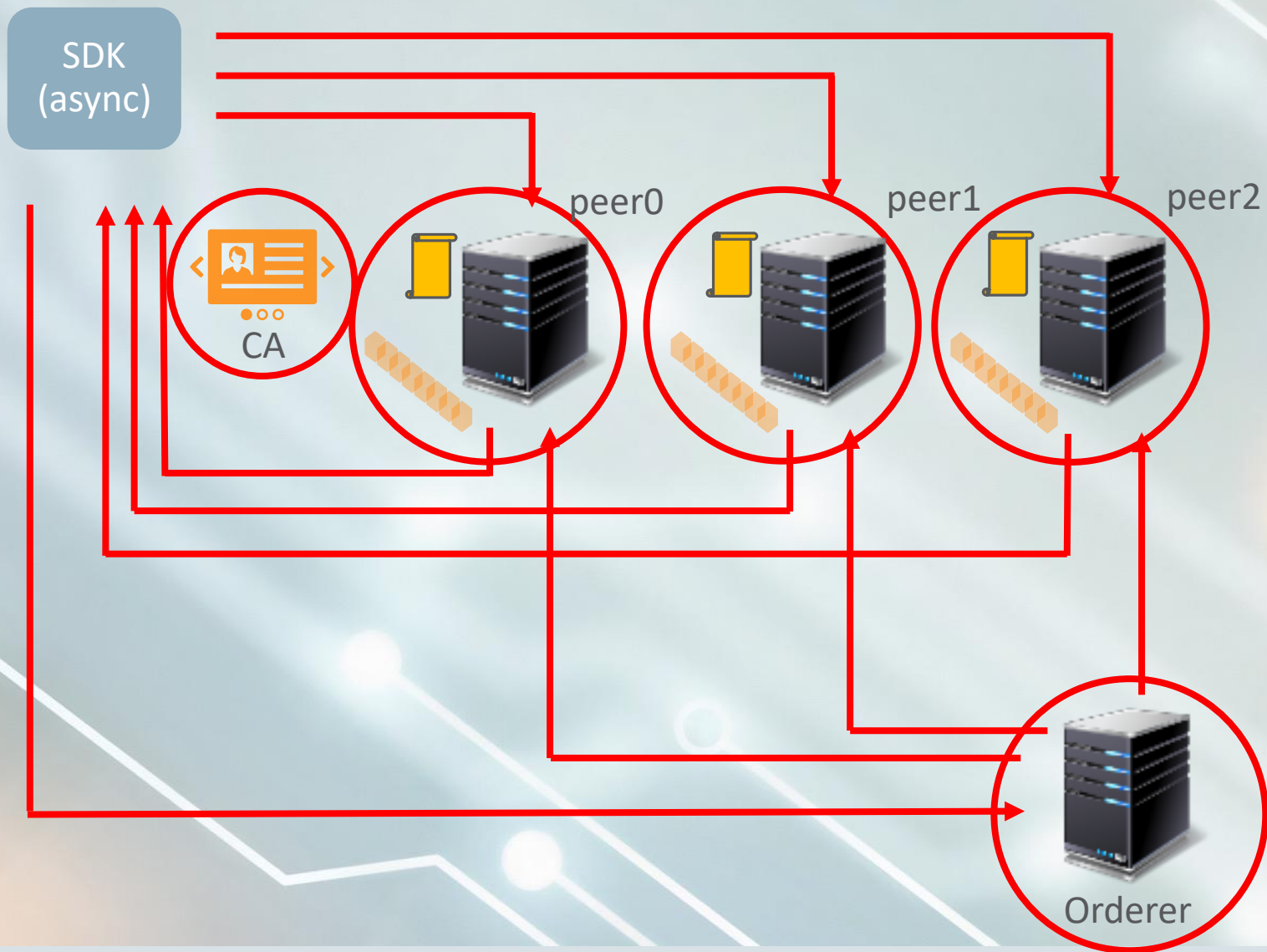
- No Specific Hardware
- No Specific Use Case
- Just Network Connectivity



Hyperledger Fabric

From Download to Production Environment

Hyperledger Fabric



Blockchain Platform 1,2,3

- 1: Create
- 2: Configure
- 3: Develop & Run

3

App Developers



Using SDK

Blockchain Network



Company A (Founder)



Company B (Participant)



<Chaincode>



Company C (Participant)

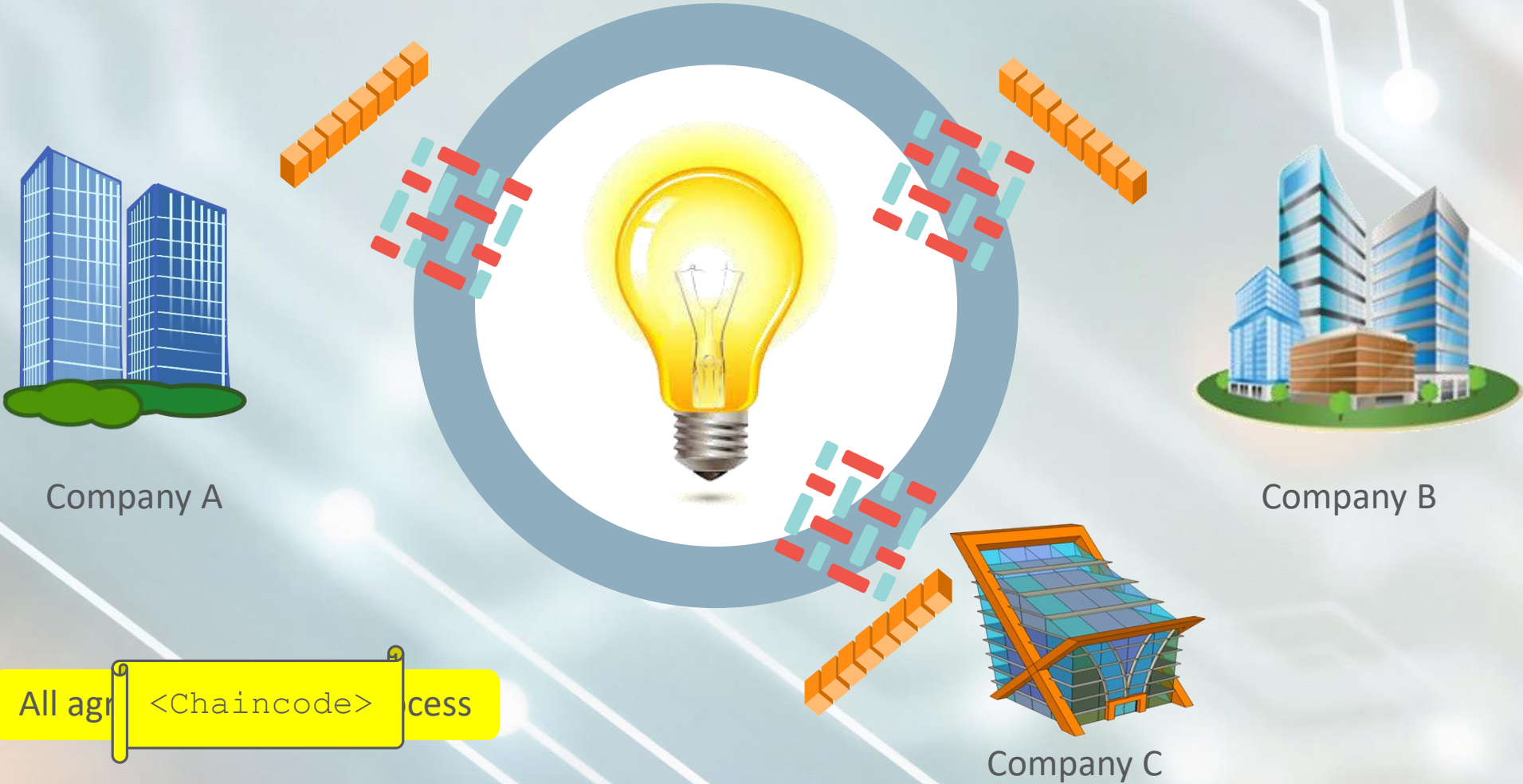


Fixing a Major Business Problem

Major Business Problem



How Hyperledger Solves this Major Business Problem

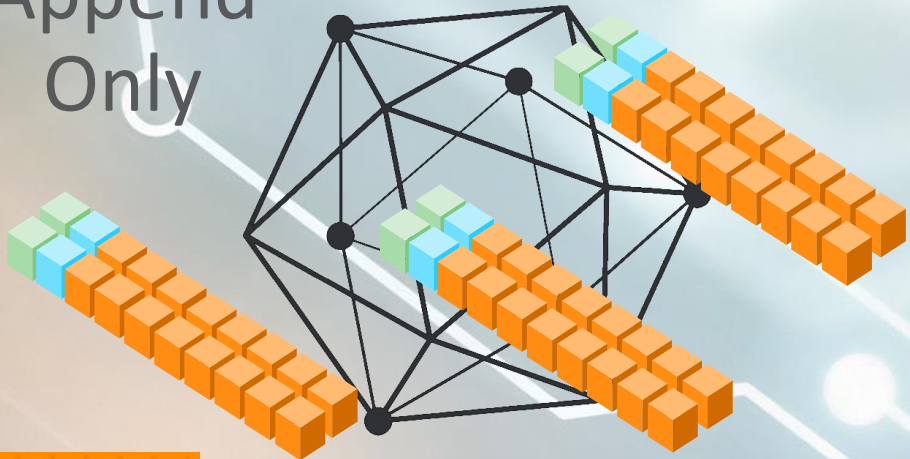


Major Business Problem

That's it ... ?



Append
Only



One Version of the Truth

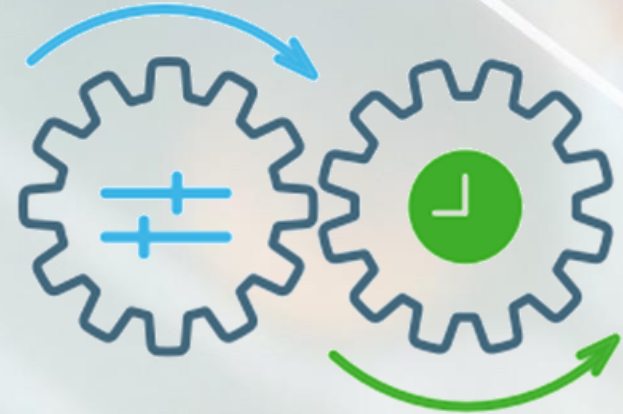
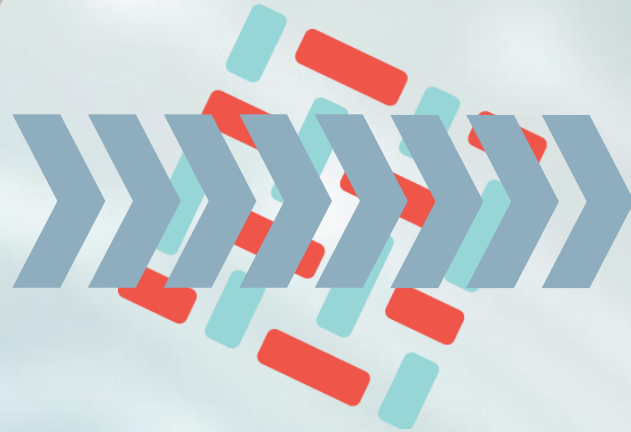


Major Business Problem

Finished .. ?



