Utilizing the Blockchain to Manage Open Source Across the Supply Chain

Mark Gisi
Director of IP & Open Source
Delivers embedded operating system platforms to 1000s of companies
  - Linux, Android, VxWorks
  - 10,000s of open source components in over a billion devices served

Biggest competitor: roll your own Linux

Extra pressure to get compliance right
  - Must mitigate risk for customers too
  - OpenChain Conforming

Independent wholly owned by Intel
Wind River Delivers SPDX Data to Customers

- **2012** - Wind River Linux 5
- **2013** - Wind River Linux 6
- **2014** - Wind River Linux 7
- **2015** - Wind River Linux 8
- **2016** - Wind River Linux 9
- **2015** – Titanium/OpenStack
- **2016** – Pulsar Linux
- **2016** – Helix Auto
- **2016** – Android
- **2017** – VxWorks 7
Agenda

- Describe the supply chain challenge
- Discuss how the Hyperledger Blockchain platform is critical to the solution
- Discuss how SPDX, OpenChain, Hyperledger are highly complementary
- Summary
- Q & A
The Challenge
IoT/Embedded Device Requirement

- Most modern day devices are constructed from 80%+ open source
- Device Runtime is governed > 100 licenses
- Every shipping device requires open source compliance artifacts:
  1. Source Code
  2. Legal Notices
  3. SPDX data
  4. Open Source Bill of Materials
  5. Security Vulnerability Report
  6. Cryptography info
[Compliance Program]

Software Part

SPDX Notices Source
IoT/Embedded Device Requirement
The Supply Chain Challenge

*Other names and brands may be claimed as the property of others.*
Solution
**Shared Ledger**

<table>
<thead>
<tr>
<th>Envelope 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, BoM</td>
</tr>
<tr>
<td>Env-Drv-23</td>
<td>WR-ID</td>
<td>add</td>
<td>SPDX</td>
</tr>
<tr>
<td>Env-VCam-5217</td>
<td>AvTec-ID</td>
<td>update</td>
<td>CODE</td>
</tr>
</tbody>
</table>
The Technology
Sawtooth Blockchain

- A digital ledger that maintains a historical record of executed transactions
- Like a database it can record information of various types (e.g., artifacts: 📝)
- Unlike databases it uses cryptography to ensure each record is immutable 🗝️
- Data is replicated across a network of servers (ledger nodes) 🌐
- Which eliminates the need for central authority or middleman
- Achieving secure record preservation and data integrity 🗠️
  ... thereby establishing accountability & trust among all supply chain participants
## Software Parts Ledger

<table>
<thead>
<tr>
<th>Entry</th>
<th>Description</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>112</td>
<td>UPDATE source-881 WITH source-919 IN envelope-222</td>
<td>Nov 8</td>
</tr>
<tr>
<td>111</td>
<td>ADD_ARTIFACT notices-824 TO envelope-13</td>
<td>Nov 5</td>
</tr>
<tr>
<td>110</td>
<td>ADD_ARTIFACT oss-bom-97 TO envelope-222</td>
<td>Nov 1</td>
</tr>
<tr>
<td>109</td>
<td>ADD_ARTIFACT notices-511 TO envelope-222</td>
<td>Nov 1</td>
</tr>
<tr>
<td>108</td>
<td>ADD_ARTIFACT source-88 TO envelope-222</td>
<td>Nov 1</td>
</tr>
<tr>
<td>107</td>
<td>ADD_ARTIFACT envelope-13 TO envelope-222</td>
<td>Nov 1</td>
</tr>
<tr>
<td>106</td>
<td>CREATE_ENVELOPE e-222 FOR part-101</td>
<td>Oct 30</td>
</tr>
<tr>
<td>105</td>
<td>CREATE_PART part-101 FOR supplier-S2</td>
<td>Oct 30</td>
</tr>
<tr>
<td>104</td>
<td>ADD_ARTIFACT oss-bom-413 TO envelope-13</td>
<td>Oct 14</td>
</tr>
<tr>
<td>103</td>
<td>ADD_ARTIFACT source-413 TO envelope-13</td>
<td>Oct 14</td>
</tr>
<tr>
<td>102</td>
<td>CREATE_ENVELOPE e-13 FOR part-37</td>
<td>Oct 12</td>
</tr>
<tr>
<td>101</td>
<td>CREATE_PART part-37 FOR supplier-S1</td>
<td>Oct 11</td>
</tr>
</tbody>
</table>
Video Camera Model 5217
Catalog of Software Parts

The building blocks of the future
Additional Considerations

- Supplier can keep artifact data private and share selectively
- Suppliers are not required to have mature compliance program to participate
- No fix requirements around artifact types or formats (notices, BoMs, ...)
- We anticipate many semi-private and public supply chains
  – Automotive, Aerospace, Medical Devices, Consumer verticals, ...
  – Single OEM/ODM can create a network with its suppliers
  – Linux Foundation could create a public ledger for it’s projects
  – Large companies could use internally to coordinate among multiple business units
- The ledger can manage more than license compliance information (BoM, crypto, vulnerabilities, certifications, ...
Current Status & How to Participate

- The SParts project provides a software ledger built on the Sawtooth platform. Source code is available:
  
  https://github.com/Wind-River/sparts

- Live demos exists, will make public in 2018 Q1

- Looking for a neutral home for the SParts project

- Production 1.0 available in 2018 Q2 (finalizing access credential management)
  - Will support: source code, notices, SPDX data, OpenChain Status

- Participation
  - Host a ledger node (easy - download and run container)
  - Contribute to requirements & roadmap – especially ODMs/OEMs and their suppliers
  - Contributors: Developers, Documentation, website design, ...
Summary

- Implementing and deploying a compliance program can be challenging.
- Coordinating among suppliers adds another level of complexity.
- The combination of SPDX, OpenChain and Hyperledger initiatives can greatly facilitate the task.

- The Sawtooth Blockchain platform in particular:
  1. Enables a supply chain to construct a shared Software Parts ledger.
  2. Where immutable and replicated records are securely preserved.
  3. Without the need for a central authority or middleman.

- To deliver the accountability required to establish trust among all the supply chain participants.
Contact

https://github.com/Wind-River/sparts

Mark.Gisi@WindRiver.com