Trusting The World of Tomorrow

IOT data and Blockchain

Lionel Florit

lflorit@cisco.com

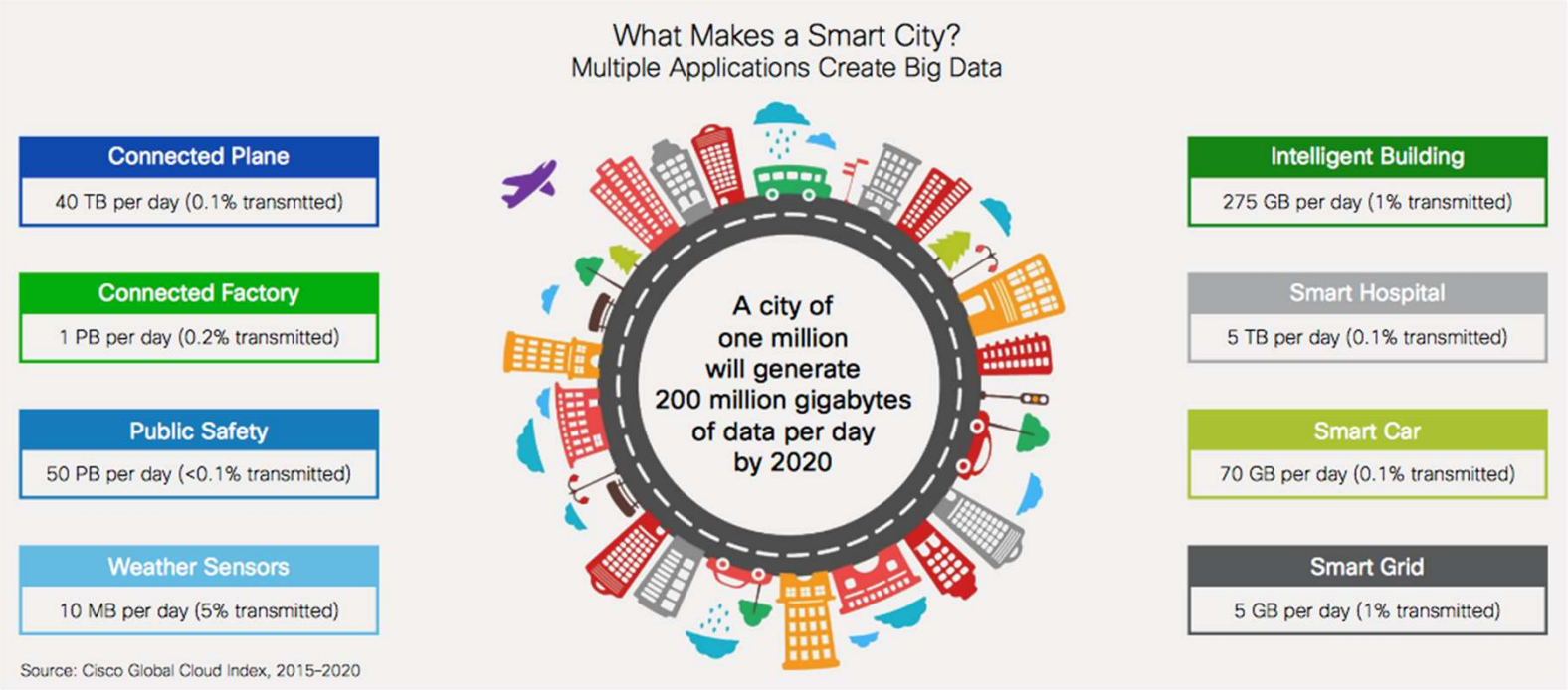
www.linkedin.com/in/lflorit

Look For the Geek-o-Meter

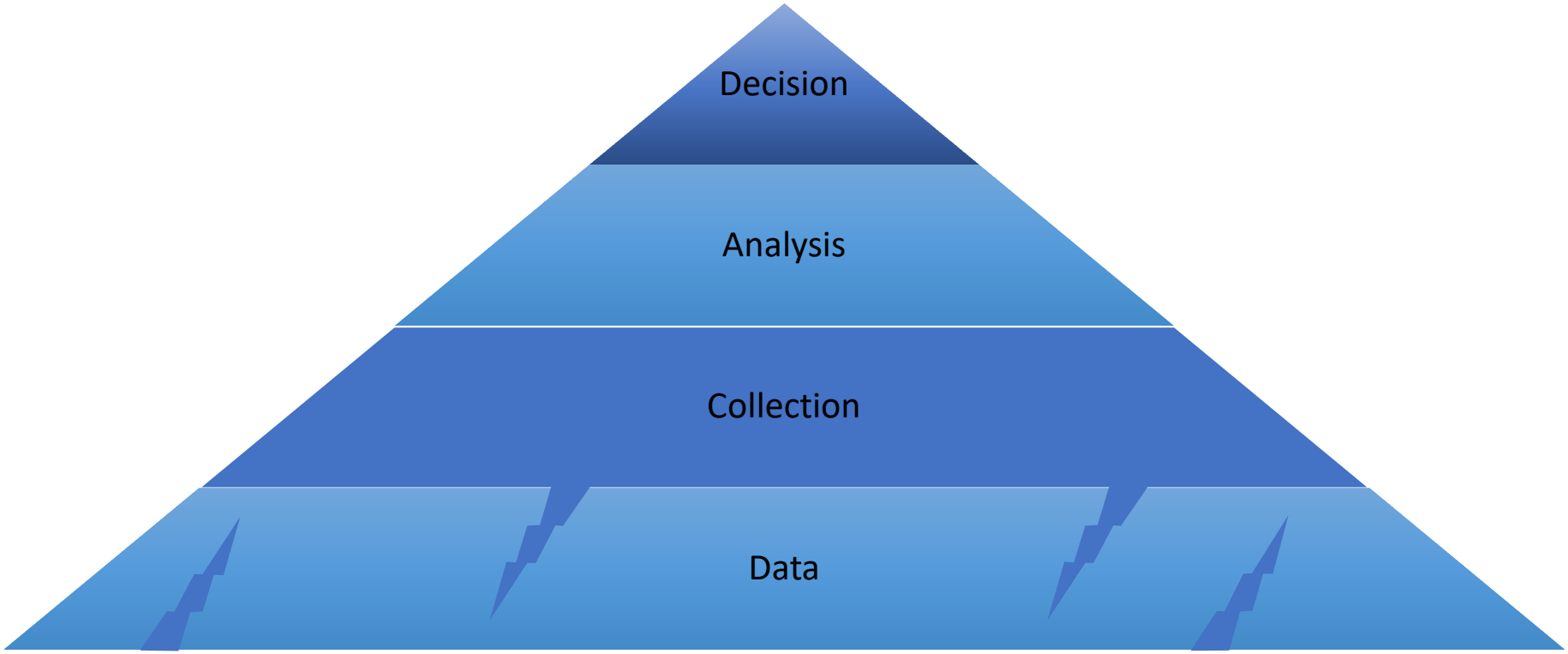
Agenda

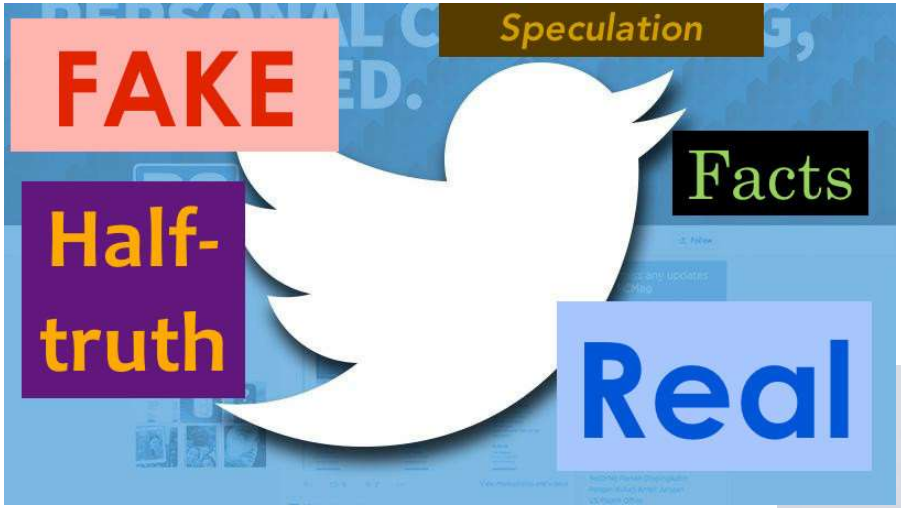
- Problem positioning
- Components of the solution
  - Fog computing
  - Blockchain
- More Use Cases
- Conclusion

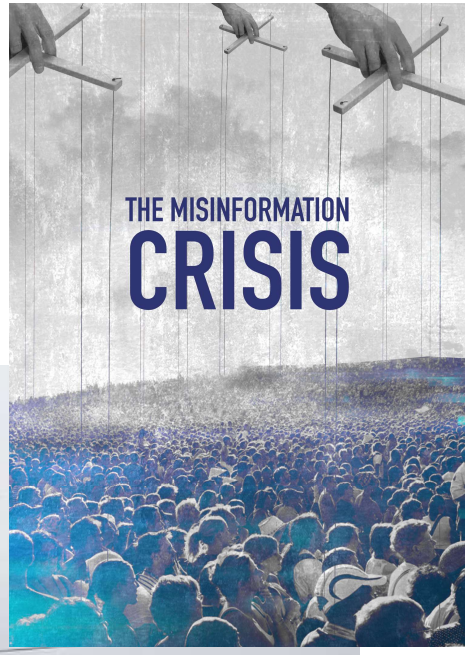
Our Lives Are Regulated by IOT Data



What Happens To The Data?




Speculation
FAKE
Facts
Half-
truth
Real


THE MISINFORMATION
CRISIS


EXTRA! EXTRA!
READ ALL ABOUT IT!
FAKE
NEWS!