Batch Processing



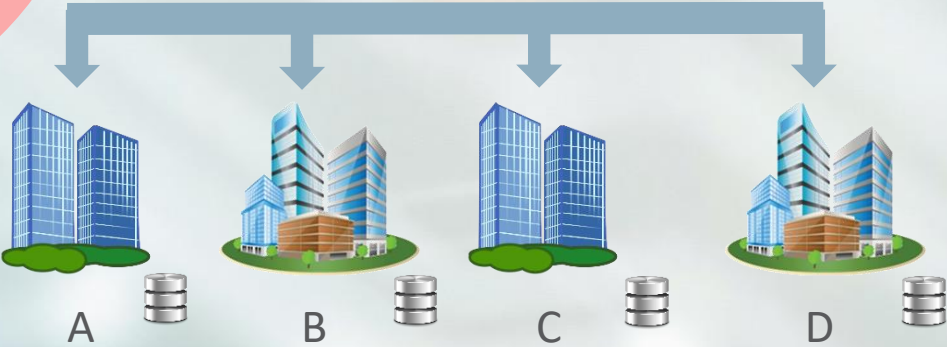
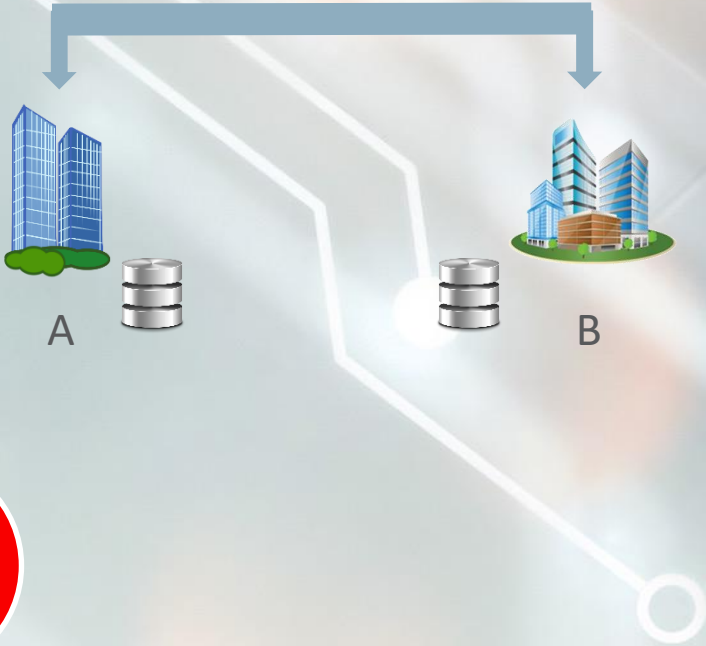
(Near) Real Time Processing



Use Cases

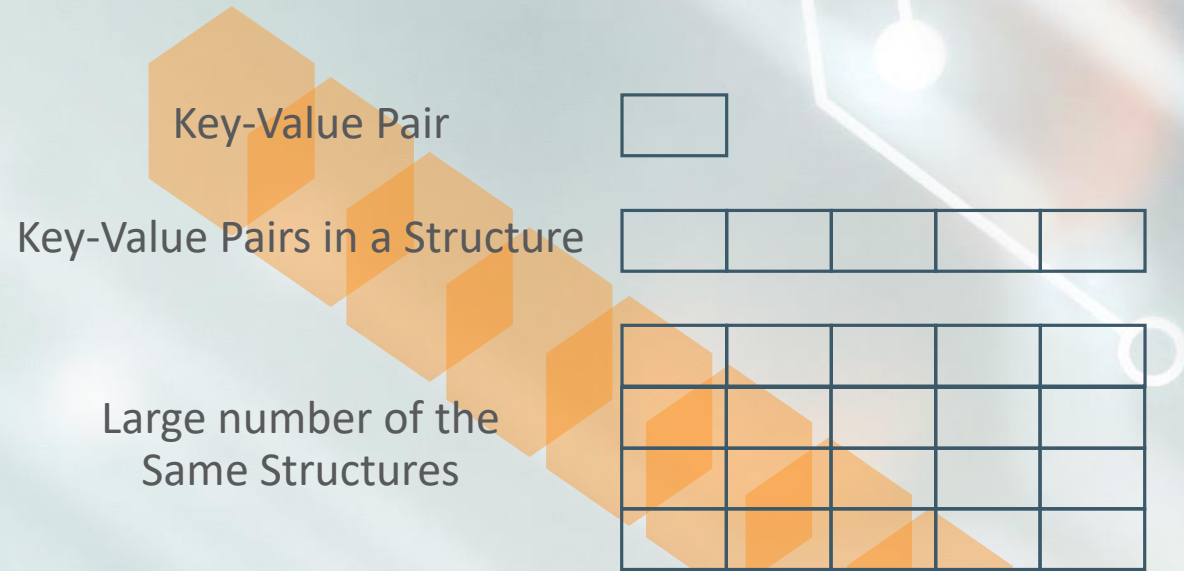
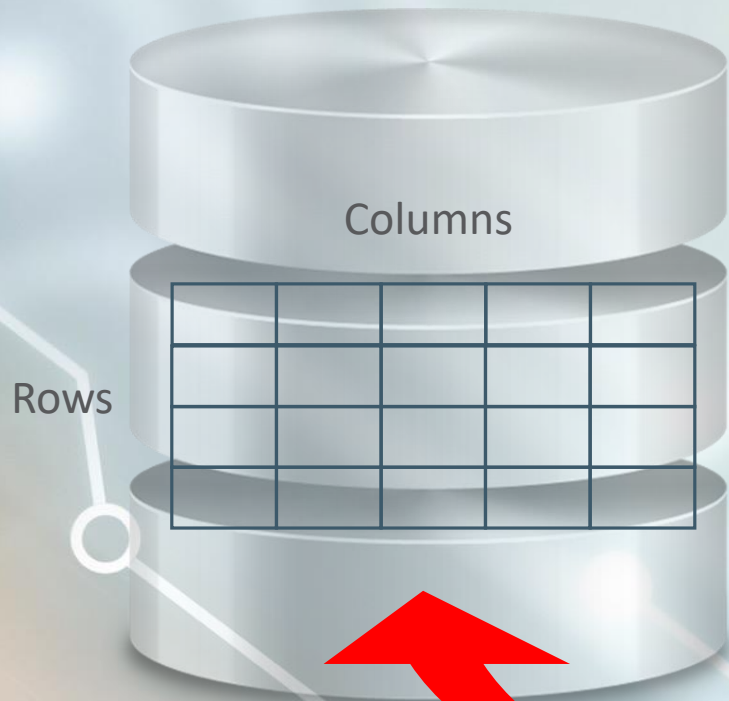
Use Cases

The Basics



Blockchains Sweet Spot

That's where you want to be



Blockchains Sweet Spot

That's where you want to be

- Well Established

- Single Point of Failure

 - Batch Processing

- Can be Tampered

- You get a single file

 - 3 Options

 - Can be tampered

- Stores Data

- Cutting Edge Technology

- Distributed (*By Design*)

 - Real Time Processing

- No Tampering (*By Design*)

- Fully Auditable (*By Design*)

 - All Transactions (read/write/rejected)

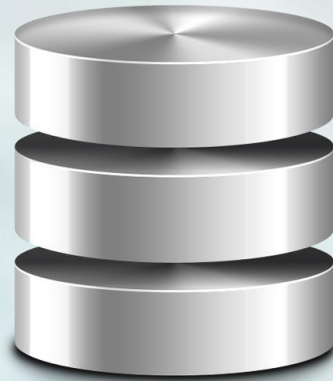
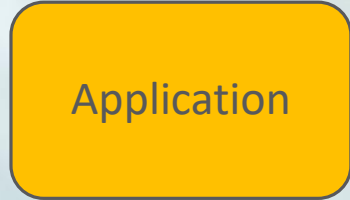
 - No Tampering

- Enforce Trust (*By Design*)

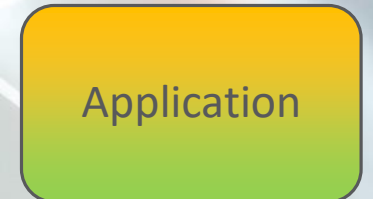
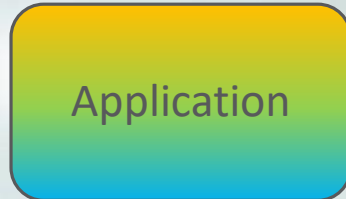
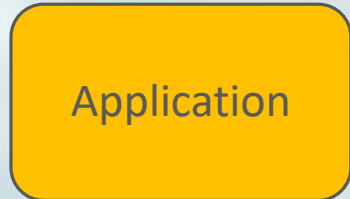
Blockchain Example

Herring

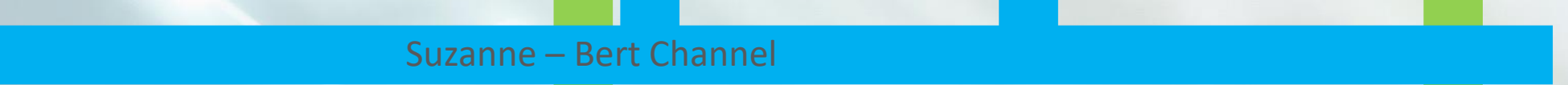
Traditional



Blockchain



recordHerring
queryHerring
updateHolder



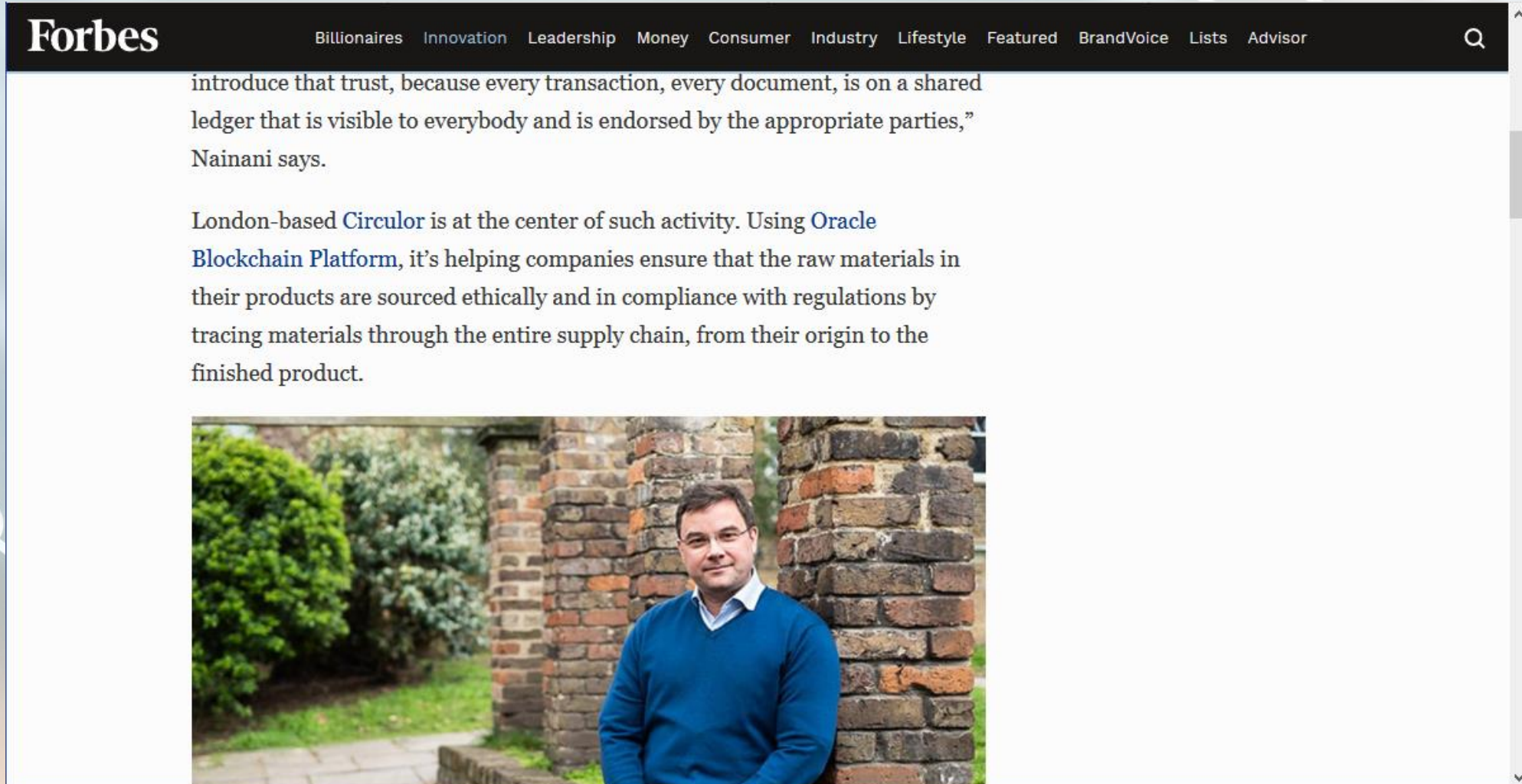
ICS Financial Systems & Arab Jordan Investment Bank

