The Ledger of Things: Using a Blockchain Ledger to Track Open Source Components Across the Supply Chain

Mark Gisi
Sameer Ahmed
Projects

SPARTS
Software Parts Ledger

HYPERLEDGER

SPDX

OPENCHAIN
Agenda

- **Problem**: Describe the open source supply chain challenge
- **Solution**: Present an open blockchain ledger solution
- **Q & A**
Part I: The Challenge
License Compliance

Tesla Inches Toward GPL Compliance in Low Gear

Security Vulnerabilities

Jeep Hacked: Taking Over a Moving Car by Remote Control

Safety Certification

Tesla Model X in Autopilot - Driver Killed in Crash
License Compliance

Security Vulnerabilities

Safety Certification

Artifacts

- List of Open Source
- Required Source Code
- Required Notices
- SPDX data

Artifacts

- List of Open Source
- CVEs

Artifacts

- List of Open Source
- Certification Evidence
[Compliance Program]
Chain of Custody

**chain of custody** - the unbroken path a product takes from the **first stage** in the supply chain to the **end customer** including - raw materials, their conversion, production and along distribution lines.
Chain of Custody
Chain of Custody
The Challenge
The Challenge

Mfg/Distributors

End Users

i) **Accountability** - How can we trust each supplier has prepared the correct artifacts?

ii) **Access** - How can we facilitate the collection and delivery of all artifacts?
Part II: Solution
Ledger Attributes

Things
Transactions
Time
Truth

= Trust
Things
Transactions
Time
Truth
≡ Trust
Then

Time

Things

Transactions

Time

Truth

= Trust
<table>
<thead>
<tr>
<th>Part/Env ID</th>
<th>Supplier</th>
<th>Action</th>
<th>Artifacts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Env-Drv-23</td>
<td>Intel-ID</td>
<td>create</td>
<td>CODE</td>
</tr>
<tr>
<td>Env-Lx-52</td>
<td>WR-ID</td>
<td>create</td>
<td>CODE</td>
</tr>
<tr>
<td>Env-VCam-5217</td>
<td>AvTec-ID</td>
<td>create</td>
<td>CODE, SPDX</td>
</tr>
<tr>
<td>Env-Drv-23</td>
<td>WR-ID</td>
<td>add</td>
<td>CODE</td>
</tr>
<tr>
<td>Env-VCam-5217</td>
<td>AvTec-ID</td>
<td>update</td>
<td>CODE</td>
</tr>
</tbody>
</table>
Summary

- SParts – Free and Open Ledger - track open source components and their meta data of IoT devices
- Code is available under the Apache-2.0
  https://github.com/hyperledger-labs/SParts
- Enabling across Supply Chain Open Source management
  - License compliance – which artifacts are OpenChain conforming
  - Security vulnerabilities
  - Safety certification
- Useful internally tracking open source artifacts across business units
- **Accountability**: establish trust among supply chain participants
- **Access**: query for current set of compliance artifacts
Video Camera Model 5217
Video Camera Model 5217
Contact

Mark.Gisi@WindRiver.com