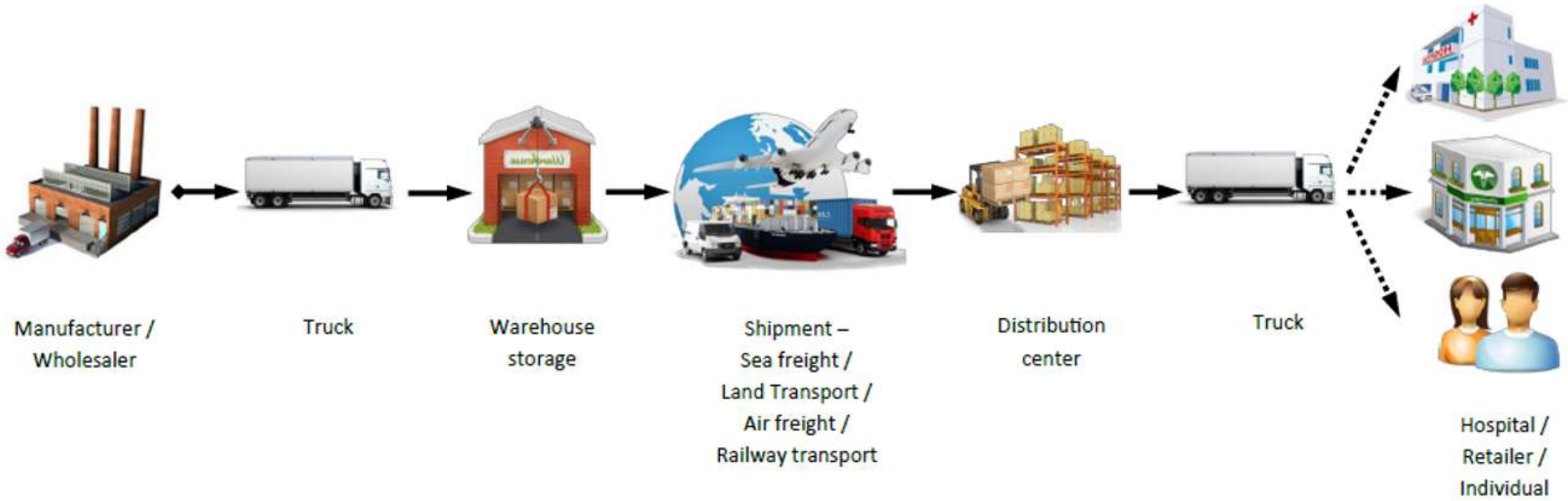
We seek Authentication

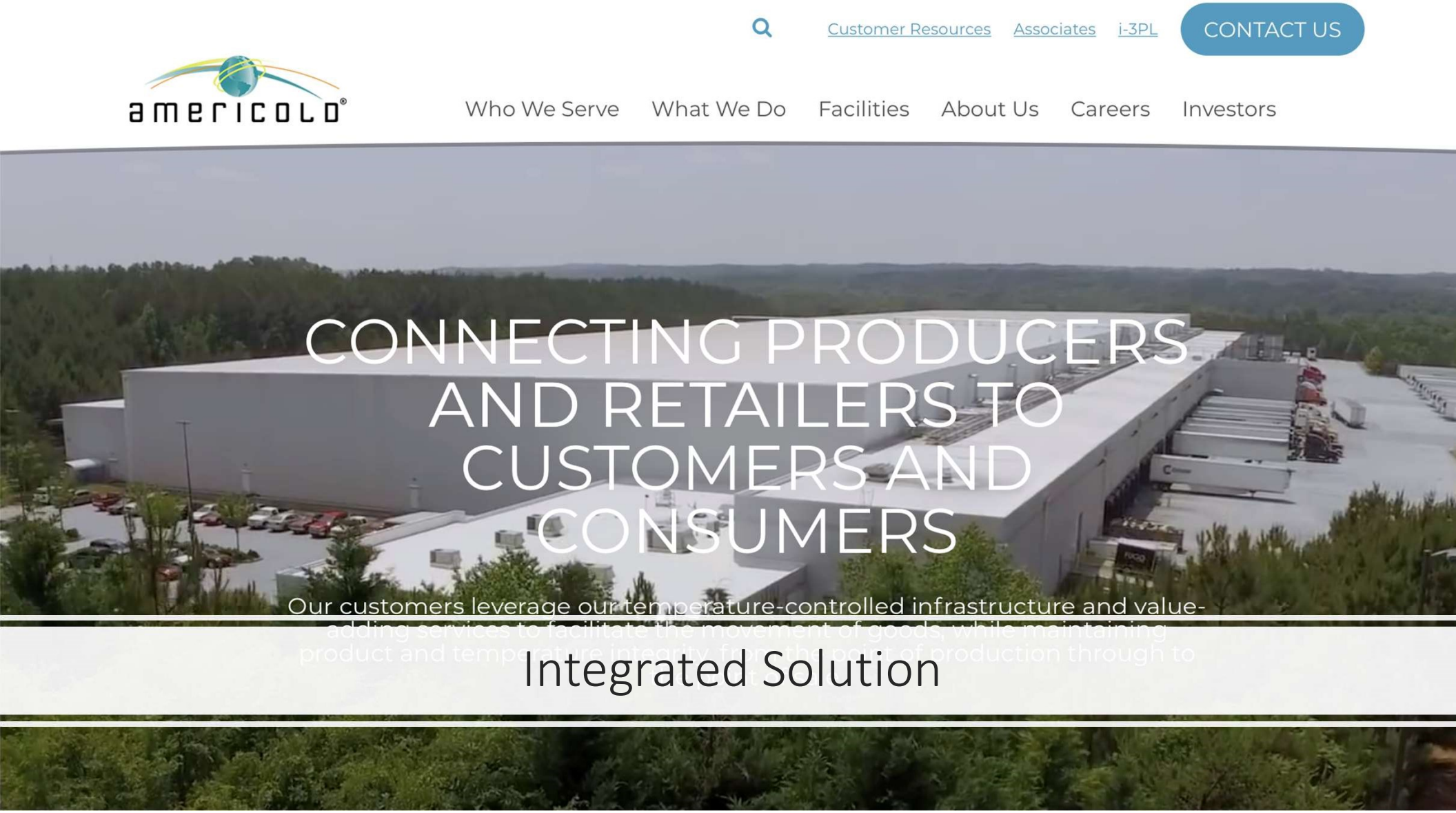
Authentication here means that the message has not been altered in any way

It is the authentic original message as produced by its author.

What if observations were immutable?

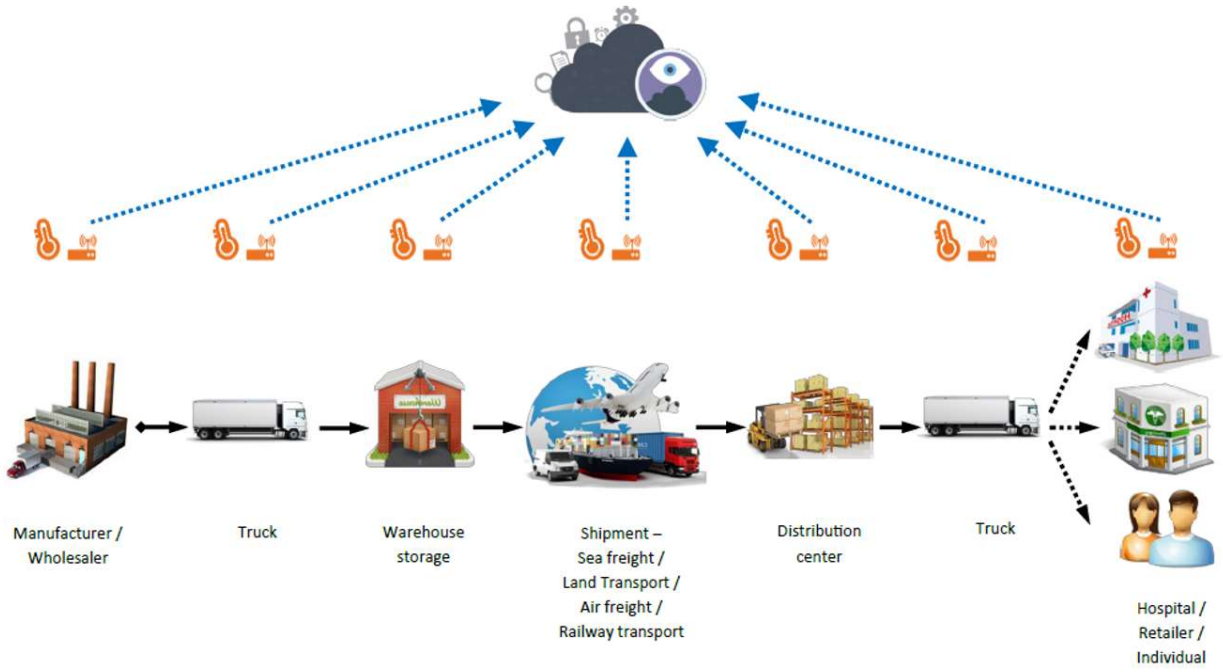
Cold Chain


Manufacturer / Wholesaler
Truck
Warehouse storage
Shipment – Sea freight / Land Transport / Air freight / Railway transport
Distribution center
Truck
Hospital / Retailer / Individual

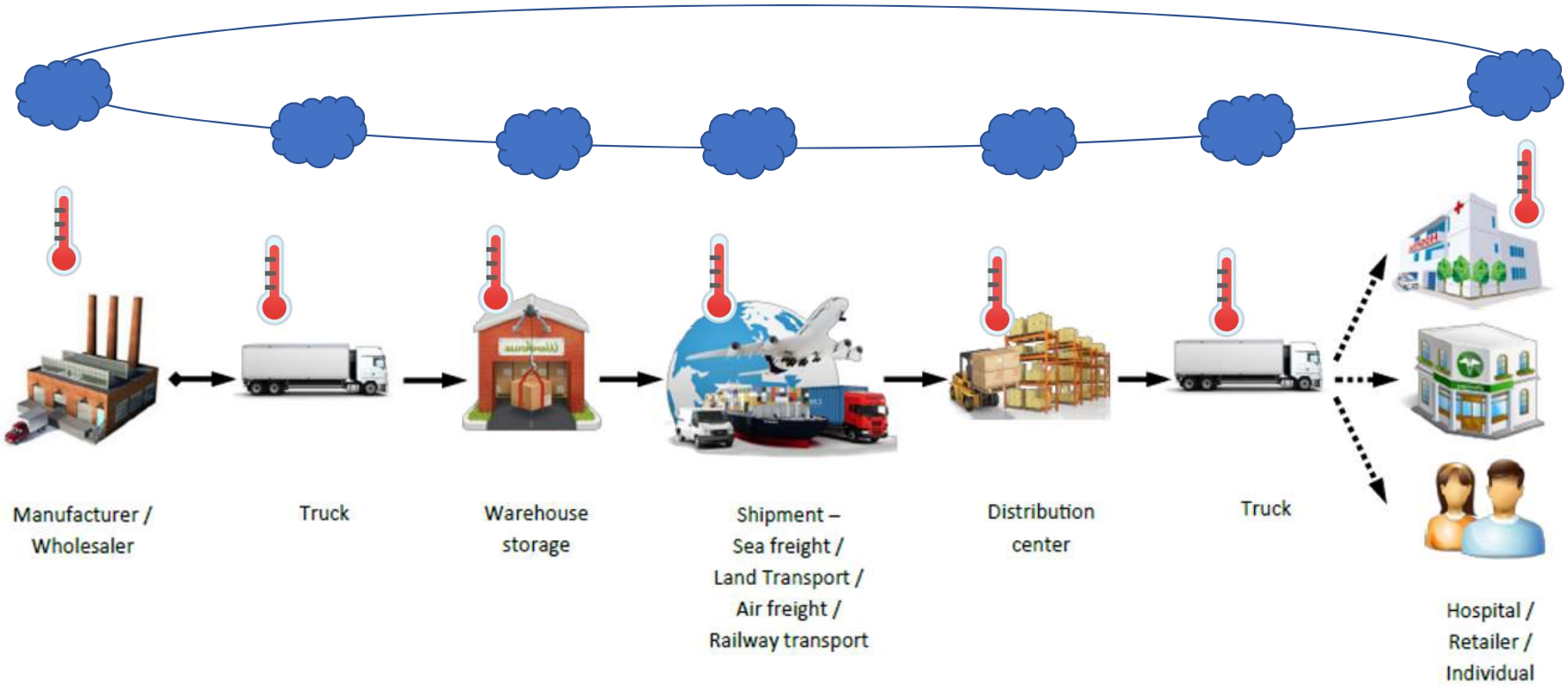


Integrated Solution

Integrated Solution



Distributed Solution



Source ETS Bio Freeze

Solution Building Blocks

Visualization	Dashboards and UIs Backend systems
Sharing	Distributed Ledger Technology
Processing	Run reports Analytics
Aggregation	Private Cloud Distribution layer in networks
Collection	IoT Gateway and the fog layer Marking and metadata
Things	Sensors, machines, tools, vehicles

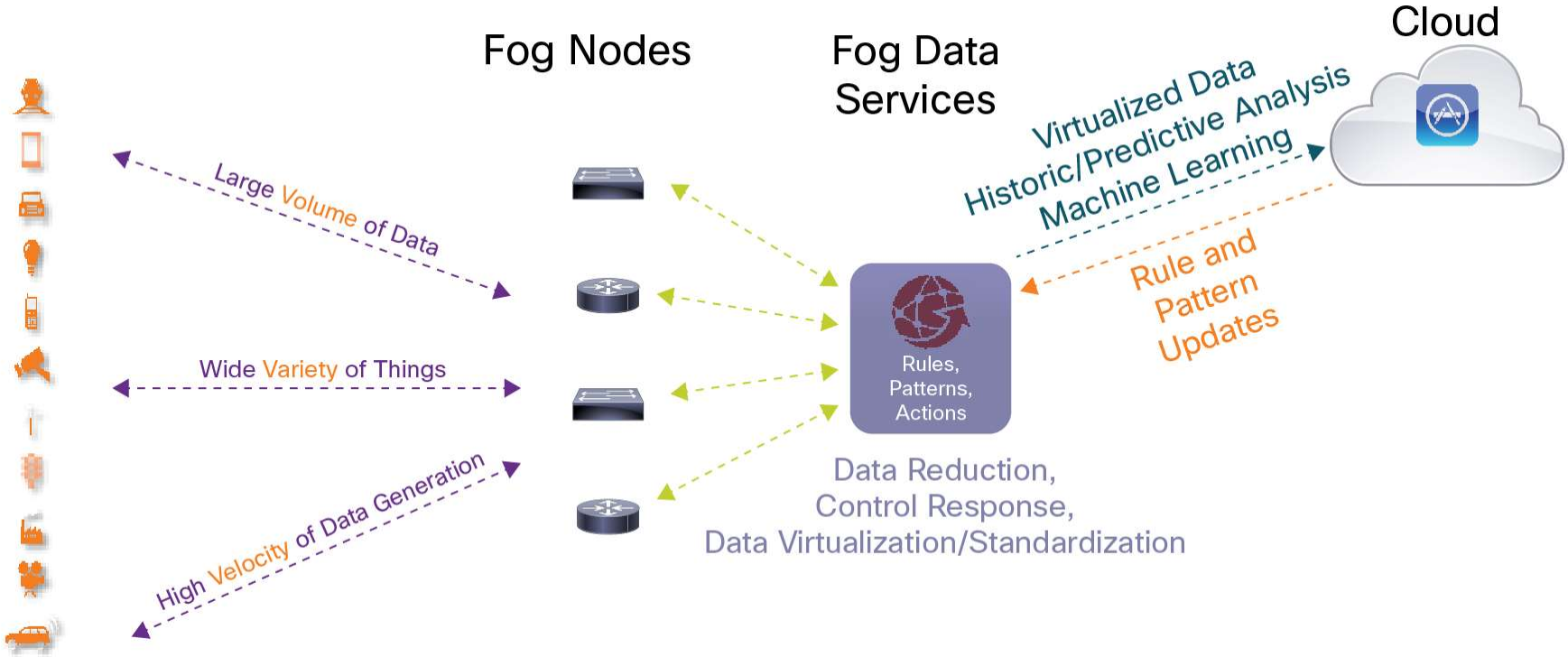
Things: The Data Producers

Visualization	• Dashboards and UIs • Backend systems
Sharing	• Distributed Ledger Technology
Processing	• Run reports • Analytics
Aggregation	• Private Cloud • Distribution layer in networks
Collection	• IoT Gateway and the fog layer • Marking and metadata
Things	• Sensors, machines, tools, vehicles

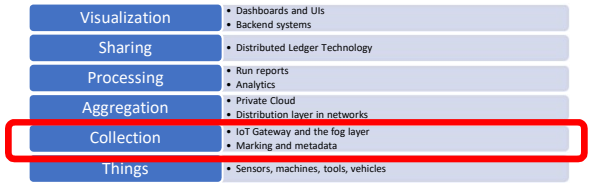
- Most time consuming
- Many shapes
- Many protocols
- Need adaptation and System Integration
- Authentication is a challenge