Money Transfer

The screenshot shows the Financial IT website. At the top right, there are links for "Submit content", "Sign in", and "Sign up". The main header features the "Financial IT" logo with the tagline "Innovations in FinTech". To the right of the logo is a dark blue banner for "INTELLIGENT AUTOMATION WEEK CHICAGO" from August 5-8, 2019, at the Sheraton Grand Chicago, with an "ACCESS AGENDA" button. Below the header is a navigation menu with links for HOME, FIT TV, BLOGS, NEWS, MAGAZINE, PRODUCTS, EVENTS, PUBLICATIONS, and ABOUT, along with a search icon. The main content area features a teal header for the article "AJIB GOES LIVE WITH ORACLE BLOCKCHAIN PLATFORM". The article includes a date of 01.04.2019 at 07:48 am, a "Blockchain" category tag, and social media icons for Facebook, Twitter, LinkedIn, and Google+. The article text states: "ICSFS & AJIB have successfully executed the first transfer of funds between the Bank's head office in Jordan and Cyprus branch. This successful milestone is one of the first blockchain execution in the MENA region on Oracle Platform, delivering an enterprise-grade blockchain implementation with industry-leading resiliency, scalability and security." Below the text is a "Like 795" button. To the right of the article is a "MAGAZINE" section with "ALL" items, showing covers for the "SPRING ISSUE" and "WINTER ISSUE". At the bottom right is a "FREE NEWSLETTER SIGN-UP" form with an input field for "Enter your email" and a "Submit" button.

Circular

Conflict Minerals Tracking




The image shows a screenshot of a Forbes article. The top navigation bar includes the Forbes logo and links for Billionaires, Innovation, Leadership, Money, Consumer, Industry, Lifestyle, Featured, BrandVoice, Lists, and Advisor. A search icon is visible on the right. The main text of the article discusses the use of Oracle Blockchain Platform for conflict minerals tracking. A photograph of a man in a blue sweater is positioned at the bottom of the article.

Forbes Billionaires Innovation Leadership Money Consumer Industry Lifestyle Featured BrandVoice Lists Advisor

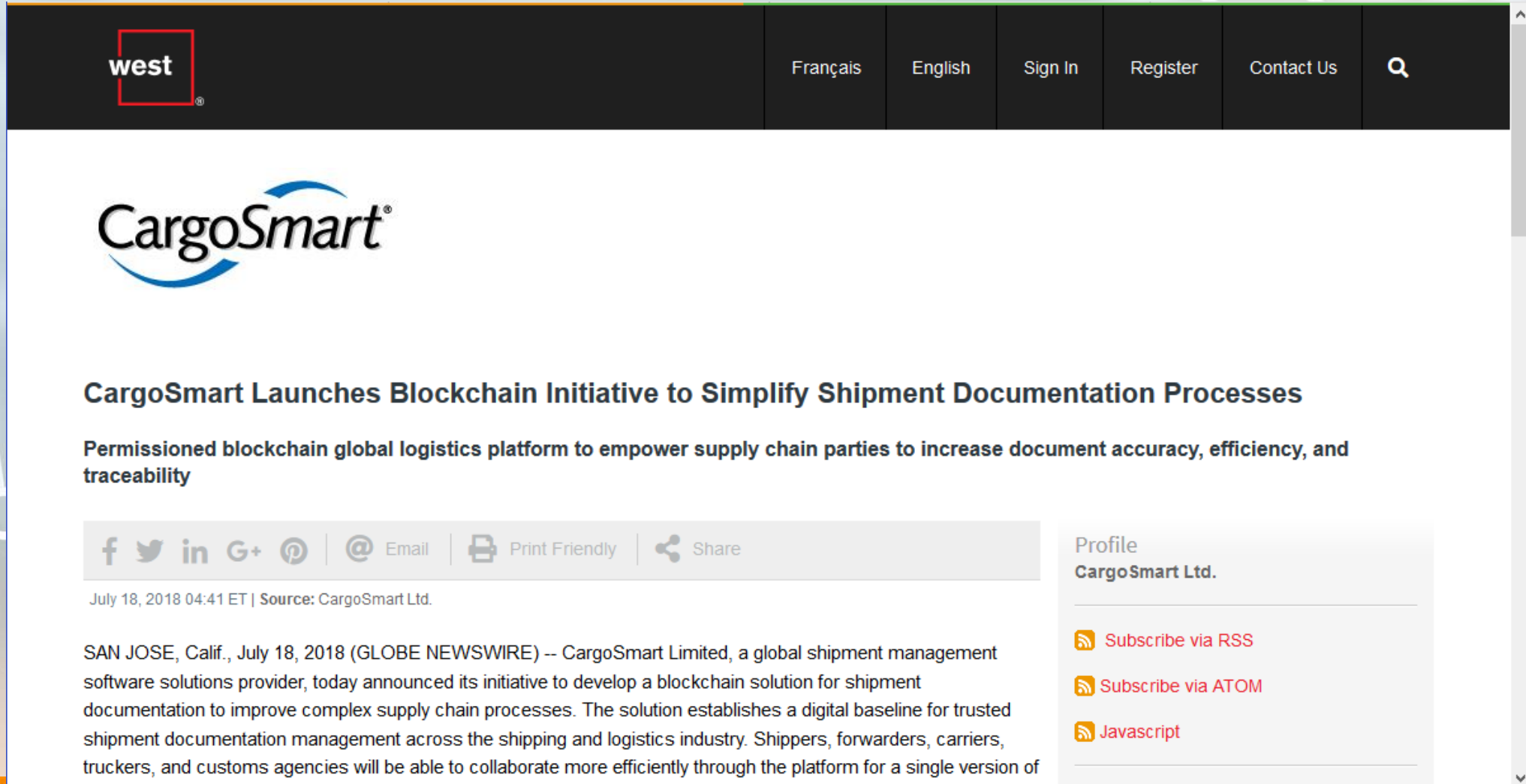
introduce that trust, because every transaction, every document, is on a shared ledger that is visible to everybody and is endorsed by the appropriate parties,” Nainani says.

London-based **Circular** is at the center of such activity. Using **Oracle Blockchain Platform**, it’s helping companies ensure that the raw materials in their products are sourced ethically and in compliance with regulations by tracing materials through the entire supply chain, from their origin to the finished product.



CargoSmart

Maritime Shipment Documentation Process



west

Français English Sign In Register Contact Us

CargoSmart

CargoSmart Launches Blockchain Initiative to Simplify Shipment Documentation Processes

Permissioned blockchain global logistics platform to empower supply chain parties to increase document accuracy, efficiency, and traceability

f t in G+ p | @ Email | Print Friendly | Share

July 18, 2018 04:41 ET | Source: CargoSmart Ltd.

SAN JOSE, Calif., July 18, 2018 (GLOBE NEWSWIRE) -- CargoSmart Limited, a global shipment management software solutions provider, today announced its initiative to develop a blockchain solution for shipment documentation to improve complex supply chain processes. The solution establishes a digital baseline for trusted shipment documentation management across the shipping and logistics industry. Shippers, forwarders, carriers, truckers, and customs agencies will be able to collaborate more efficiently through the platform for a single version of

Profile
CargoSmart Ltd.

- Subscribe via RSS
- Subscribe via ATOM
- Javascript

Certified Origins

Provenance of Extra Virgin Italian Olive Oil

Tuesday, May 28, 2019

enterprise times

NEWS NEWS IN BRIEF FEATURES BLOGS PODCASTS TIPS MEET THE TEAM PREMIER PARTNERS

Home > Latest News > Blockchain > Extra Virgin Olive Oil (EVOO) proven by Oracle blockchain

Latest News Blockchain

Extra Virgin Olive Oil (EVOO) proven by Oracle blockchain

By Charles Brett - April 1, 2019

f t G+ in



Certified Origins Italia hopes to transform consumer confidence in the source of Extra Virgin Olive Oil (EVOO) by using Oracle Blockchain in its supply chain. EVOO is one of a number of high value food products susceptible to consumer loss of confidence

(another is wine – as My Story describes). One difference, however, between wine and EVOO is that accusations of fraud in the olive oil industry (selling inauthentic, cheap or

NEWSLETTER

Don't want to miss out on the latest news and stories? Sign up to our weekly newsletter

