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
Our Lives Are Regulated by IOT Data

What Makes a Smart City?
Multiple Applications Create Big Data

- **Connected Plane**: 40 TB per day (0.1% transmitted)
- **Connected Factory**: 1 PB per day (0.2% transmitted)
- **Public Safety**: 50 PB per day (~0.1% transmitted)
- **Weather Sensors**: 10 MB per day (5% transmitted)
- **Intelligent Building**: 275 GB per day (1% transmitted)
- **Smart Hospital**: 5 TB per day (0.1% transmitted)
- **Smart Car**: 70 GB per day (0.1% transmitted)
- **Smart Grid**: 5 GB per day (1% transmitted)

A city of one million will generate 200 million gigabytes of data per day by 2020.

Source: Cisco Global Cloud Index, 2015-2020
What Happens To The Data?

- Data
- Collection
- Analysis
- Decision
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?
CONNECTING PRODUCERS AND RETAILERS TO CUSTOMERS AND CONSUMERS

Our customers leverage our temperature-controlled infrastructure and value-adding services to facilitate the movement of goods, while maintaining product and temperature integrity from production through to Integrated Solution.
Integrated Solution
Distributed Solution

Source: ETS Bio Freeze
<table>
<thead>
<tr>
<th>Solution Building Blocks</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Visualization</strong></td>
</tr>
<tr>
<td>Dashboards and UIs</td>
</tr>
<tr>
<td>Backend systems</td>
</tr>
<tr>
<td><strong>Sharing</strong></td>
</tr>
<tr>
<td>Distributed Ledger</td>
</tr>
<tr>
<td>Technology</td>
</tr>
<tr>
<td><strong>Processing</strong></td>
</tr>
<tr>
<td>Run reports</td>
</tr>
<tr>
<td>Analytics</td>
</tr>
<tr>
<td><strong>Aggregation</strong></td>
</tr>
<tr>
<td>Private Cloud</td>
</tr>
<tr>
<td>Distribution layer in</td>
</tr>
<tr>
<td>networks</td>
</tr>
<tr>
<td><strong>Collection</strong></td>
</tr>
<tr>
<td>IoT Gateway and the</td>
</tr>
<tr>
<td>fog layer</td>
</tr>
<tr>
<td>Marking and metadata</td>
</tr>
<tr>
<td><strong>Things</strong></td>
</tr>
<tr>
<td>Sensors, machines,</td>
</tr>
<tr>
<td>tools, vehicles</td>
</tr>
</tbody>
</table>
Things: The Data Producers

• Most time consuming
• Many shapes
• Many protocols
• Need adaptation and System Integration
• Authentication is a challenge
Fog Nodes

- Visualization
- Sharing
- Processing
- Aggregation
- Collection
- Things

- Distributed control
- Backend systems
- Distributed Ledger Technology
- IoT Gateway and the fog layer
- Sensors, machines, tools, websites

Fog Nodes

- Large Volume of Data
- Wide Variety of Things
- High Velocity of Data Generation

Fog Data Services

- Rules, Patterns, Actions
- Data Reduction, Control Response, Data Virtualization/Standardization
- Virtualized Data
- Historic/Predictive Analysis
- Machine Learning

Cloud

- Rule and Pattern Updates
IoT Gateway and Fog Layer

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

Tagged Message  Root Hash (1/sec)

NB Export/Import  DL SDK

HSM  Tagging & Aggregation

Protocol Processing

Things

Sequence Number
RouterID
Message Hash

Visualization
Sharing
Processing
Aggregation
Collection
Things

- Visualization
  - Build/prototype UI
  - Backend systems

- Sharing
  - Distributed Ledger Technology

- Processing
  - Run reports
  - Analytics

- Aggregation
  - Private Cloud
  - Distributed state in networks

- Collection
  - IoT Gateway, and the fog layer
  - Marking and metadata

- Things
  - Sensors, machines, tools, websites

Things
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

Merkel Tree

List of Outer Hashes (512-4k)

Digital Ledger

Top Hash

Outer Hash of 1 IoT msg

Hash of concat(A,B)
The Data Signature

IoT GW 1

IoT GW N

Data Signature

1sec

Time
Aggregation Function

- Dashboards and UIs
- Backend systems
- Visualization
- Distributed Ledger Technology
- Sharing
- Run reports
- IoT Gateway and the fog layer
- Analytics
- Private Cloud
- Distribution layer in networks
- Collection
- Marking and metadata
- Things

Digital Ledger

Data Repo

Transaction ID

Top Hash

Private Cloud

Fog Nodes

Tagged Messages: many/sec

1 Top Hash / sec

Outer Hash of 1 IoT msg

IoT Msg

- Compute Hash
- Build Tag

Tagged Msg

- Compute outer hash

Data Signature
Digital Ledger

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

Data Repo

Private Cloud

Data Aggregation

Reporting
Block Chain Attributes

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

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

Report
- OriginatorID
- Aggregate Results
- Make a claim! Temp < 10 deg met
- Data Signature
- Signature Transaction ID
Verification Process
Verifying the data signature of the report

- 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

Msg to verify + TAG -> outer Hash

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

- Thing
- Tagged Messages
- Distributed Ledger
- Signing
- Edge Router
- Verification Service
- IoT Application
- 3rd Party or IoT App

```
routerId: "FX211405A",
verified: true,
hash: "7fa12061adaf917816580e296d13ebab7ebd0a49e4e02d0f6d17c05c6d412baa6d",
messageHash: "2146936fa32b72f6f89773b99873a42fc33a3aa6120e6293006355016f565f6887",
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

Things

Data Lake
A Possible Use Case
A Possible Use Case
Proof of Immutable Records
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.
SCADA

HMI/SCADA Master

External Control Points

Remote Substation

Remote Terminal Unit (RTU)

Programmable Logic Controller (PLC)

Intelligent Electronic Devices

SCADA Master Station/Control Center

Comm. Links

1200 bps + (down to 300 bps in actual installations)

Radio Microwave Spread-spectrum

Twisted-pair Fiber-optics Dial-up Leased line
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.
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-specific data.
Signing the DNP3 Messages
South Bound Use Case

Command Verification
Can I trust that request?

# int e0 shut
Use Case

Company A

Company B

Company C

Network Owner

Policies
Use Case

Company A

Verification

TransactionID

Smart Contract Policies

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 mainstream
Thank You