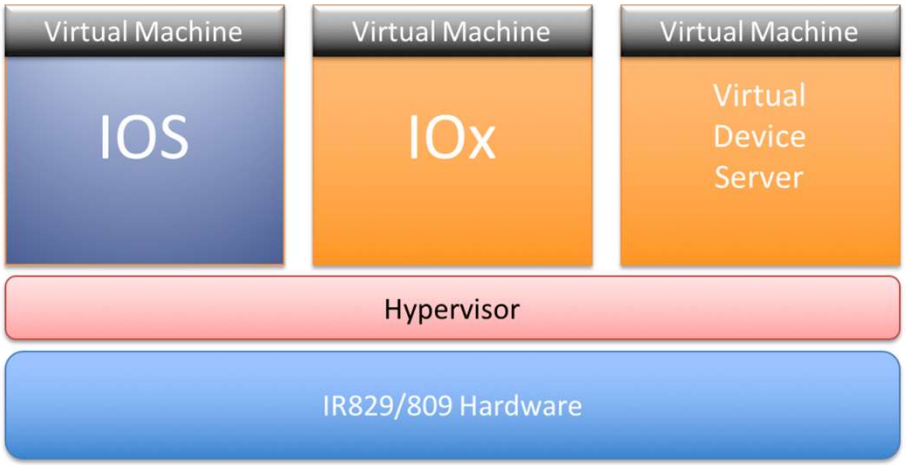
Fog Nodes

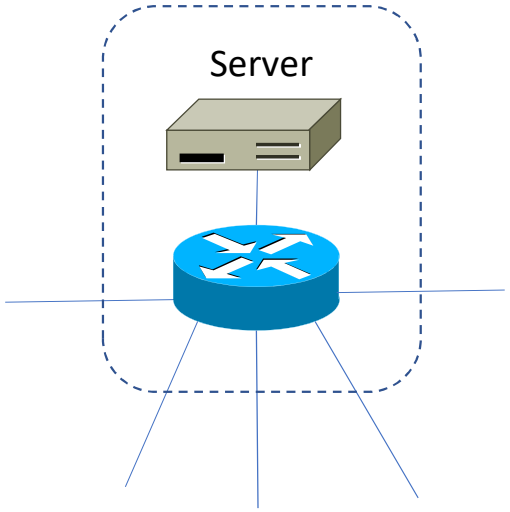
Visualization	• Dashboards and UIs • Backend systems
Sharing	• Distributed Ledger Technology
Processing	• Run reports • Analytics
Aggregation	• Private Cloud • Distribution layer in networks
Collection	• IoT Gateway and the fog layer • Marking and metadata
Things	• Sensors, machines, tools, vehicles



IoT Gateway and Fog Layer

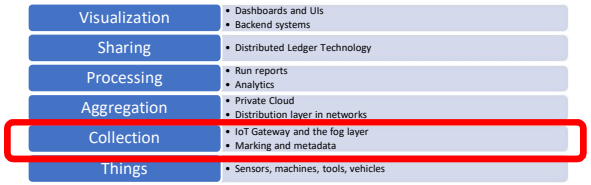


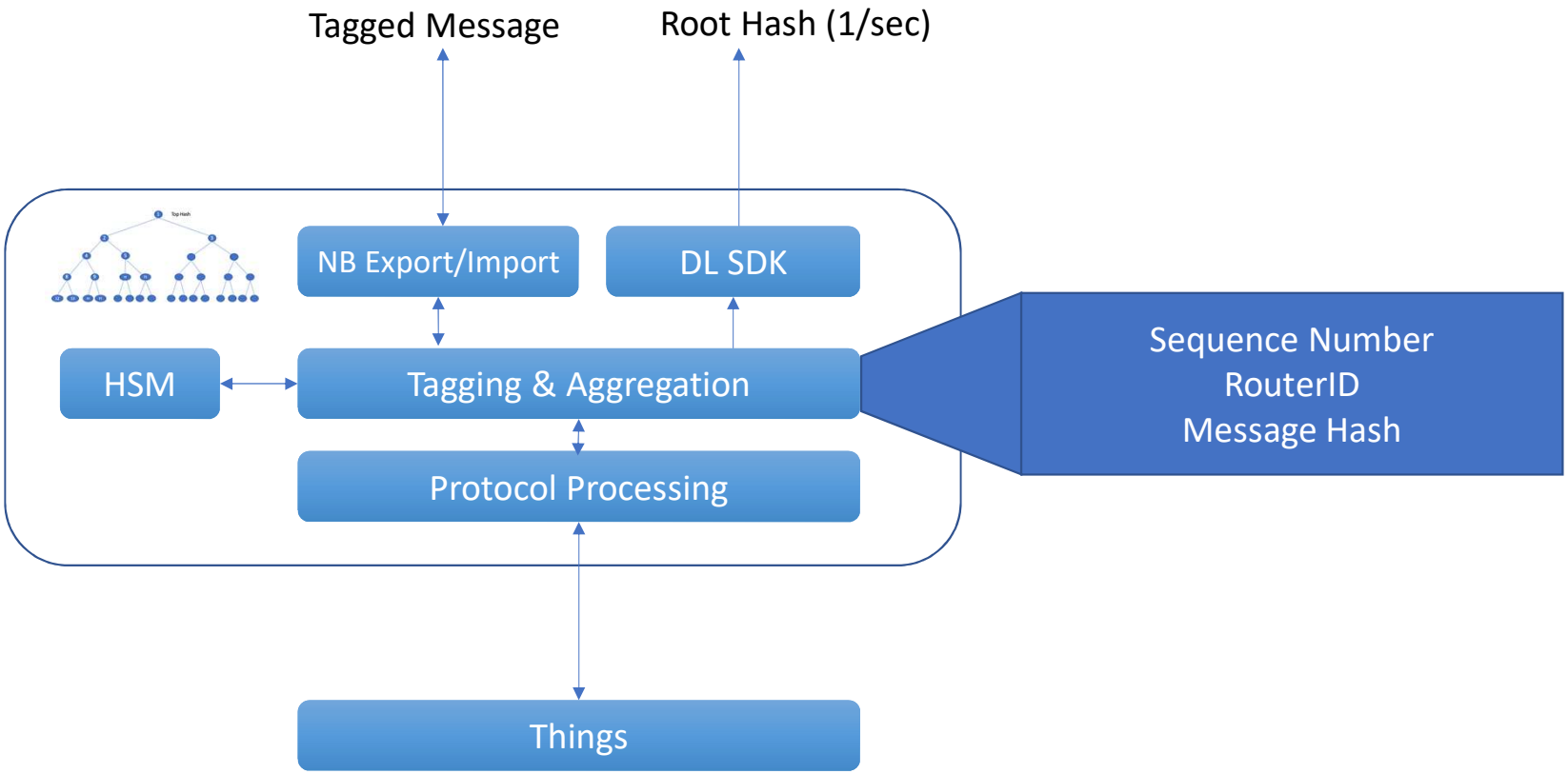




Several routers/switches: IR8XX, IC3000, IR1100, IE4000, ISR800, CGR1000, Cat9k, ISR4K/1K

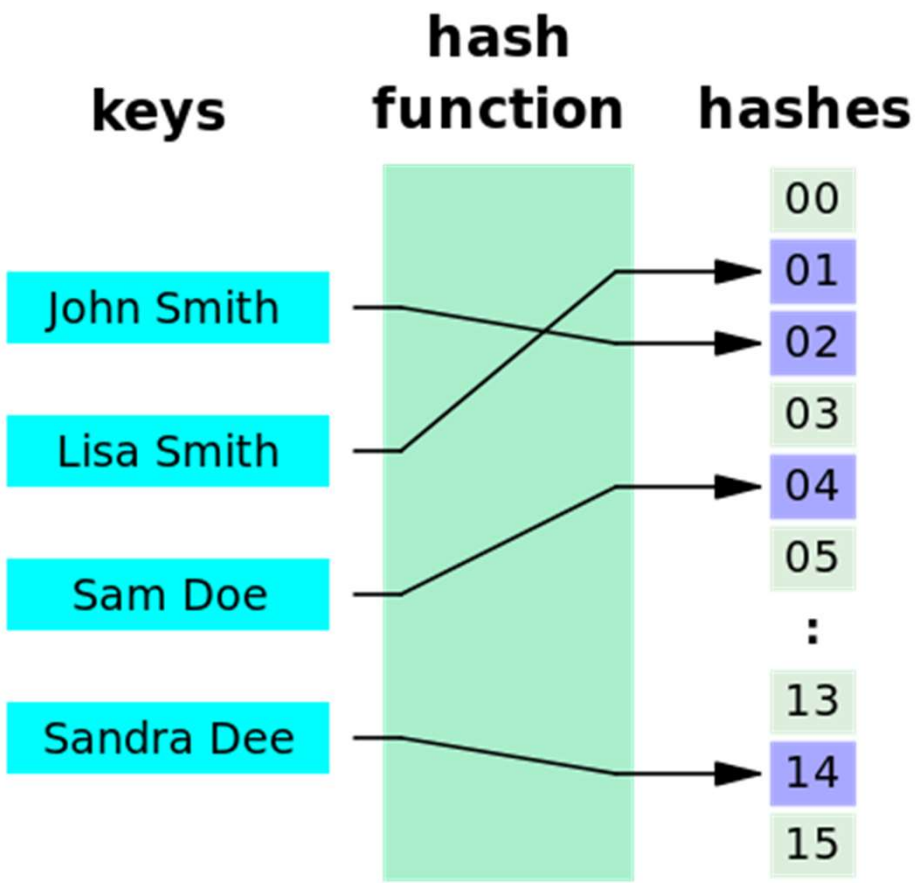
Fog Node Operation



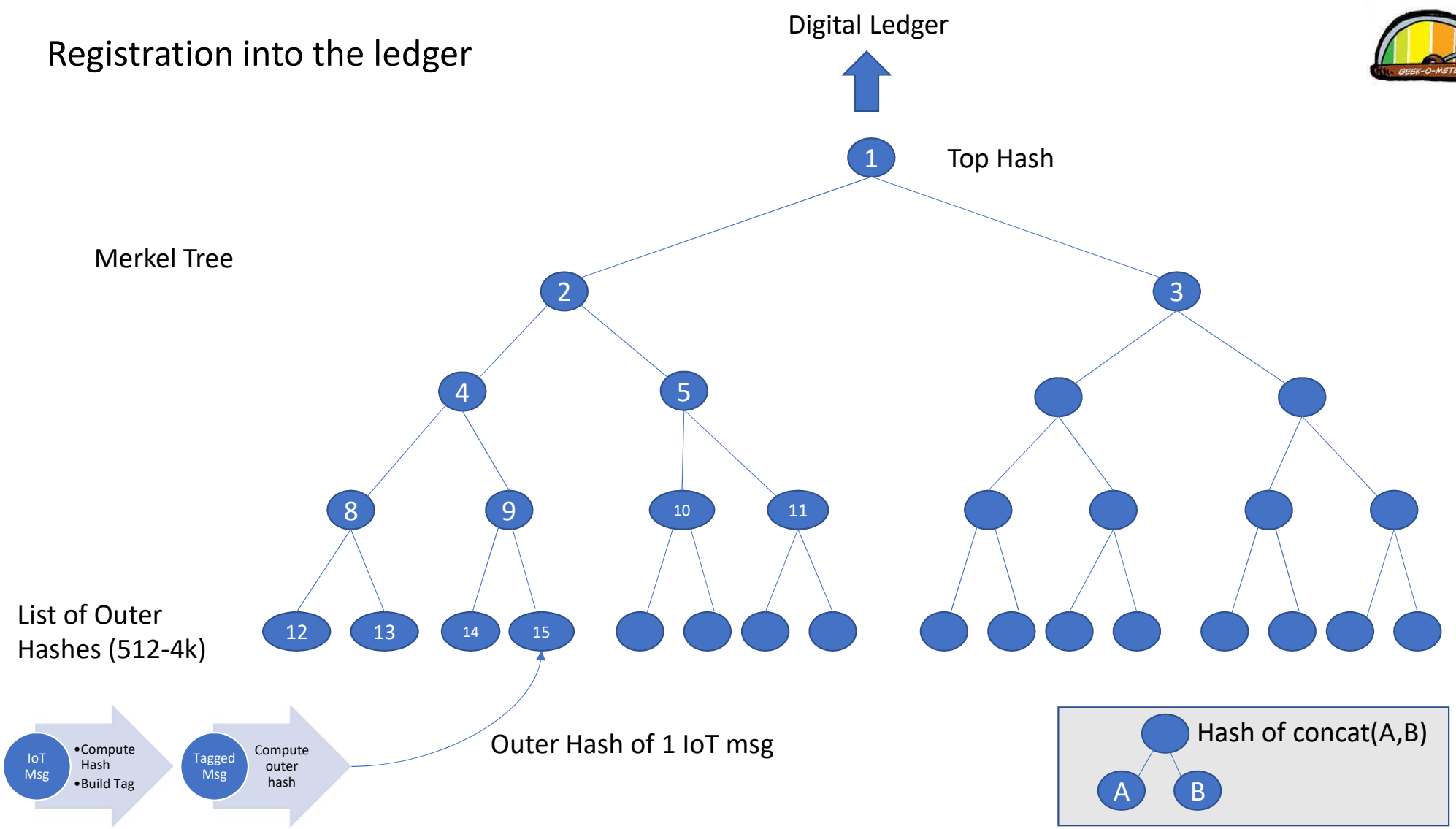


A Few Words about Hash Functions

- Properties of secure hashes
  - Collision free: given H, nobody can find x and y such as H(x)=H(y)
  - Hiding: given H(x) nobody can guess what x was. If x comes from a small set, we can add entropy to it by concat additional bits: H(r|x)