Your email address

Sign up

FOLLOW US

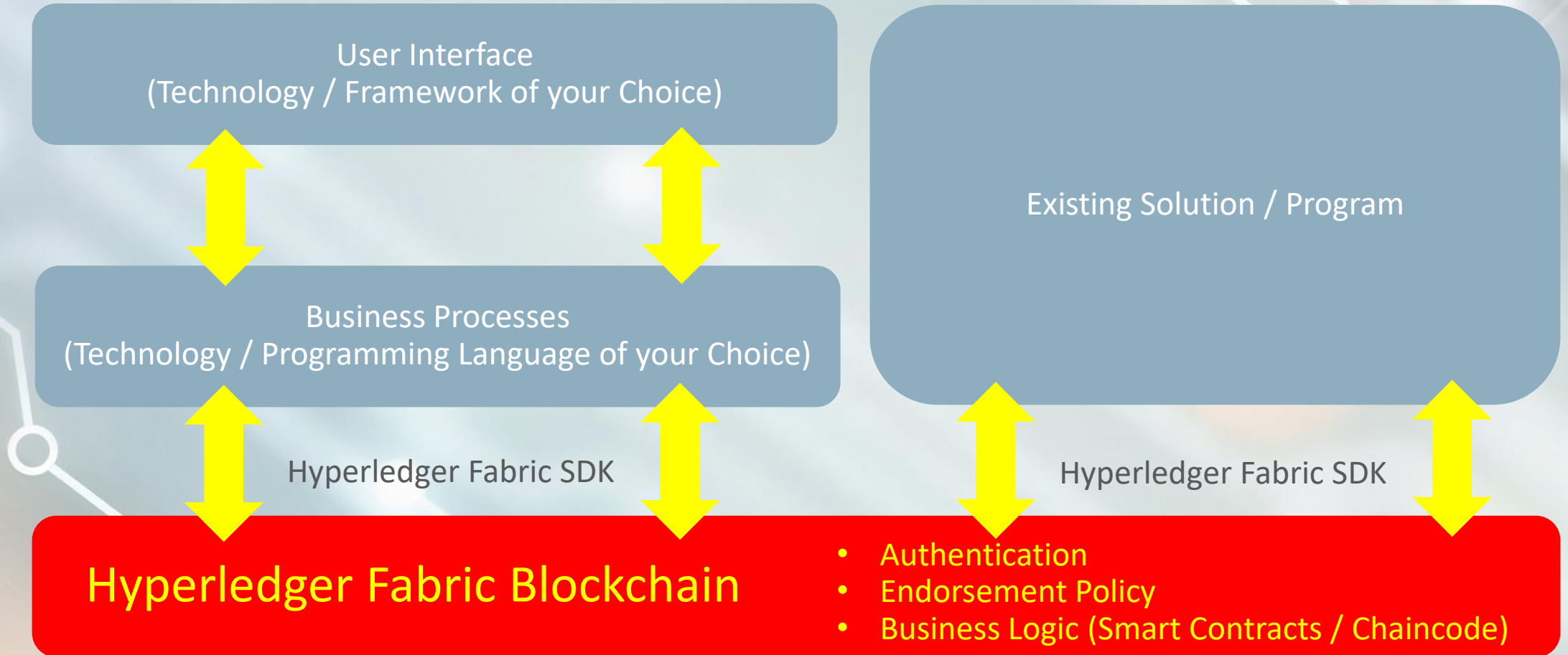
f t G+ in



Architecture

Architecture

Freedom of Choice



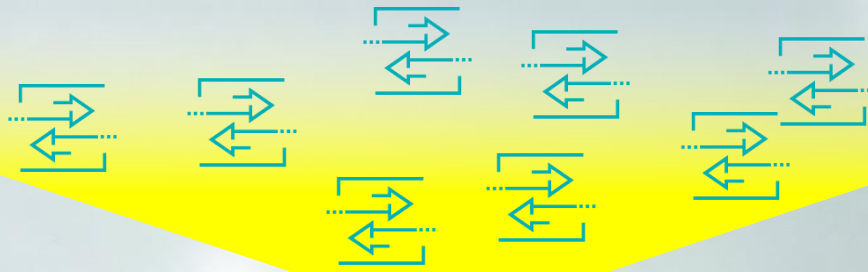
Endorsement & Basic Workflow

Hyperledger Fabric

Endorsing Transactions

More or less generally on Blockchains

Transactions



Order

Execute

(by Peers)



Endorsing Transactions

Hyperledger Fabric

Transaction
Proposals

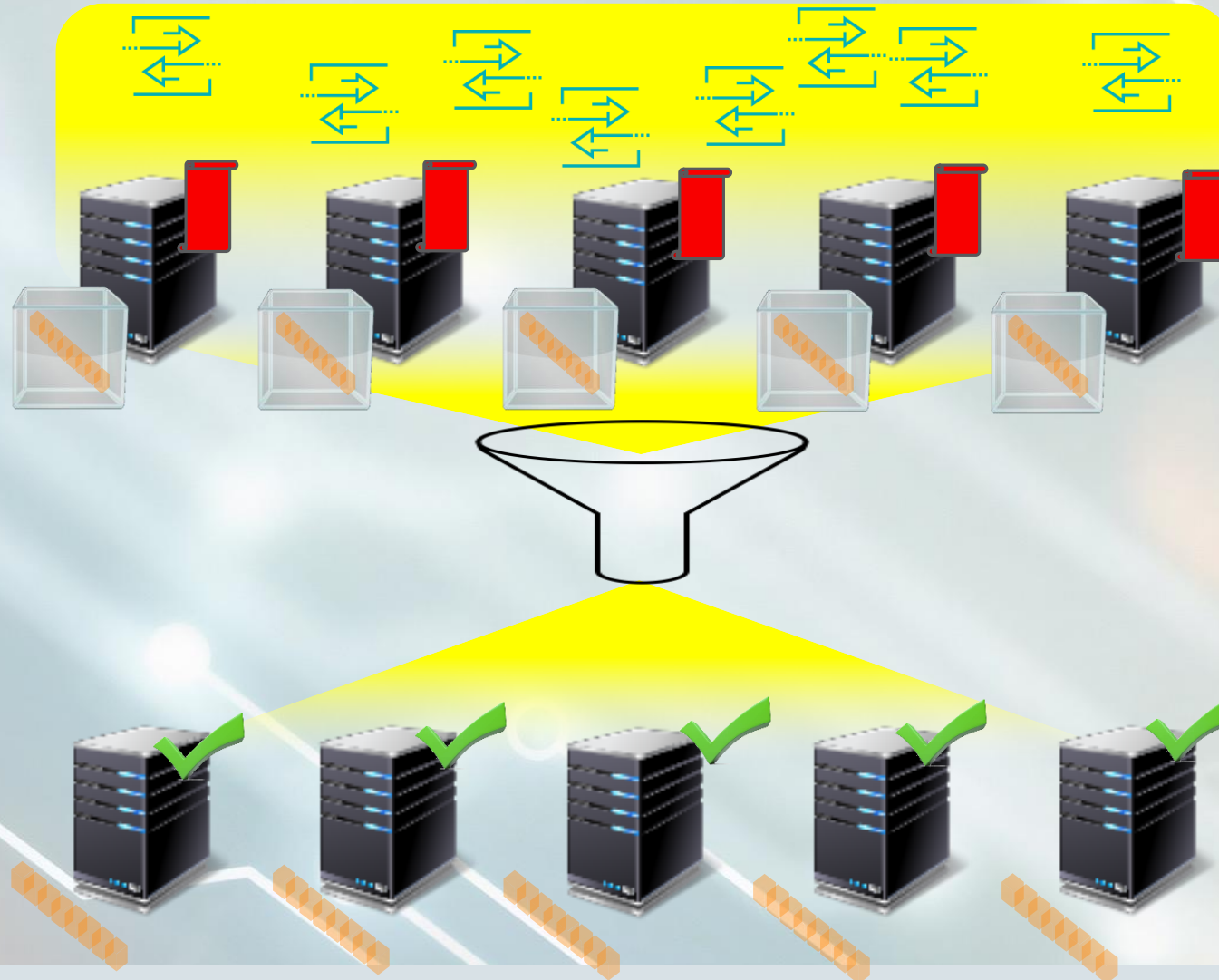
Execute

(by Peers who
are also
Endorsers)

Order

Validate

(by Peers)





