Blockchain for Industrial Applications: use cases

Sylvere Krima, Ph.D.
09/17/2018
Agenda

• Introduction
• Blockchain for Industrial Applications COI
• Securing the digital threat for smart manufacturing
• Lessons learned
• Next steps
• Conclusion
Introduction

• Blockchain is often believed to be limited to cryptocurrencies/finance
  • Popularity, visibility, good and bad rep

• Transactions/exchanges of physical and digital assets are omnipresent in a lot/most of industries
  • Manufactured goods
  • Food
  • Medications/pills
  • ...

• Identify and explore these use cases
  • Can they benefit from using a blockchain-based solution?
Introduction

• Two parallel efforts

<table>
<thead>
<tr>
<th>NIST</th>
<th>Blockchain for Industrial Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016</td>
<td>Use case</td>
</tr>
<tr>
<td>2017</td>
<td>Design</td>
</tr>
<tr>
<td>2017</td>
<td>Implementation #1</td>
</tr>
<tr>
<td>2017</td>
<td>Implementation #2</td>
</tr>
<tr>
<td>2018</td>
<td>Implementation #3</td>
</tr>
<tr>
<td>2018</td>
<td>Documentation</td>
</tr>
<tr>
<td>Today</td>
<td></td>
</tr>
</tbody>
</table>
Blockchain for Industrial Applications COI

• Objectives:
  1. Identify and document industrial use cases
  2. Identify, document and tackle threats and challenges

• Open participation

- Government
- Software vendors
- Industry
- Academics
Blockchain for Industrial Applications COI

Phase 1 looked at:

- Smart manufacturing and its digital thread
- Pharmaceutical supply chain
- Secure messaging
- Healthcare data management
- Resilient Vehicle-Infrastructure System
- Food traceability
- Information asymmetry
Securing the digital threat for smart manufacturing

• CIA triad security model

Confidentiality
- Prevent sensitive information from reaching the wrong people.

Integrity
- Maintain the consistency, accuracy, and trustworthiness of data over its life cycle.

Availability
- Ensure that the information concerned is readily accessible to the authorized viewer at all times.
Securing the digital threat for smart manufacturing

- Additive manufacturing
  - Cheaper and often easier
  - Can “easily” be hacked

- Product data is key
  - Has the data been tampered with?

- Corrupted data can be catastrophic
  - Loss of revenue, customers ...
Securing the digital threat for smart manufacturing

- Tampered data lead to faulty parts
  - Structurally weaker parts (failure)
  - Functionally different parts (physical hijack)
    - PCBs at risk in the future

- Cyber attacks often take time to be identified and fixed
  - In 2016, the Mean Time To Identify (MTTI) was 191 days
  - In 2016, the Mean Time To Contain (MTTC) was 66 days

1. "2017 Cost of Data Breach Study: Global Overview" by IBM&Ponemon
Securing the digital threat for smart manufacturing

- The objective is to reduce the digital threat

- Protect data fingerprints in a tampering-free environment

- Trace data transactions between the different actors

- Secure data identity

- Identify corrupted data
Secure data identity

1. Generate unique identifier for each data set/file
2. Generate metadata about the data set/file
3. Record information in the secure registry
Securing the digital threat for smart manufacturing

Identify corrupted data

(1) Generate unique identifier for each data set/file exchanged
(2) Query registry for the identifier
(3) Retrieve source of corruption
Securing the digital threat for smart manufacturing

Why Blockchain?

• A replicated source of information that cannot be tampered
  • Secure: replication guarantees availability of the information
  • Trustworthy: data cannot be modified

• Data insertion is controlled by business rules randomly performed by nodes
  • Lack of single source of authority
  • Customizable to different scenario
Securing the digital threat for smart manufacturing

• A set of information (metadata) is required to enable data traceability and identify corrupted data and source(s) of corruption
Securing the digital threat for smart manufacturing

• Ethereum to implement the blockchain network

• Reuse of our Digital Manufacturing Certificate (DMC) toolkit
  • Generate data fingerprint
  • Digital sign data using software and hardware (PIV/CAC) X.509 certificates

• Development of a client application to record and retrieve data on the blockchain (web3.js)
Securing the digital threat for smart manufacturing

Implementation

1. **Sign file** - DMC
2. **Extract sig.** - DMC
3. **Build MD** - BPD
4. **Notify approval** - BPD
5. **Request approval** - BPD
6. **Submit block** - BPD

- **Content signature (step)**
- **Transaction signature**

**Flowchart Diagram**

- File
- Sign file
- Extract sig.
- Build MD
- Notify approval
- Request approval
- Submit block

**Steps:**
- Sign file
- Extract signature
- Build MD
- Submit block

**Approval Steps:**
- Request approval
- Notify approval

**Signature Steps:**
- Content signature
- Transaction signature

**Approval and Signature Process:**
- Approval
- Signature

**Signatures:**
- File signature
- Content signature
- Transaction signature
- Request signature
- Notify signature

**BPD and DMC:**
- BPD (Business Process Domain)
- DMC (Digital Manufacturing Core)
Lessons learned

Three main challenges to solve:

1. Lack of design patterns
2. Need for cross ledgers integration
3. Ledger evaluation
Lessons learned

1. Design patterns

• Different ways to represent data
  • Size of the information
  • Complexity of the data
  • Privacy policy and legal requirements …

• How to identify the best representation?
  • Smart contracts? Zero knowledge proof? …

• Map business requirements to technical features
Lessons learned

2. Cross ledgers integration

• Heterogeneity of data and transactions in some industries
  • Business data and processes
  • Engineering concepts
  • Financial transaction
  • Logistics ...

• Complexity and globalization of the supply chain
  • Data silos organized by geographical regions

• Vertical and industry-specific blockchains need to be integrated to support full lifecycle traceability
3. Ledger evaluation

• New ledgers/blockchains are flooding the market

• How to pick the right one for your project?
  • This needs to be addressed during the design phase

• Map business requirements to technical features
  • E.g., what design pattern(s) do I need?
Conclusion

• Blockchain is not limited to cryptocurrencies and financial applications

• There are key challenges to solve

• It is not too late to join us
  sylvere.krima@nist.gov