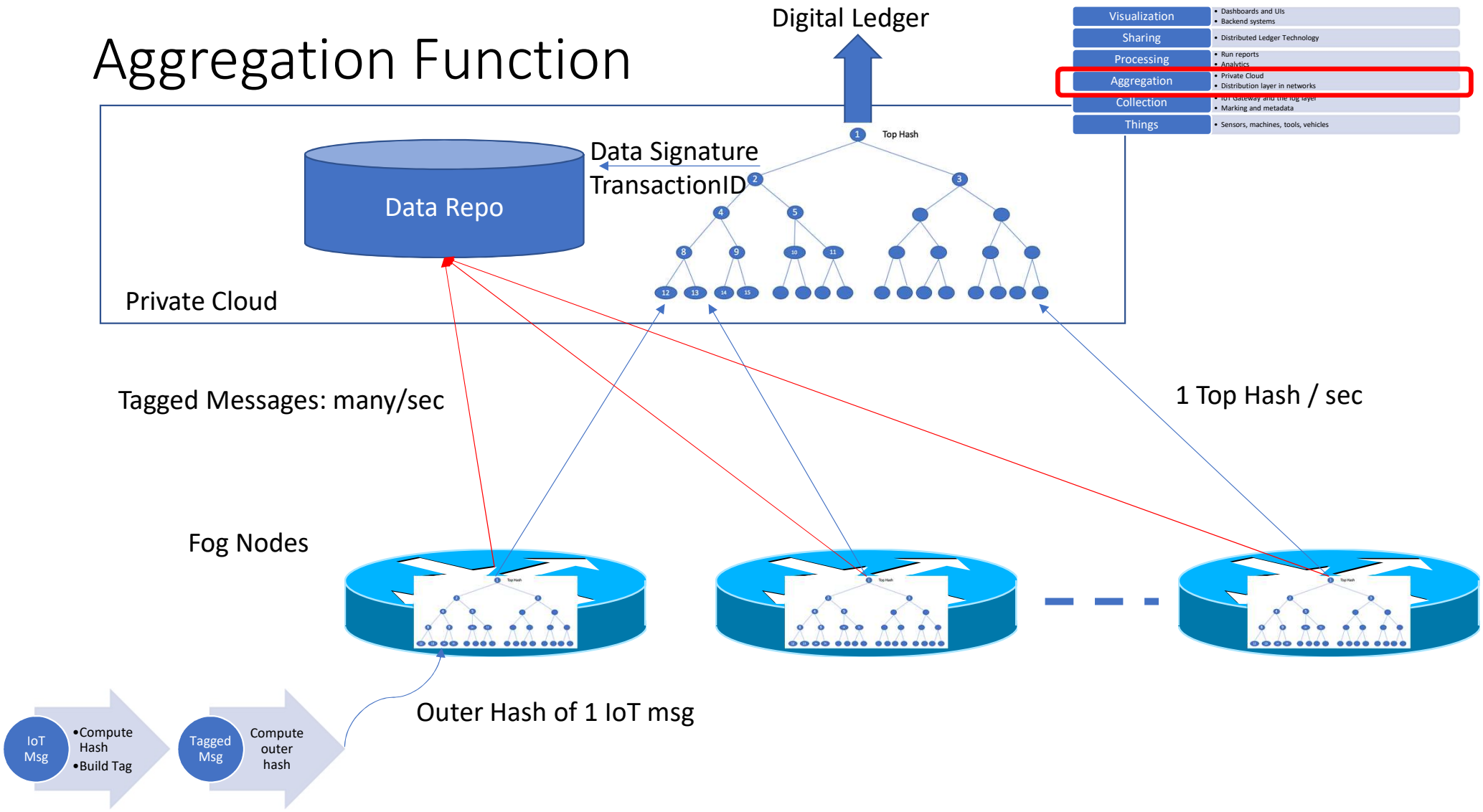


Registration into the ledger



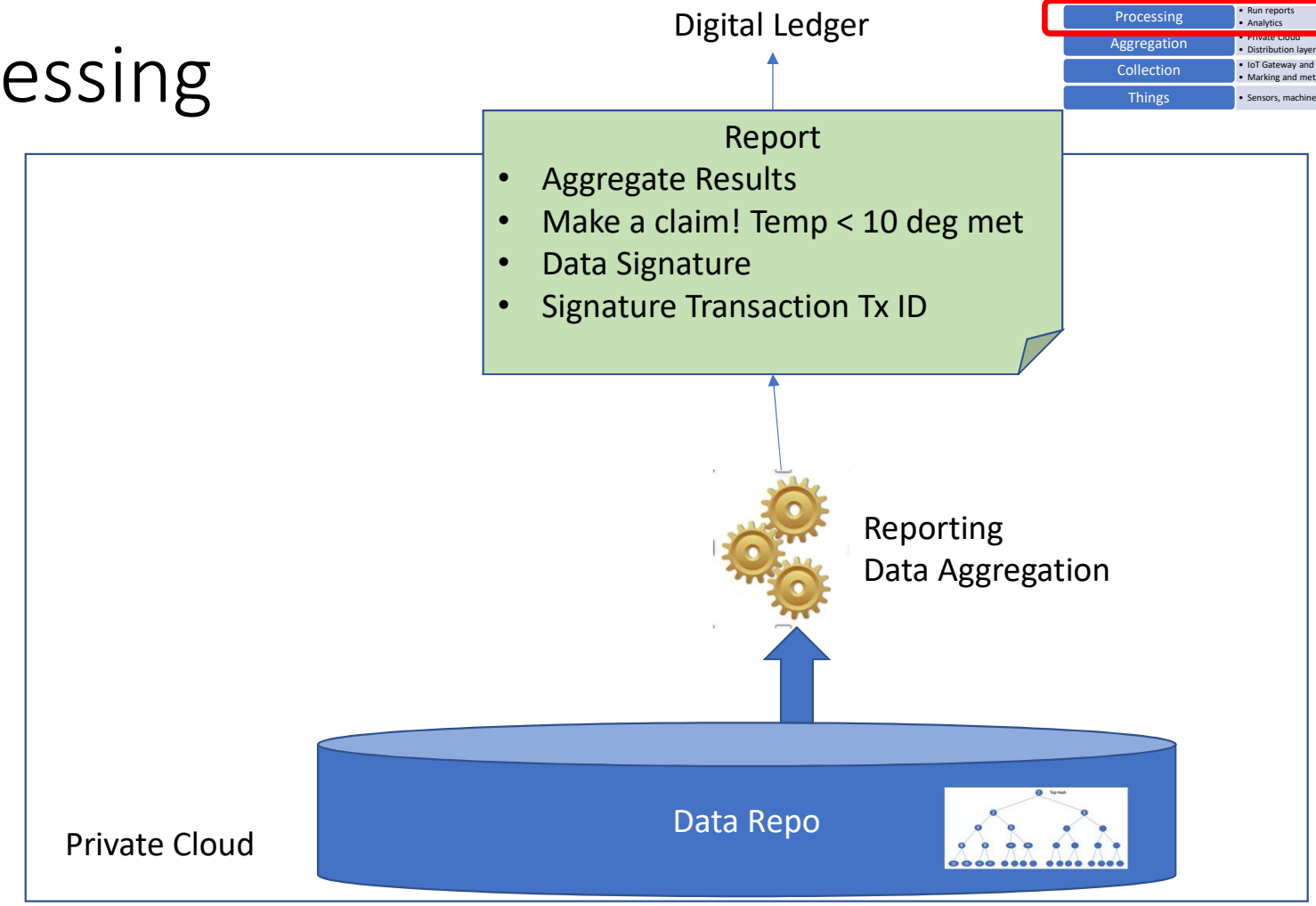
The Data Signature

Aggregation Function



Processing

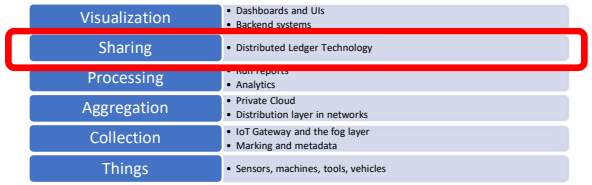

Visualization
• Dashboards and UIs
• Backend systems
Sharing
• Distributed Ledger Technology
Processing
• Run reports
• Analytics
Aggregation
• Private Cloud
• Distribution layer in networks
Collection
• IoT Gateway and the fog layer
• Marking and metadata
Things
• Sensors, machines, tools, vehicles

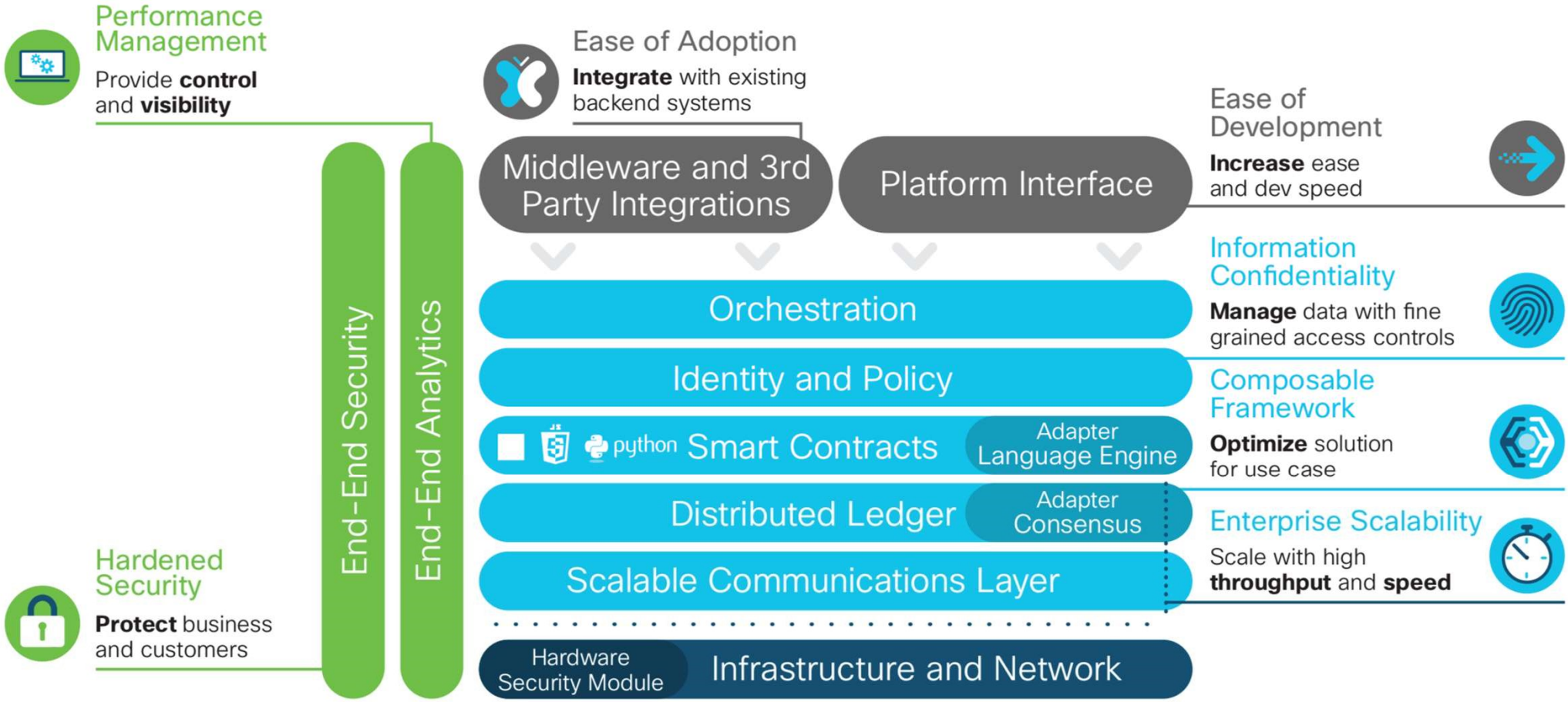

Digital Ledger
Report
• Aggregate Results
• Make a claim! Temp < 10 deg met
• Data Signature
• Signature Transaction Tx ID
Reporting
Data Aggregation
Data Repo
Private Cloud