Client



peer0



peer1

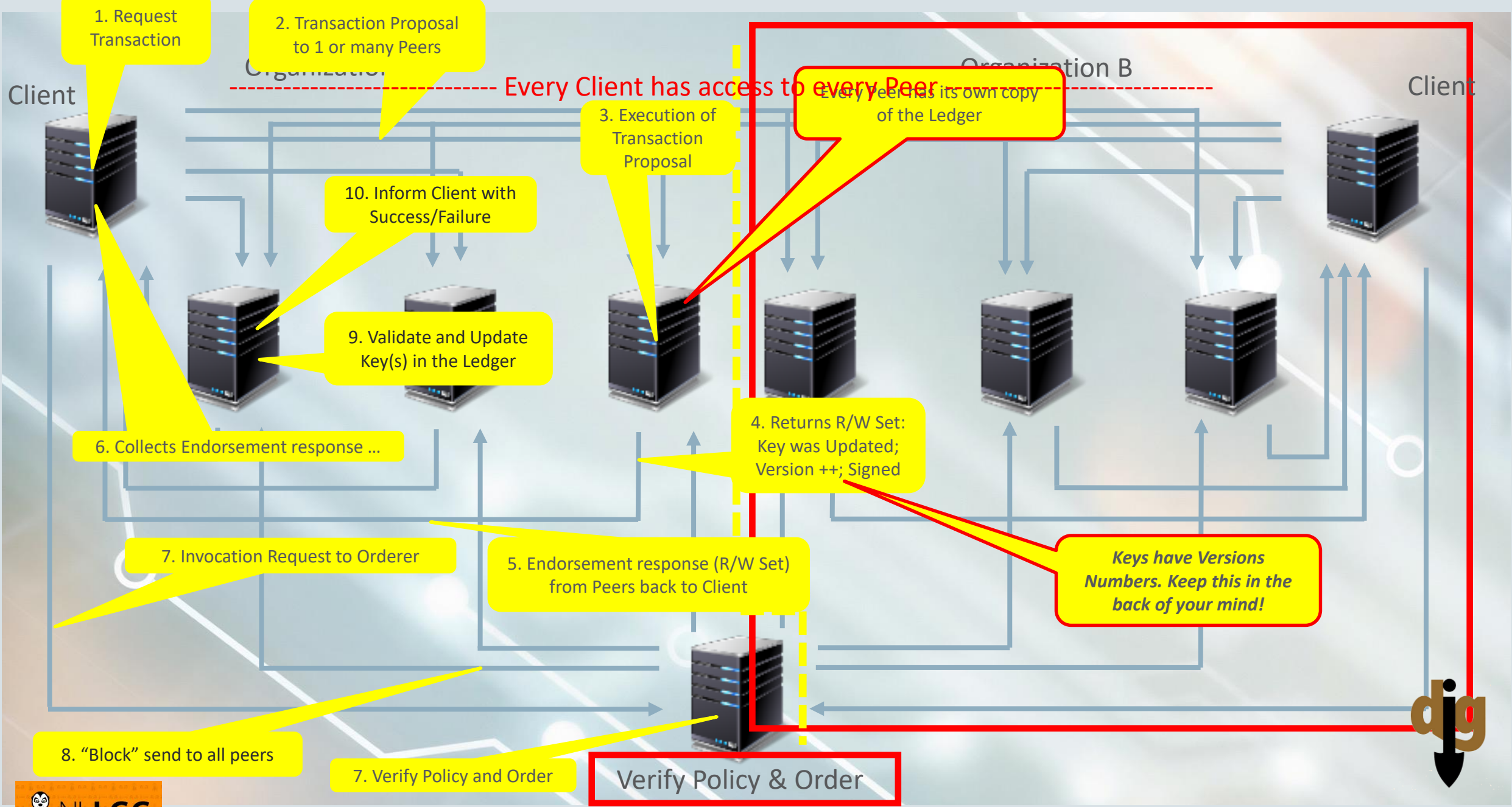


peer2

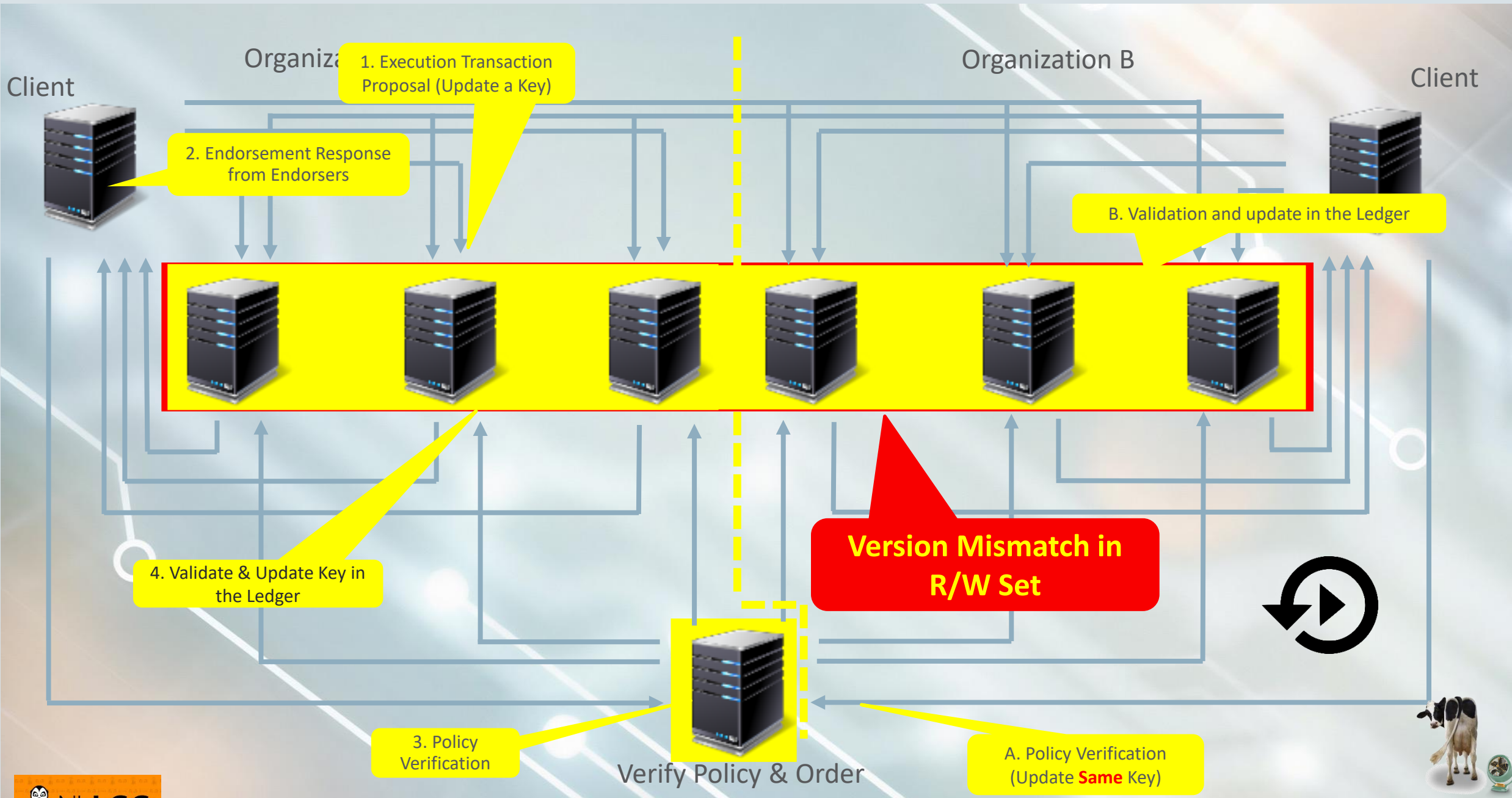


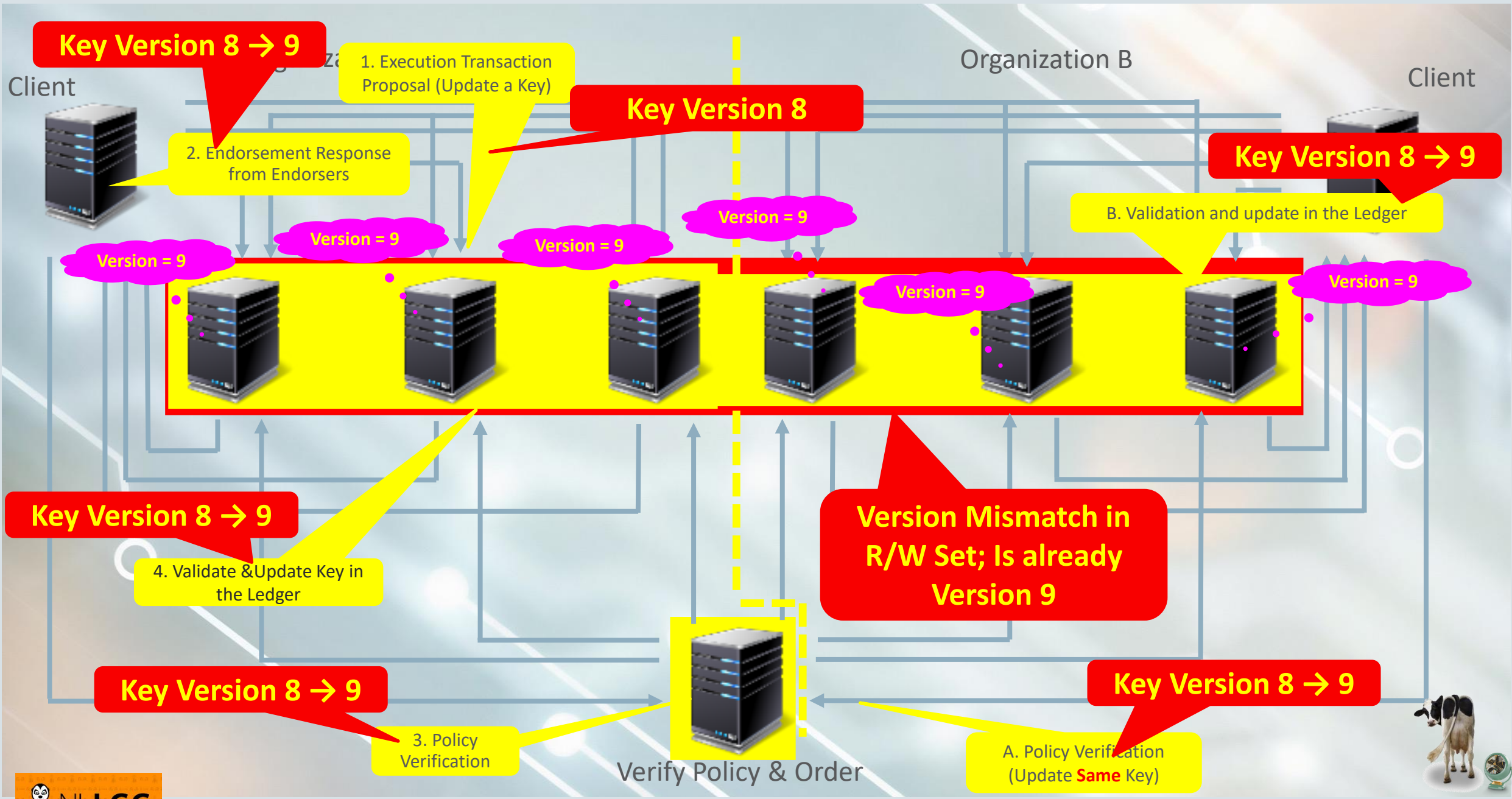
Orderer













The Ledger

Hyperledger Fabric

The Ledger

Every Channel has it's "own" Ledger



Writing to the Ledger

TxValid = True



World State Database

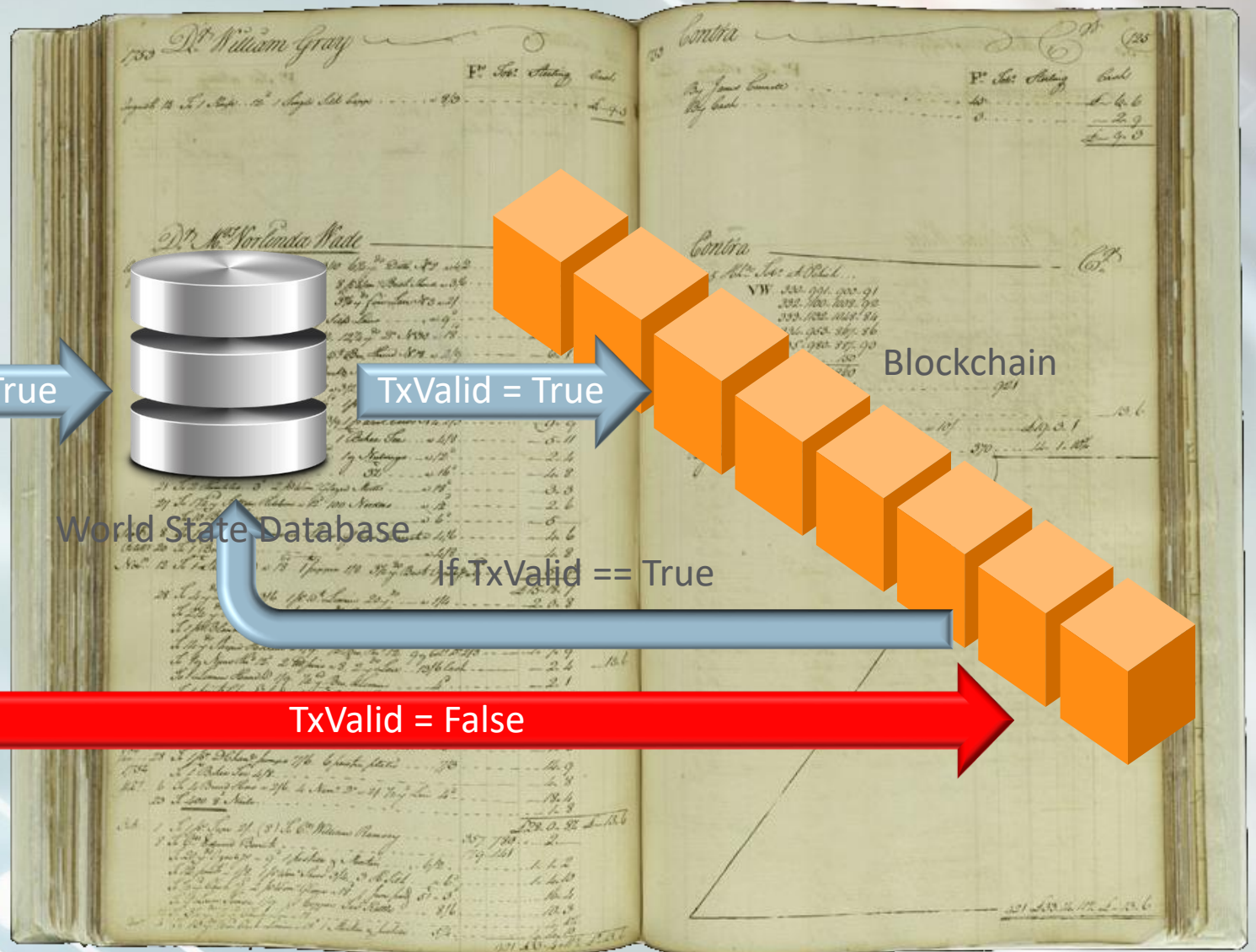
TxValid = True

Blockchain

If TxValid == True

TxValid = False

Writing to the Blockchain





What are oracles & Why do we need them?