Block Chain Attributes

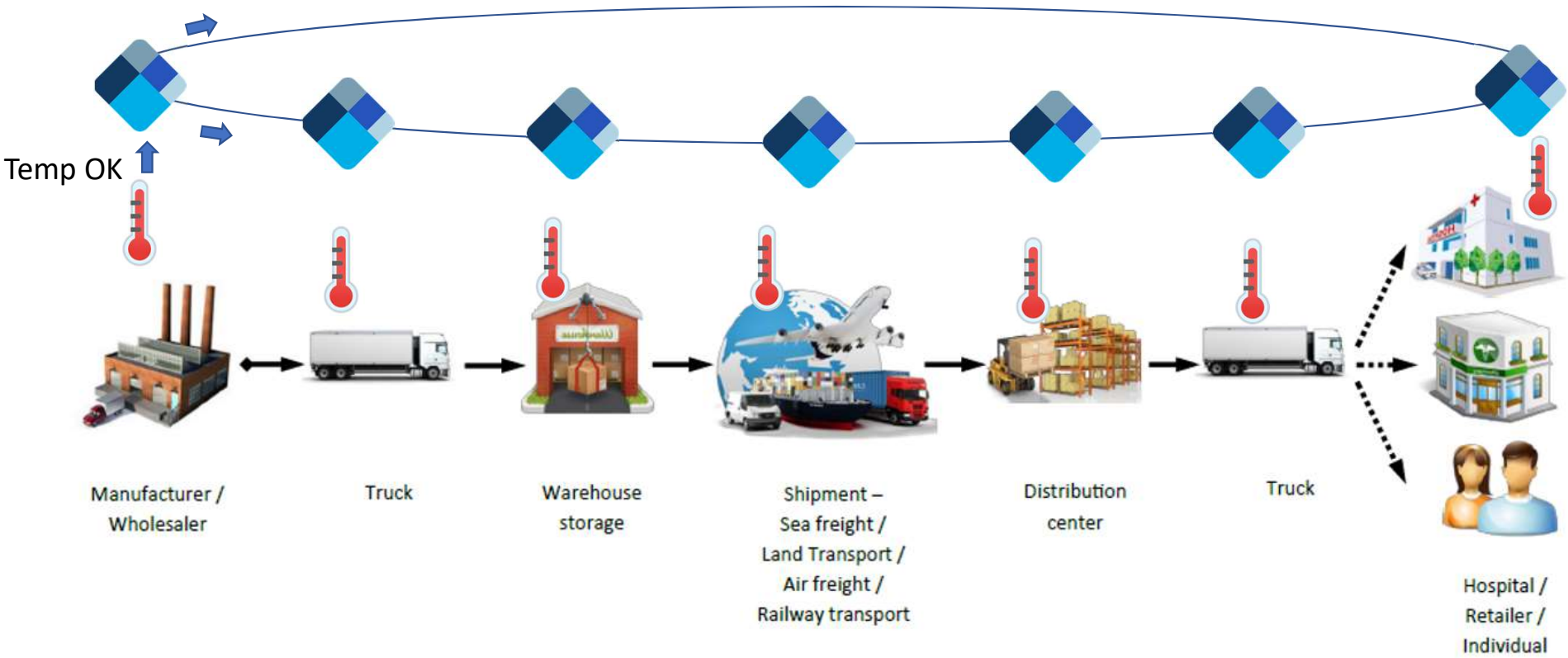
- Decentralized database
- Much harder to attack
- Temper Proof
- Smart contracts to satisfy agreements before the exchange of messages

Digital Ledger





Distributed Ledger



Source ETS Bio Freeze

Recap

The problem we are solving is authenticity

We can do this by signing IoT messages as soon as they are received

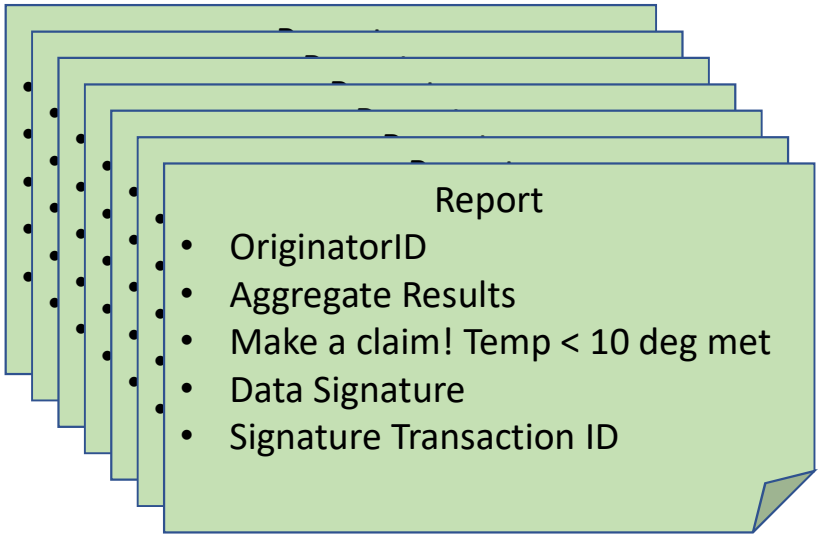
We use the properties of the fog nodes and the ledger

Going Back in Time, Verifying The Records

- Someone broke the cold chain, who is it?

Can We Trust What Is Reported?

- We have the claims
- We have a data signatures
- How can we prove report authenticity?
- Report owner needs to provide the raw data



Verification Process

Verifying the data signature of the report

Report

- OriginatorID
- Aggregate Results
- Make a claim! Temp < 10 deg met
- Data Signature
- Signature Transaction ID

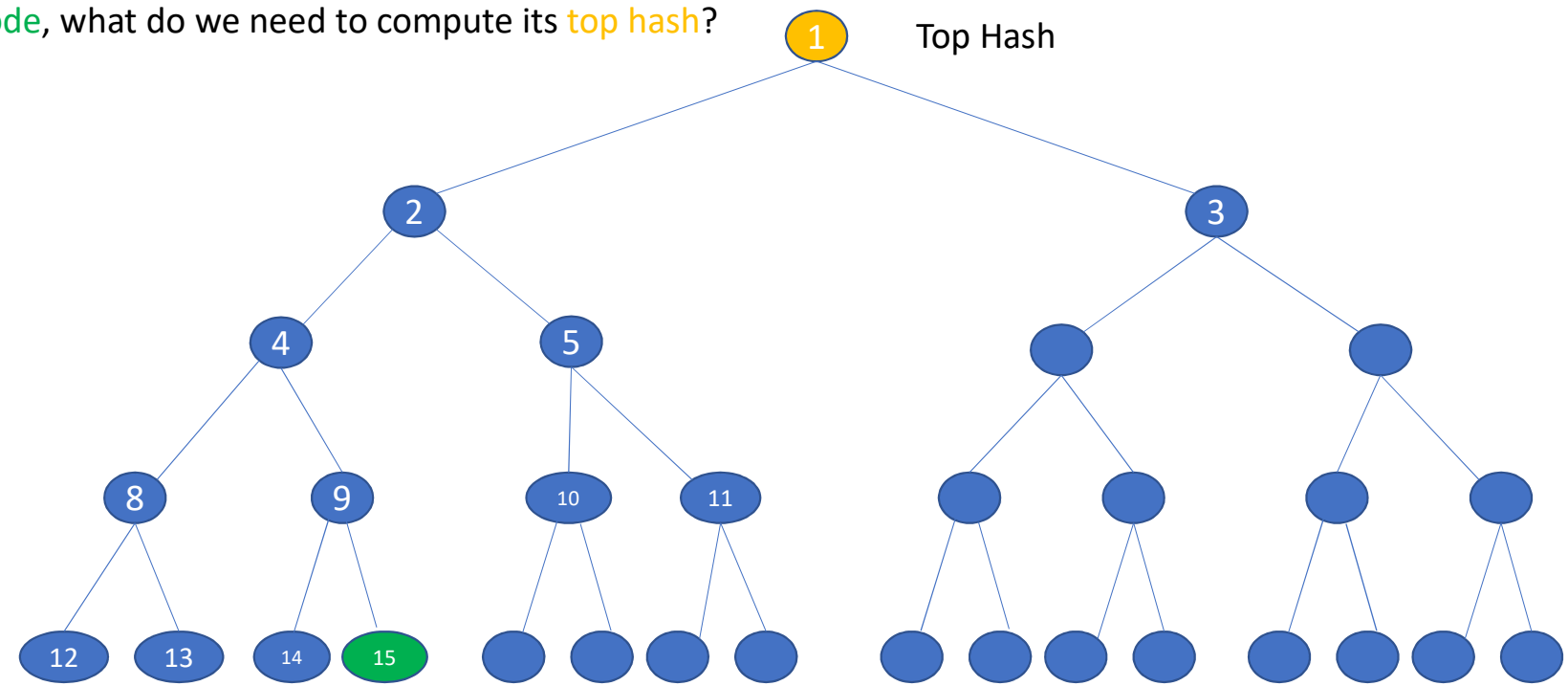
- TransactionID is in the report
- Straight request to the ledger returns the data signature
- Next, data verification

Going to court?

- All parties need to provide some raw data with signatures
- What’s a signature?

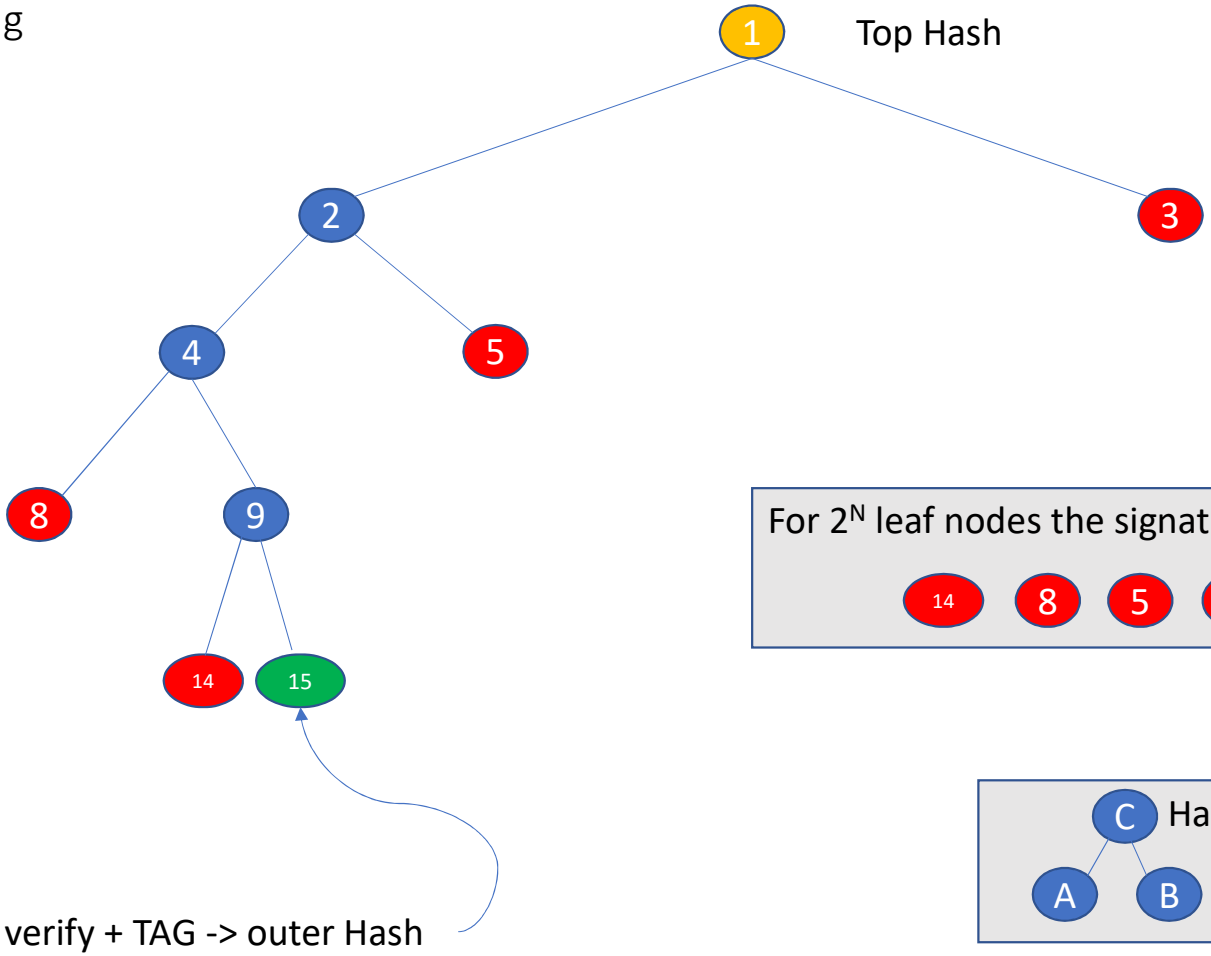
Verification Process

If we have a leaf node, what do we need to compute its top hash?

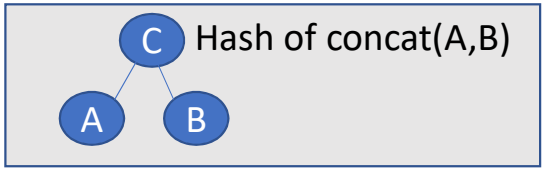


Verification Process

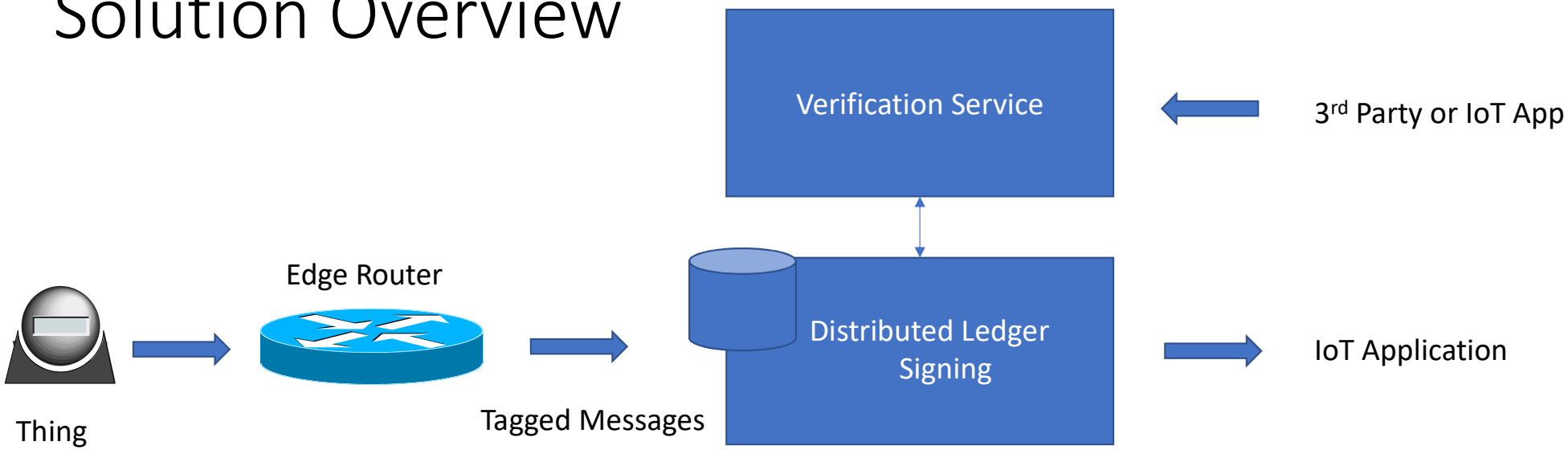
Signature computing



For 2^N leaf nodes the signature size is N-1



Solution Overview




```
routerId: "FTX2114Z05A",
verified: true,
hash: "7fe120e3abc791781658c28edd3e9ab7b60a49e4ce02d0fd417c0c5b6412aa6d",
messageHash: "211493fa32b79f68977b99873a42fc63a1aaa6120ae6293001635516f5f67887",
sequenceNumber: 62,
timestamp: 1551378049303,
message: "{"FridgeTemp":12}",
```