In ancient Greek mythology, **oracles** were known as spiritual beings & sources of **infinite wisdom & knowledge** due to their connection communication with the gods on Mount Olympus (the spiritual world)



BLOCKCHAIN

oracle



A



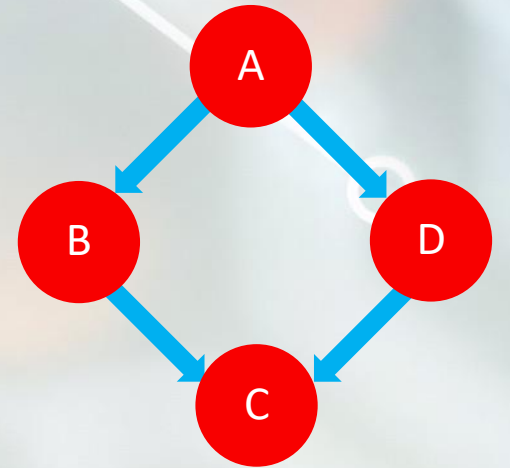
B



C

Deterministic

Gives it immutability but reduces flexibility



A

B

C

D

Non-Deterministic

Increased flexibility but creates problems with transparency

WrtTemp(28,x23)

Client

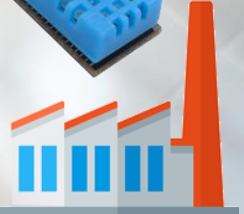
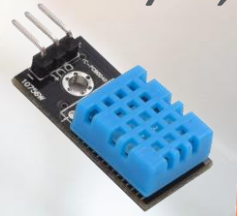


peer0



```
Func WrtTemp(FctryID, tDev)
{
  t=GetTemp(tDev);
  WriteValue(FctryID, t);
}
```

$T \pm 0,001^\circ$



Pharmaceutical



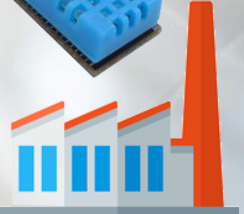
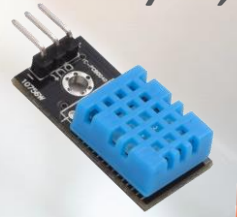
Orderer

WrtTemp(28,x23)

Client

Endorsement Policy: 3 Endorsers

T +/- 0,001°



Pharmaceutical

peer0

peer1

peer2

Use an oracle

Call with FactoryID, DeviceId and **Defined Date & Time**

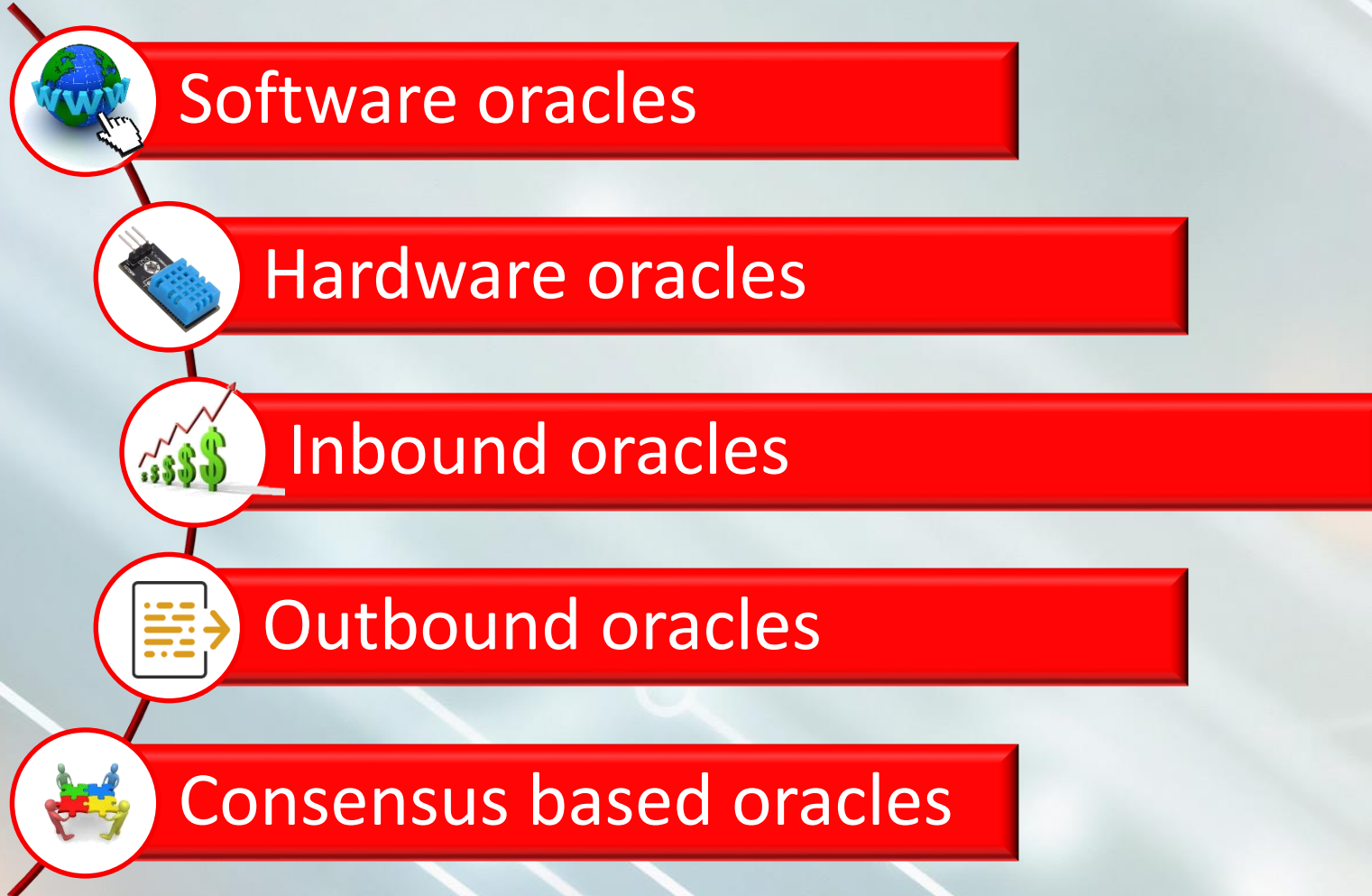


Orderer



RWSets are not equal ... STOPPING is probably the most sensible thing todo

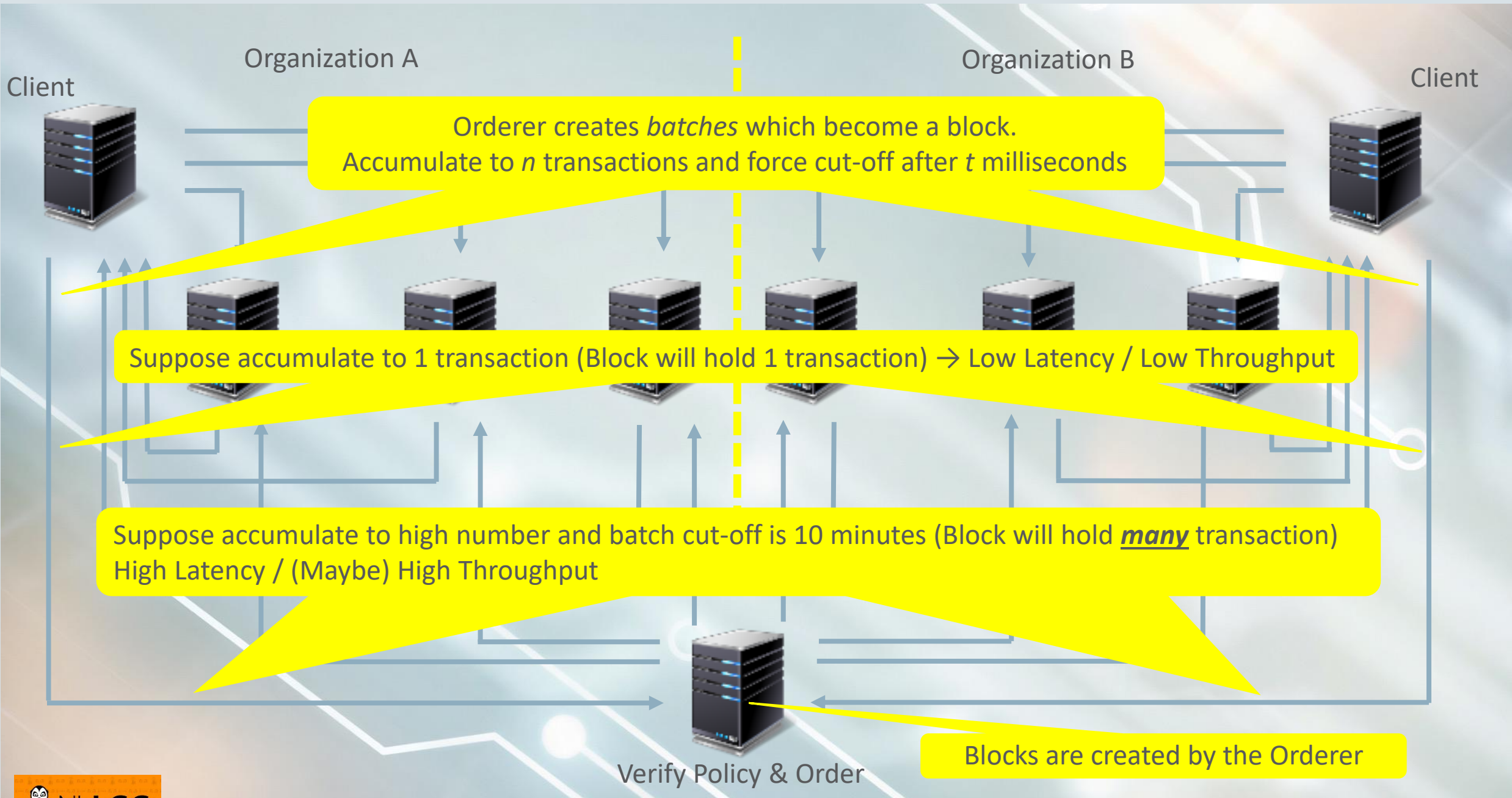
oracle types

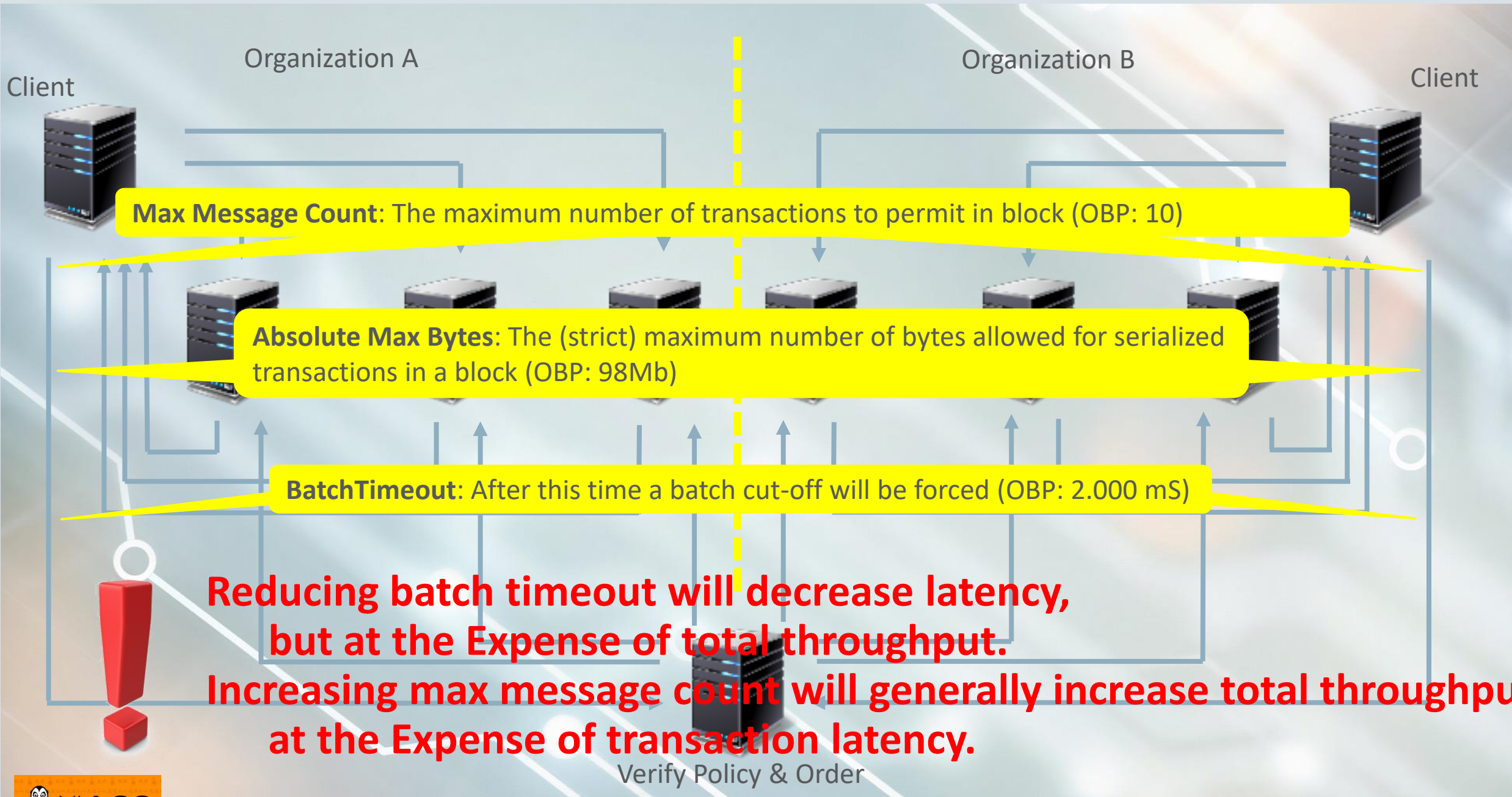




Blocksize

Hyperledger Fabric







Hot Keys

Remember Row Locking from Database World

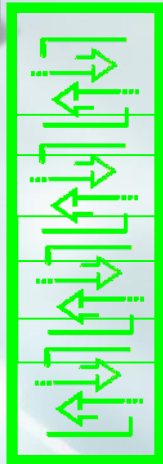
Client



peer0



TxCnt Version = 8



- ✓ Version → 9
- ✗ 8 ≠ 9
- ✗ 8 ≠ 9
- ✗ 8 ≠ 9

**TxCnt Version = 8
Write TxCnt →
Version ++**



Orderer

Max Message Count = 4

Hot Key!

```

Func Whatever()
{
  ...
  cnt=GetValue(TxCnt);
  cnt++;
  WriteValue(TxCnt, cnt);
  ...
}

```

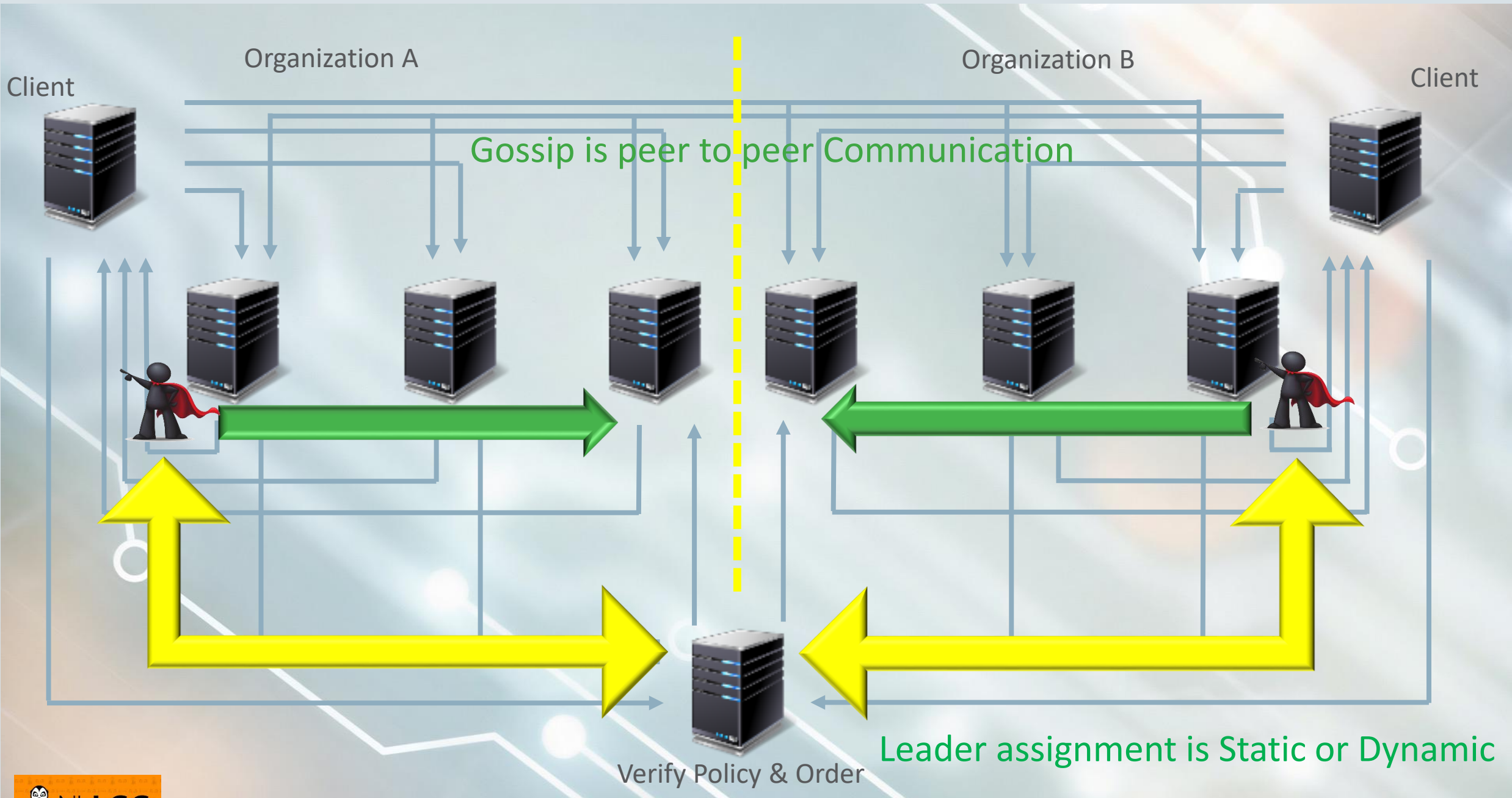


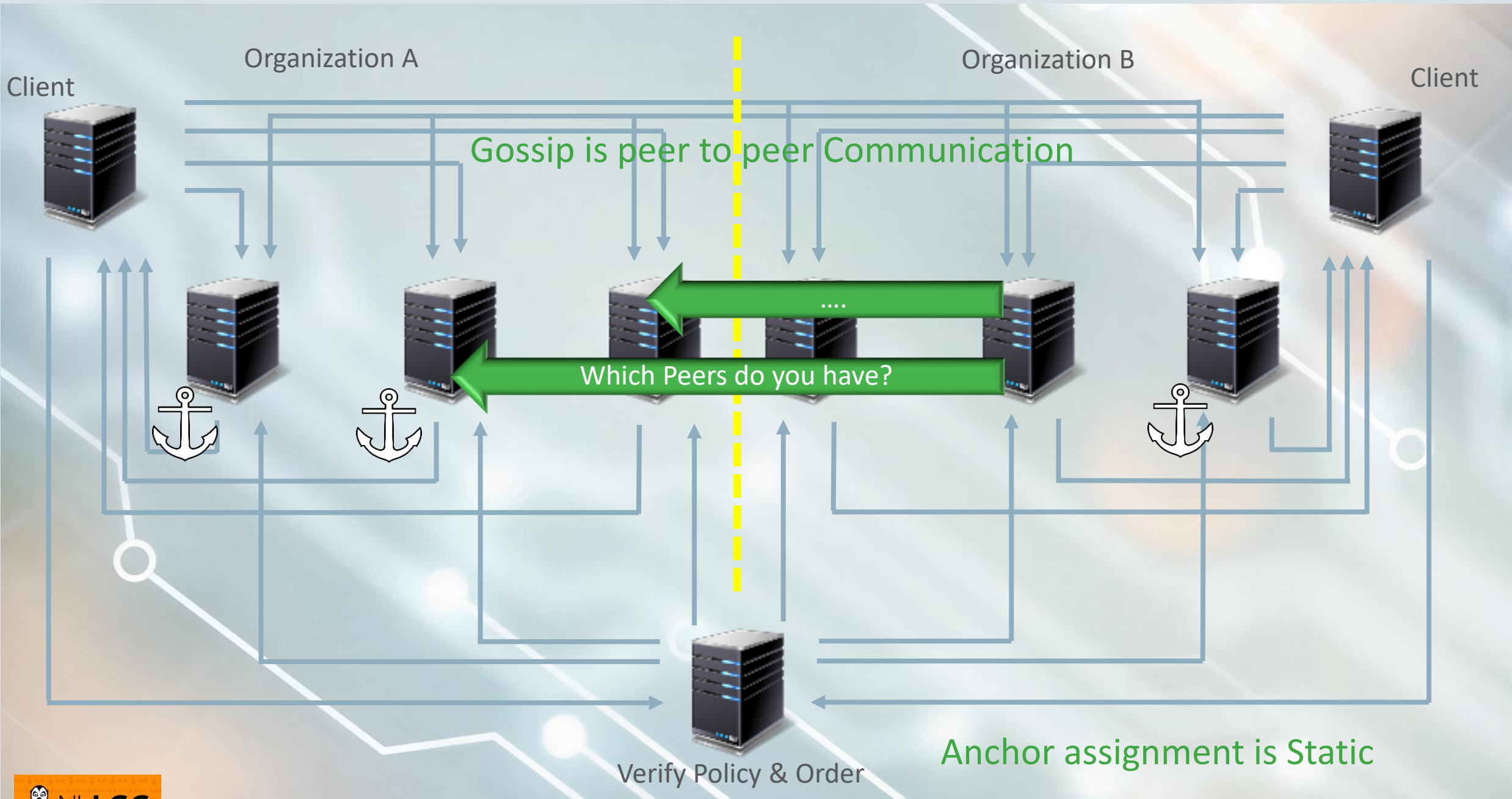


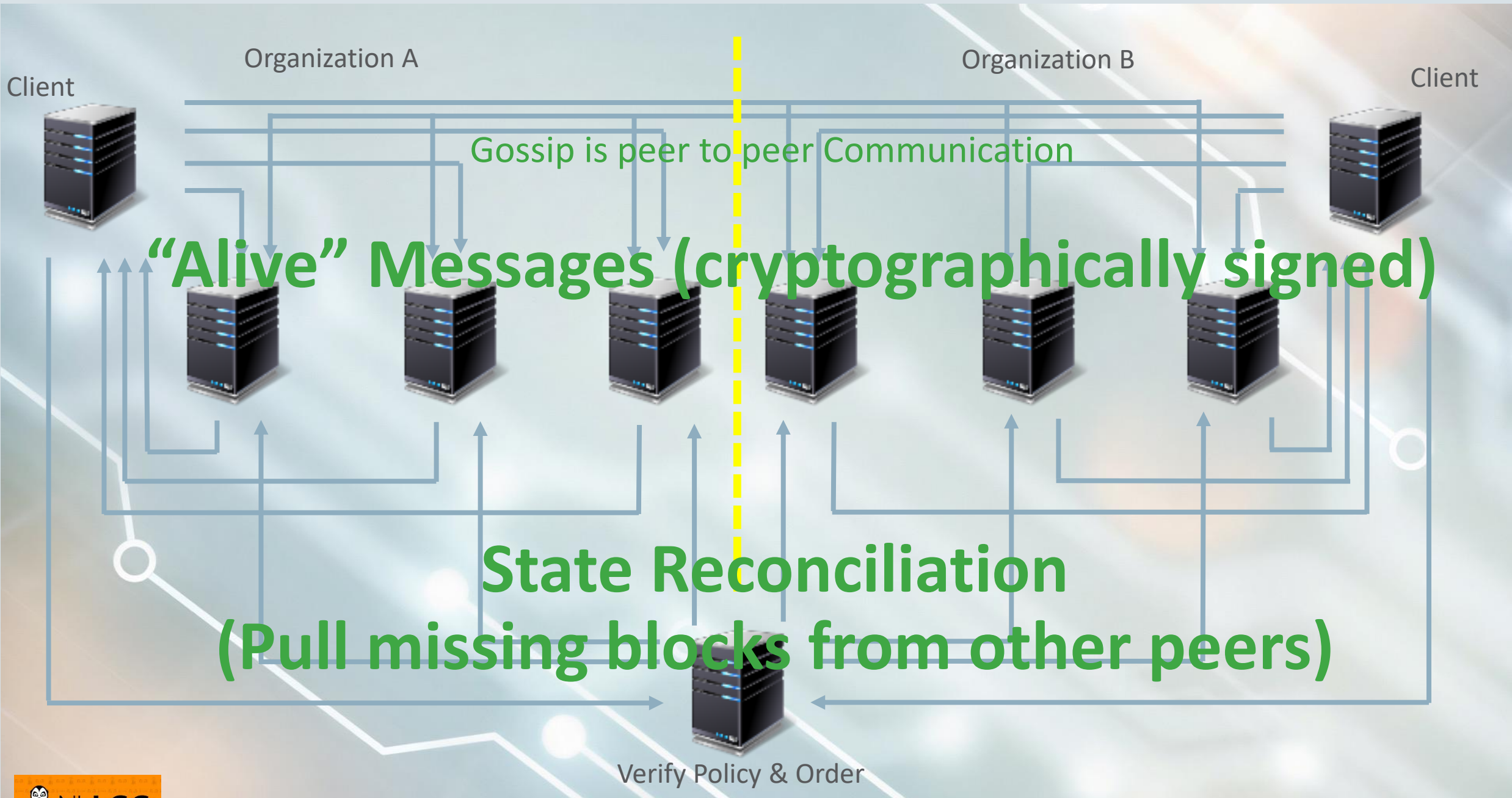
Leader Peer & Ancher Peer(s) and Gossip

Hyperledger Fabric











Defining an Endorsment Policy

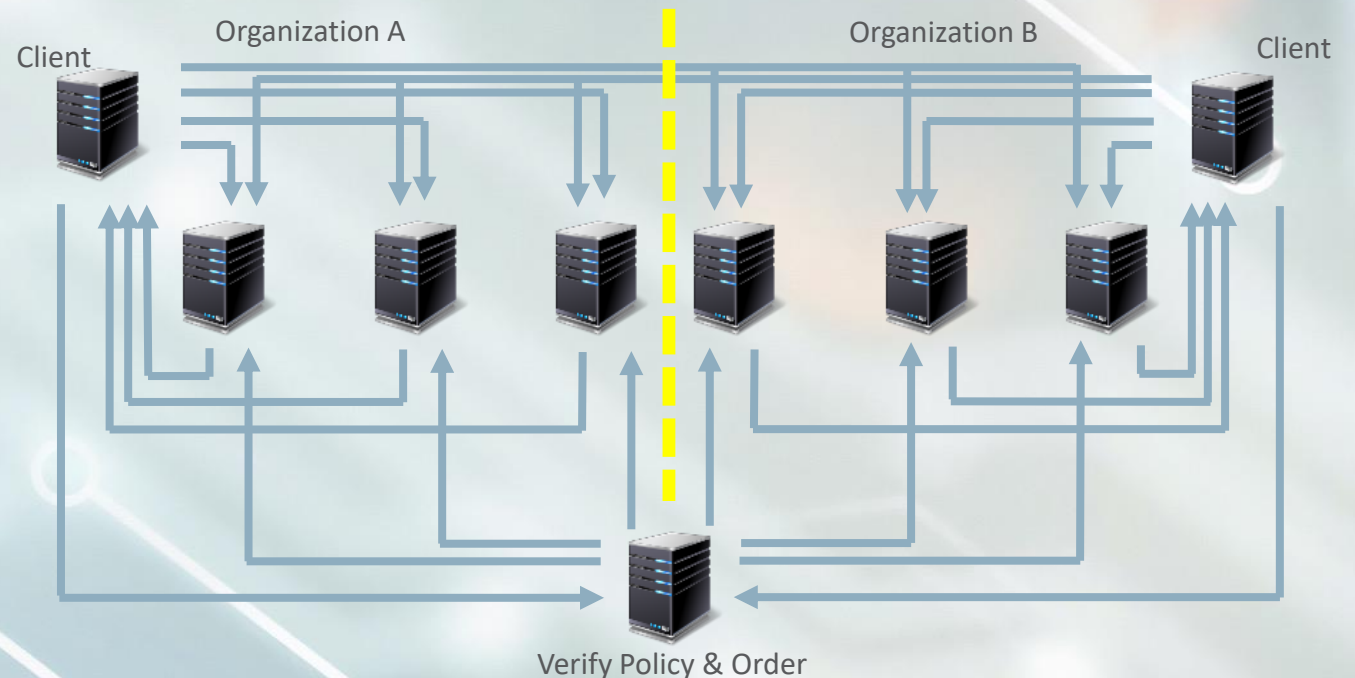
Hyperledger Fabric

Define an Endorsement Policy

From a Technical Point of View

- What would you Consider a good (technical) Endorsement Policy
 - In Real life the Business will also have requirements on the Endorsement Policy
 - Very probably related to trust (or the lack of..)

- Any 1/6
 - 2/6, 3/6, 4/6, 5/6, 6/6
- 1 from A & 1 from B
 - 2/A & 2/B, 3/A & 3/B
- 1 or 2 or 3 from “Myself”
- ...





Private Data (SideDB)

Hyperledger Fabric

Car Factory



Sell 1234567890

Car Dealer 1



Car Dealer 2



CarPart Data

ItemNR: 1234567890

SerialNR: 0987654321

Name: Wheel

Size: 17 Inch

Colour: Silver

Owner: *Changes Over Time*

Price: *...It depends ...*

Car Factory



Car Dealer 1



Endorsement Policy:
1 Peer of 1 Organization

Car Dealer 2



Sell 1234567890

Factory Client does Transaction Request to "1 Peer of Factory"

```
sellpart(ItemNR, SerialNR, newOwner, price);
```

Peer returns **RWSet**

Collected by Factory Client; Send to Orderer

Orderer does Policy Check; Create Block; Send to **ALL Peers**

Every Peer Validates **RWSet; Commit**

**PRIVATE
EVENT**

Private Data Solution

- Private Data is stored in a “Collection”
 - Non-Private Data is in the Transaction and stored in the Ledger
- Goal is to Exclude Private Data from Transaction