Recap

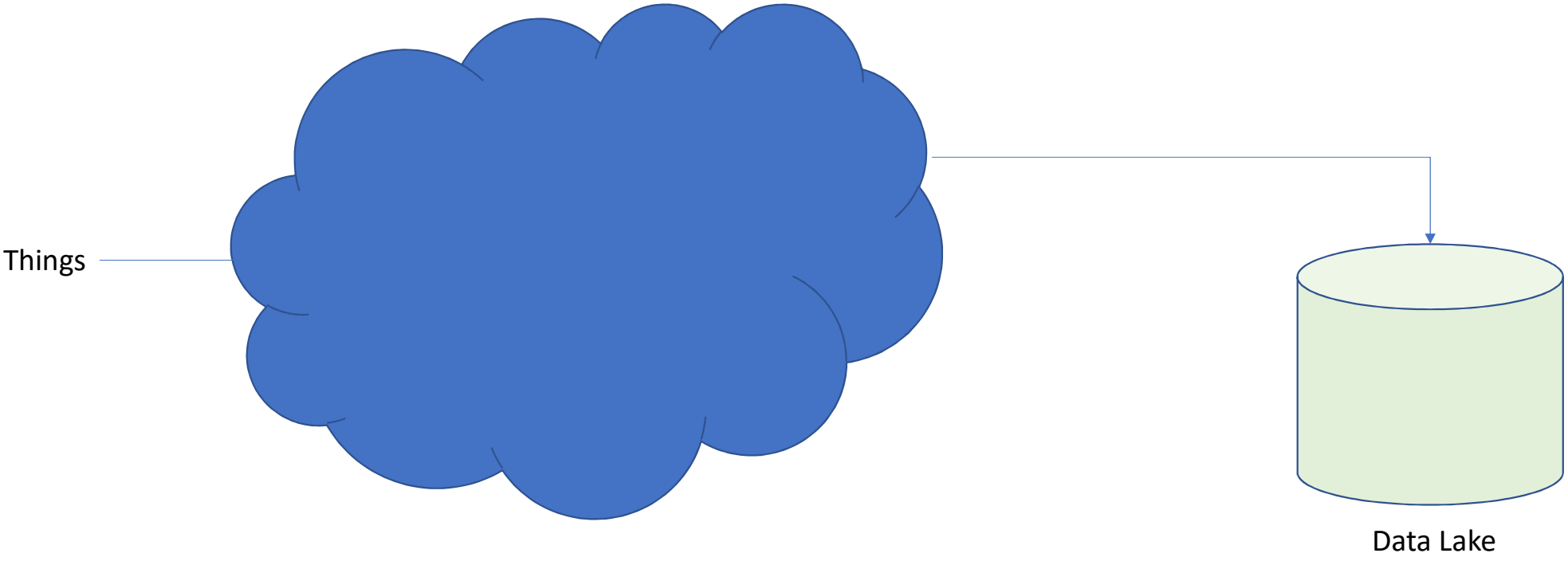
We have defined a verification system

Works either near real-time or long after the message reception

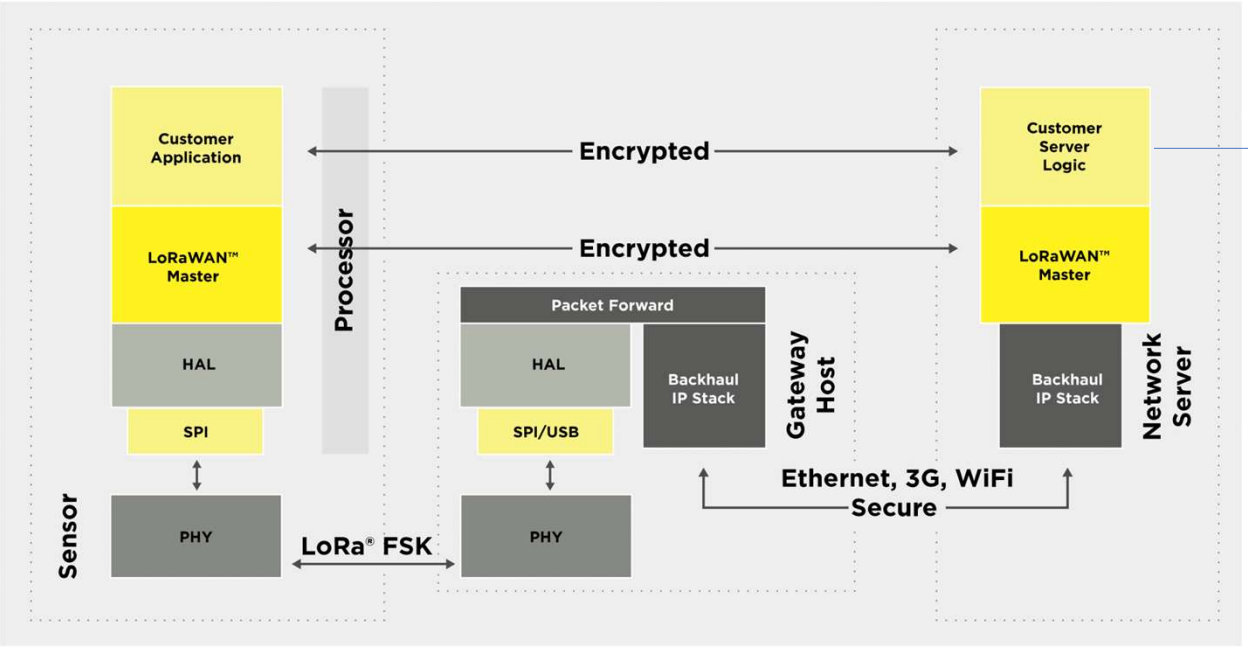
Involves storing messages + metadata + hashes

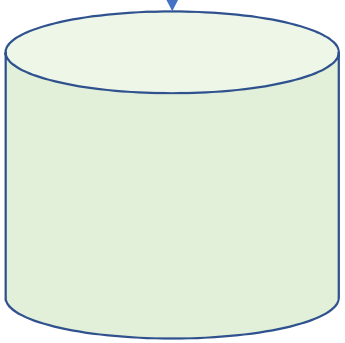
What if there is no Fog at the Edge?

Likely Solutions



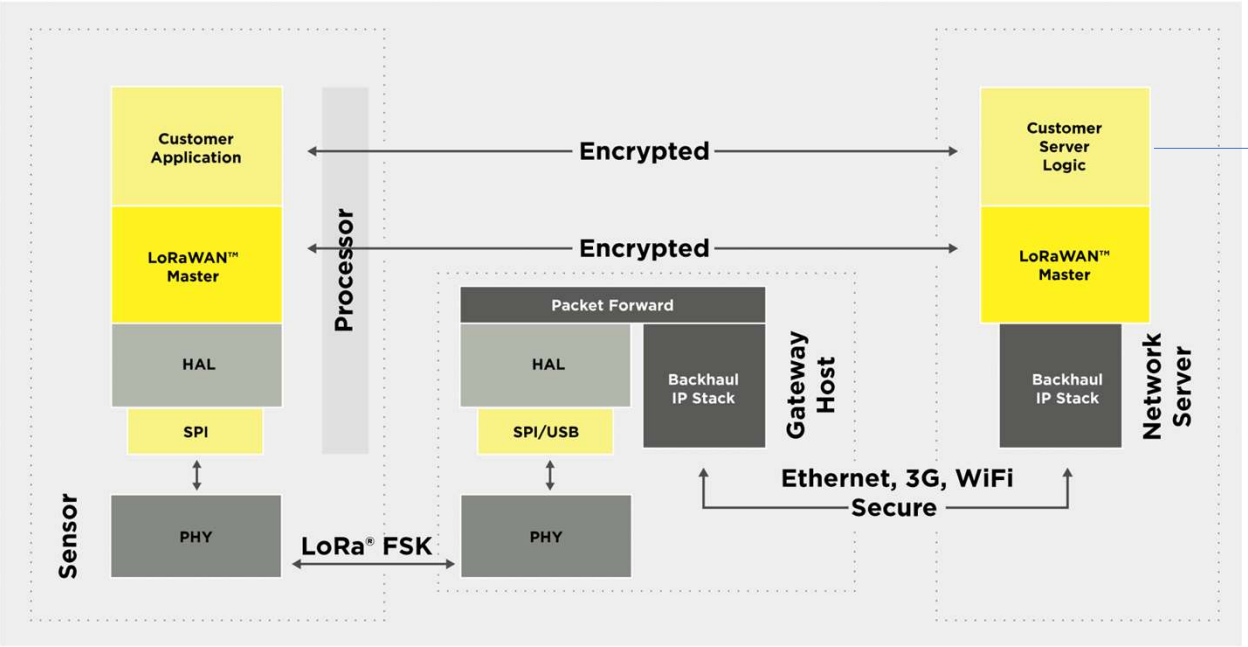
A Possible Use Case

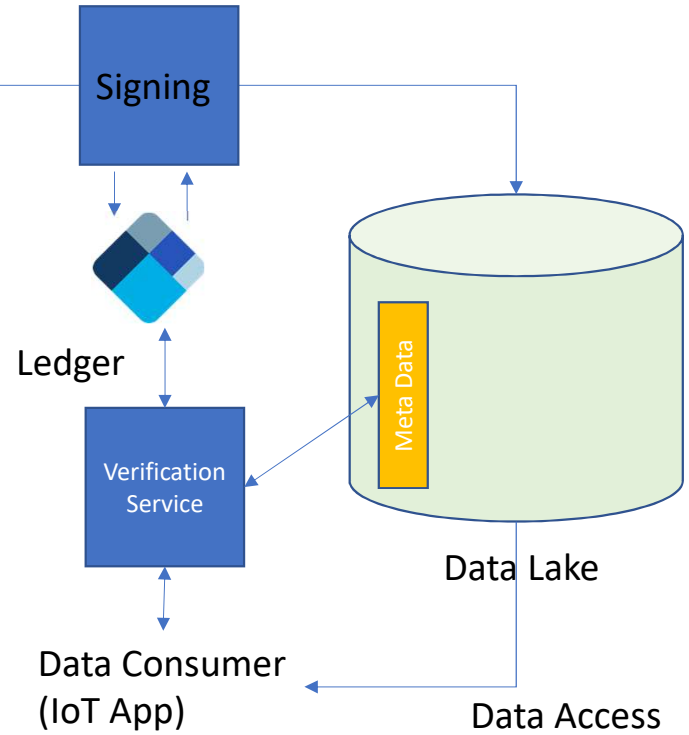


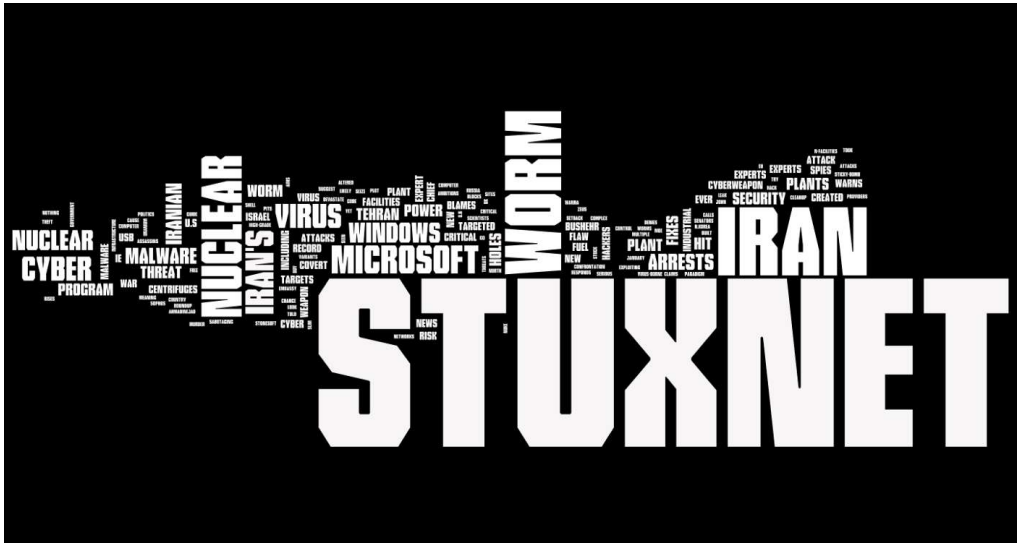


Data Lake

A Possible Use Case
Proof of Immutable Records





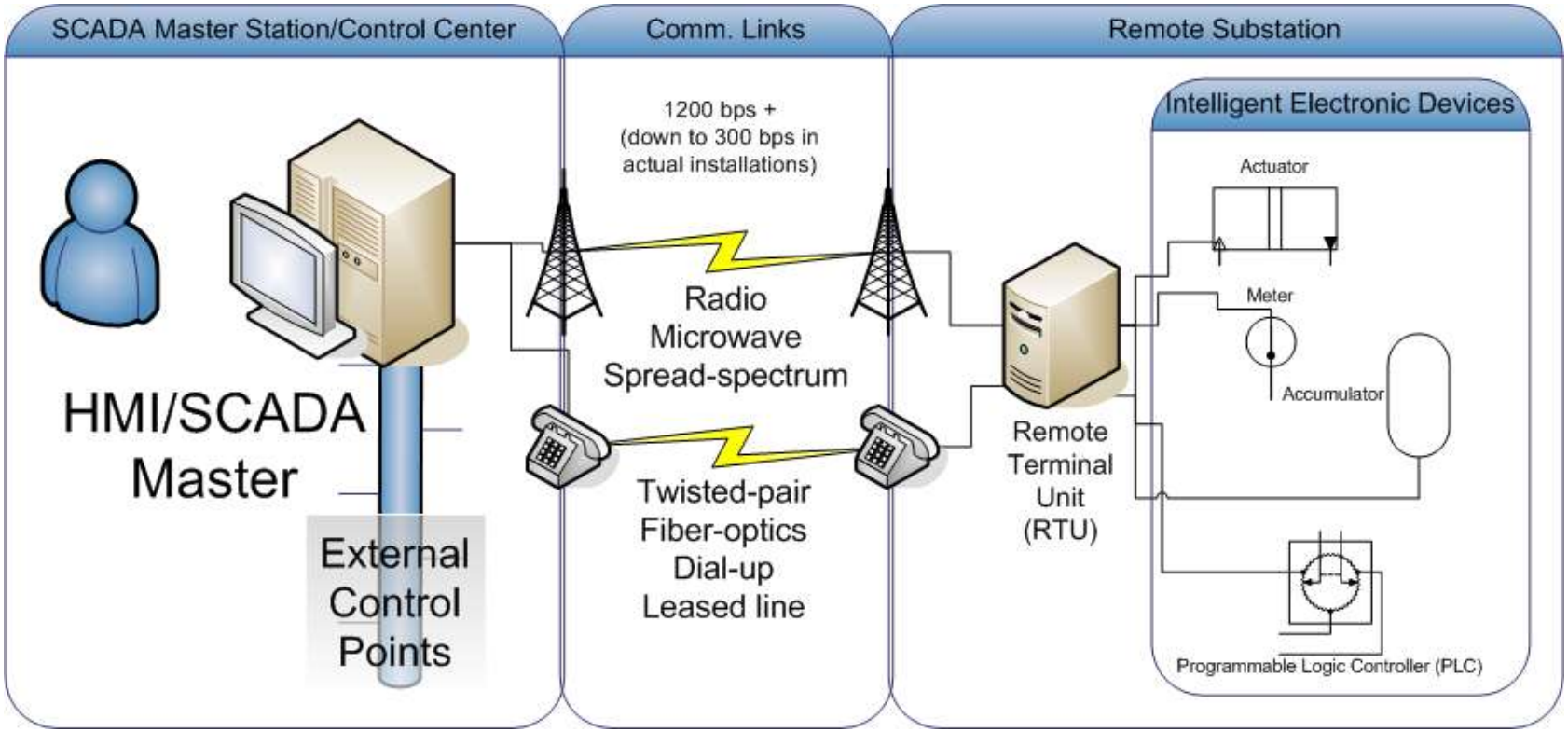

STUXNET
WORM
IRAN
NUCLEAR
IRAN'S
MICROSOFT
WINDOWS
VIRUS
CYBER
NUCLEAR
MALWARE
PROGRAM
THREAT
IRANIAN
WORM
TEHRAN
POWER
SECURITY
PLANTS
ARRESTS
PLANT
HIT
FIXES
CENTRIFUGES
TARGETS
ATTACKS
RECORD
COVERT
NEWS
RISK
CYBERWEAPON
EXPERTS
SPIES
ATTACK
WARNS
CREATED
BUSHEHR
FLAW
FUEL
NEW
INDUSTRIAL
FACILITIES
BLAMES
CRITICAL
TARGETED
EXPERT
CHIEF
ISRAEL
U.S.
USD
WAR
WEAPON
CYBER

StuxNet

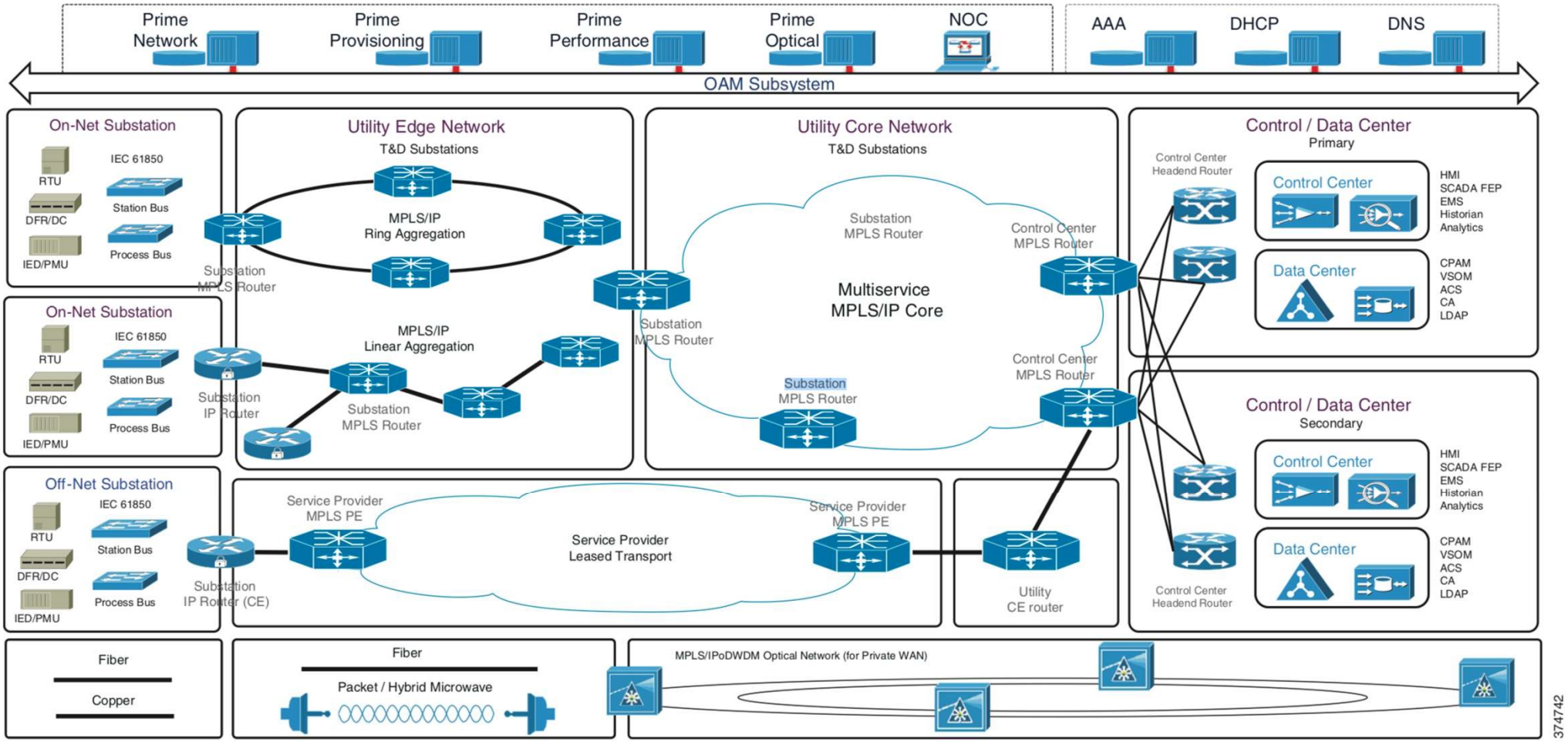
- Stuxnet is a malicious computer worm
- Stuxnet targets SCADA systems
- It is believed to be responsible for causing substantial damage to Iran's nuclear program.

Stuxnet

SCADA

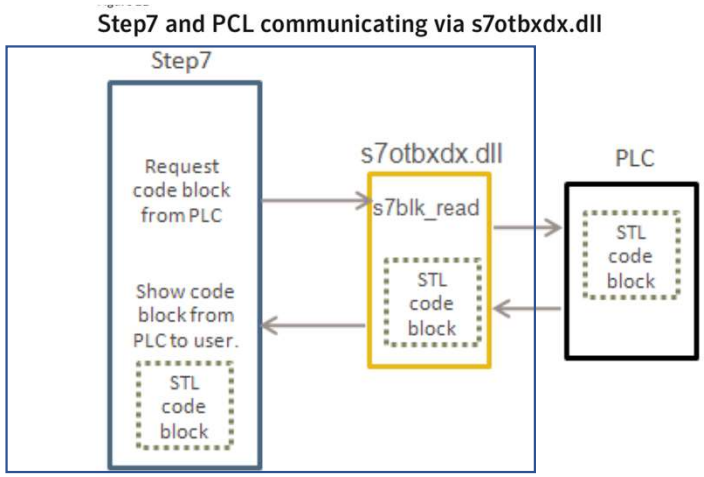

SCADA Master Station/Control Center
Comm. Links
Remote Substation
1200 bps +
(down to 300 bps in
actual installations)
Intelligent Electronic Devices
Actuator
Meter
Accumulator
Radio
Microwave
Spread-spectrum
HMI/SCADA
Master
Remote
Terminal
Unit
(RTU)
Twisted-pair
Fiber-optics
Dial-up
Leased line
External
Control
Points
Programmable Logic Controller (PLC)

Scada Moving to IP…



How StuxNet worked (partially)

- To reprogram the PLC, the Stuxnet worm seeks out and infects STEP 7 project files, which are used by Siemens SIMATIC WinCC, a SCADA and human-machine interface (HMI) system used to program the PLCs.



Windows PC

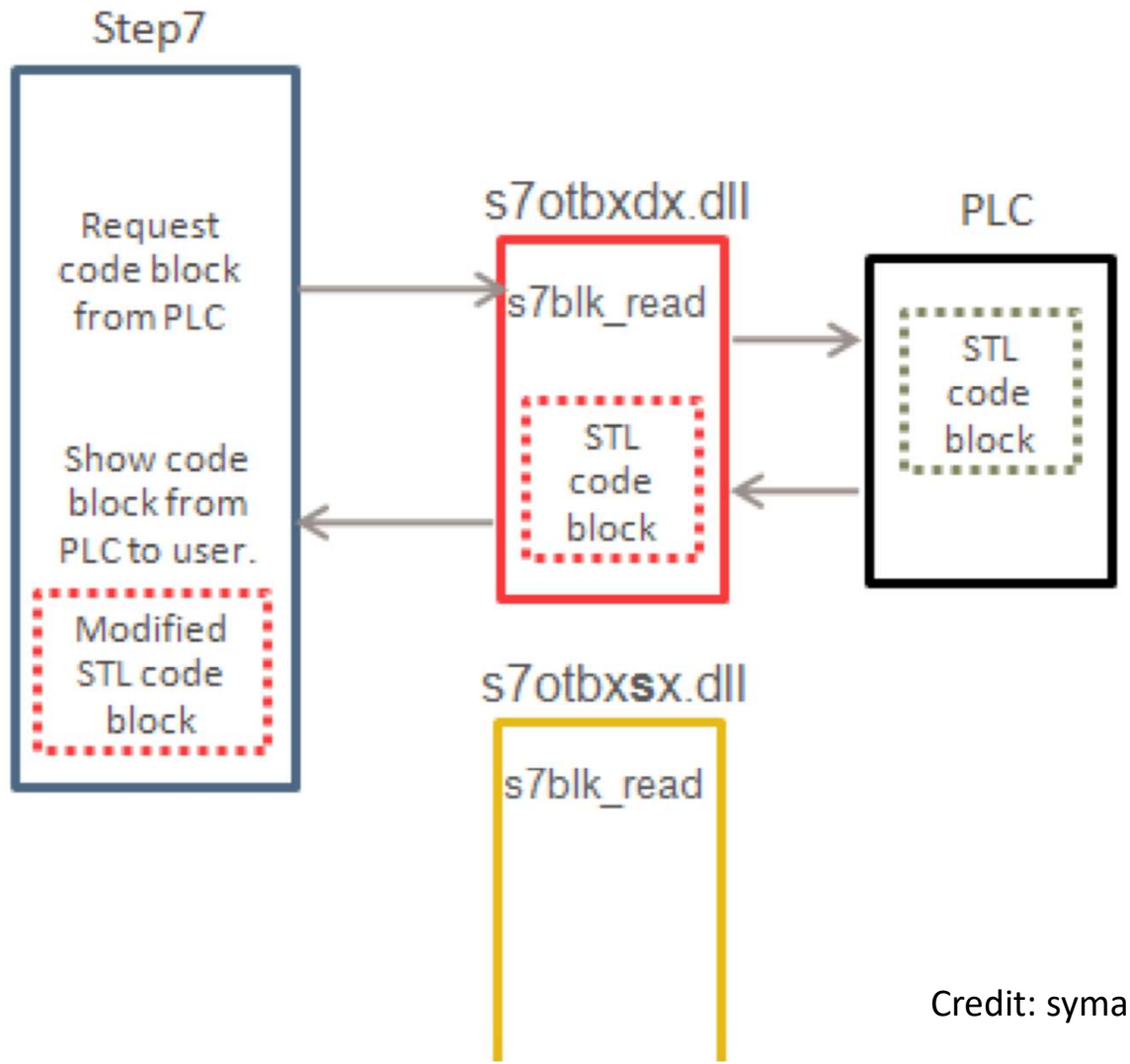
Stuxnet's s7otbxdx.dll file contains all potential exports of the original .dll file – a maximum of 109 – which allows it to handle all the same requests. The majority of these exports are simply forwarded to the real .dll file, now called s7otbxsx.dll, and nothing untoward happens. In fact, 93 of the original 109 exports are dealt with in this manner. The trick, however, lies in the 16 exports that are not simply forwarded but are instead intercepted by the custom .dll file. The intercepted exports are the routines to read, write, and enumerate code blocks on the PLC, among others. By intercepting these requests, Stuxnet is able to modify the data sent to or returned from the PLC without the operator of the PLC realizing it. It is also through these routines that Stuxnet is able to hide the malicious code that is on the PLC.