 - No Private Data Through Orderer
- Private Data is shared peer-to-peer with authorized peers
 - Defined within the “Collection”
- Hash of Private Data is Included in Transaction and stored in State Database
 - Hash serves as evidence of Private Data
 - Hash is used for Validation of Private Data

Transaction & Collection

Transaction

Primary RWSet

- ItemNR, SerialNR, Name, Size, Colour, Owner
Hashed Private RWSet

Who will be allowed to receive this Data

Required

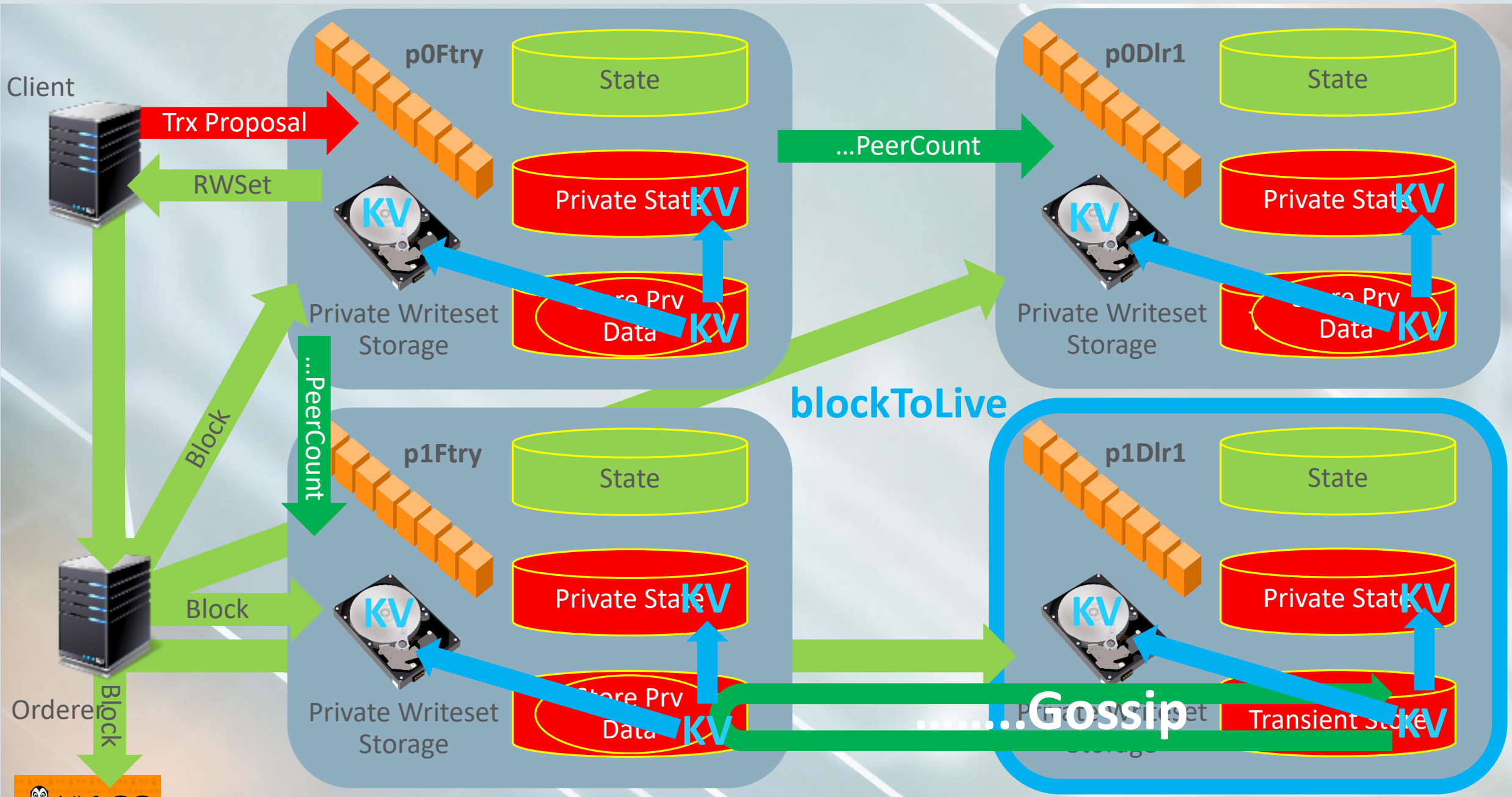
Dissemination during Endorsement

Collection: CarPart Private Details

- Private Write Set
 - Price
- Policy: Ftry, Dlr1
requiredPeerCount: 1
maxPeerCount: 2
blockToLive: 3

Attempt to Disseminate during Endorsement

Time to live in block count





Hyperledger Fabric Overall Performance

Language of Application

Client



Chaincode Language

peer0



peer1



peer2



(Virtual) Iron & (Virtual) Infrastructure

Distribution of Work in Blockchain Network

World State Database

Consensus Mechanism

Block Size



Orderer





Arjan ten Hoopen

500+
connections

Domain Architect Blockchain & Digital
eXperience at Oracle
Almere Stad Area, Netherlands
| Information Technology and Services

Current	Oracle
Previous	Oracle, Oracle Corporation, Stellant
Education	HTS Enschede
Recommendations	1 person has recommended Arjan ten Hoopen

Thank you

Happy to Connect
www.linkedin.com/arjantenhoopen



NLLGG

Nederlandse Linux Gebruikers Groep

Vereniging voor iedere Linux- en open source-liefhebber