The following are the most common types of blocks used by a PLC:

- Data Blocks (DB) contain program-spe-

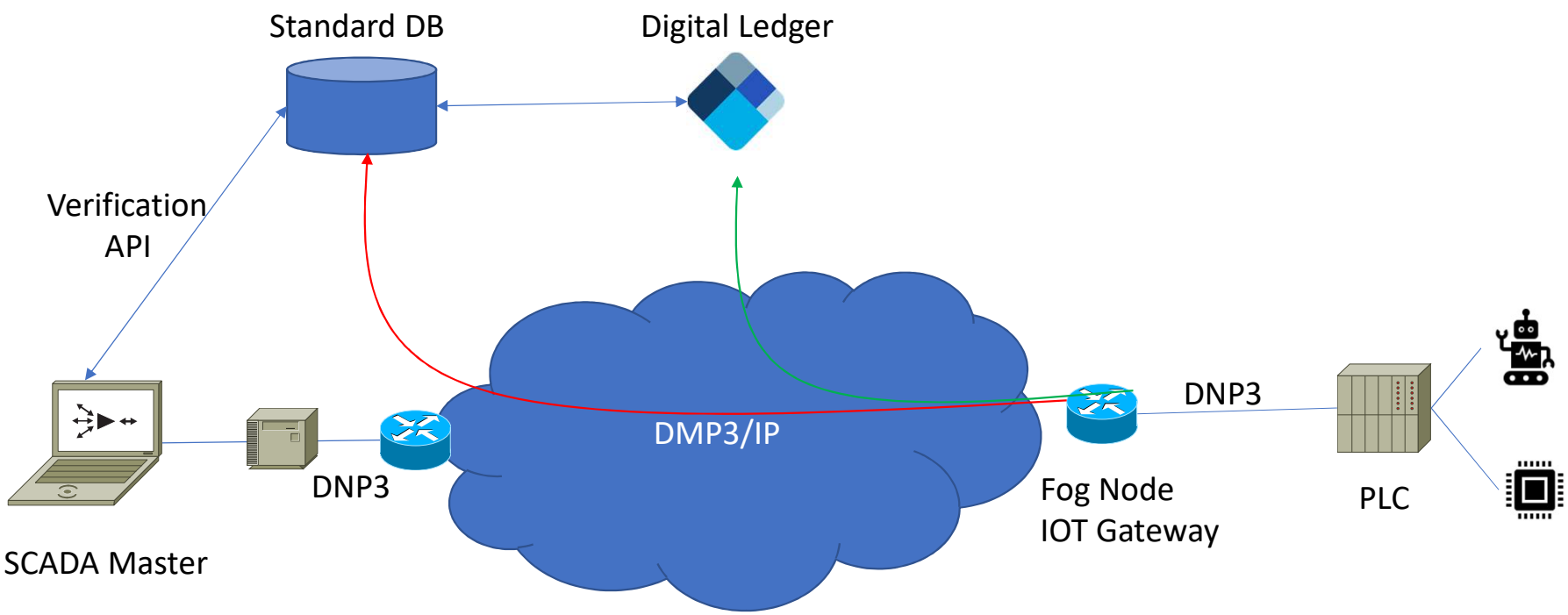
Figure 23

Communication with malicious version of s7otbxdx.dll



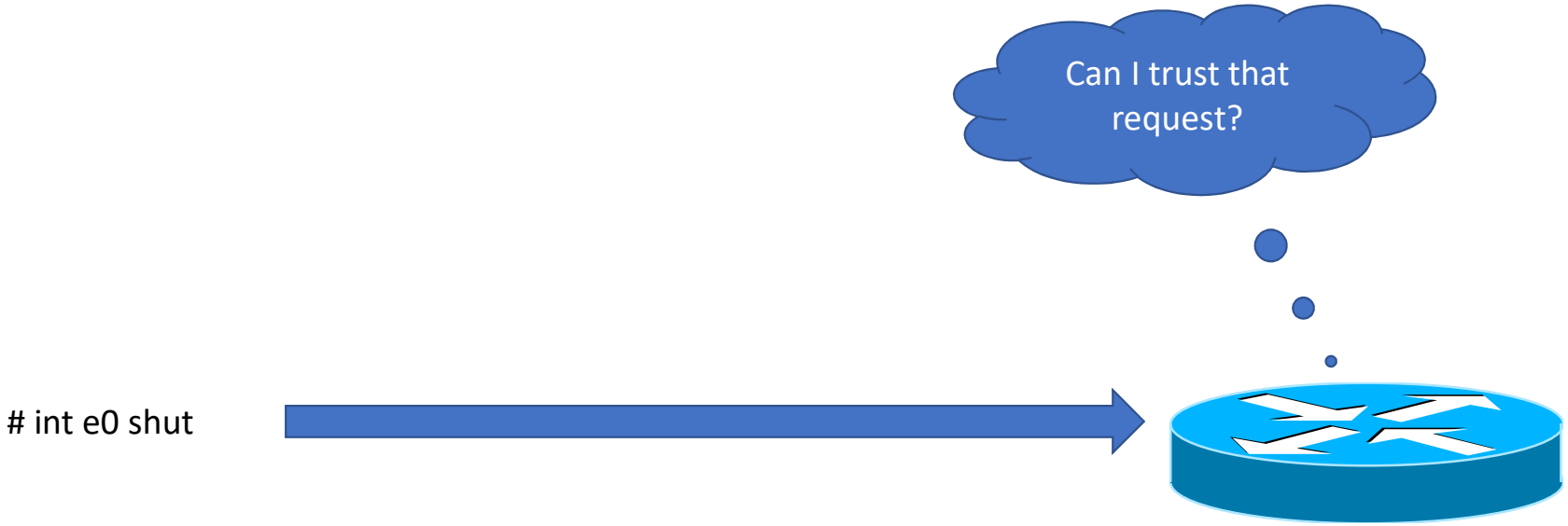
Credit: symantec

Signing the DNP3 Messages

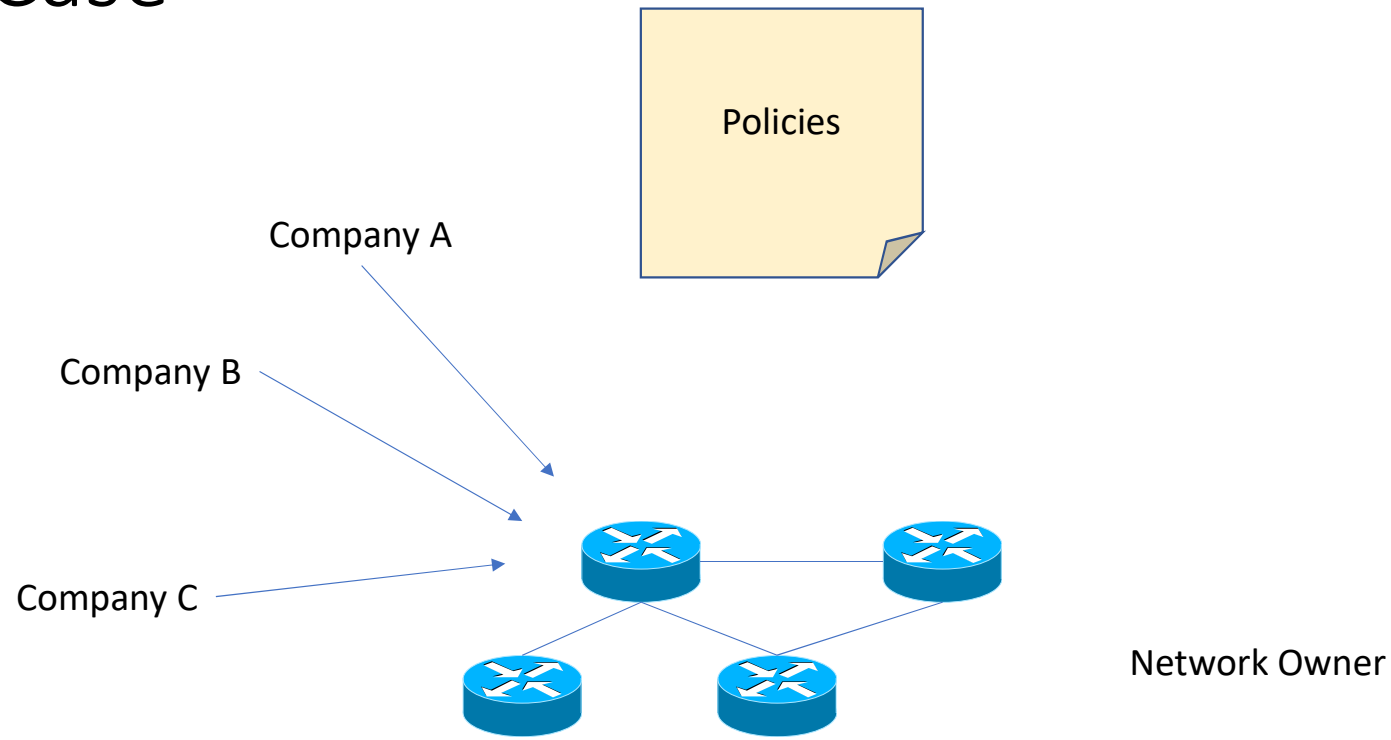


South Bound Use Case

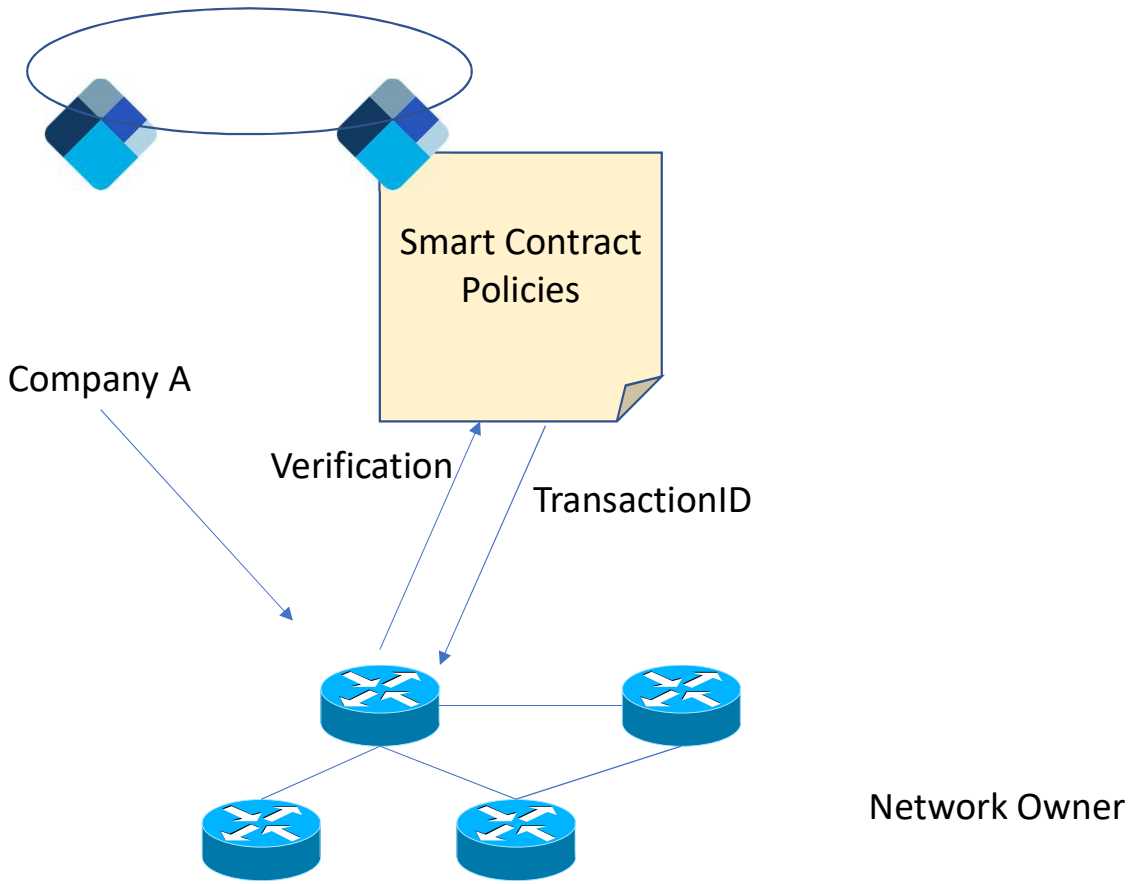
Command Verification


Can I trust that request?
int e0 shut

Use Case



Use Case


Smart Contract
Policies
Company A
Verification
TransactionID
Network Owner

Recap

- IoT and Blockchain are a good fit
- It’s just one layer of trust
- Putting them together needs some thinking
- Integration will become easier as technologies go main stream

Thank You