WIND

Blockchain Ledger in the Wild: Track and Manage Open Source Across the Supply Chain

Mark Gisi, Director, IP & Open Source

Sameer Ahmed, Sr. Member of Technical Staff

WHEN IT MATTERS,
IT RUNS ON WIND RIVER.

Abstract

A software solution, whether it is an application, library, container or a Linux runtime – is comprised of some percentage of open source software. Tracking which components were used and by whom across the software supply chain has multiple benefits. We discuss the benefits and how a Blockchain ledger is used to solve the open source tracking problem. We will present a public Blockchain ledger used to track and manage open source compliance artifacts (source, notices, bill of materials, SPDX data) for various hardware runtime builds of the Zephyr operating system.

GE Smart Street Light

- Linux
- User space applications
- Vision Sensor Drivers
- Audio Sensor Drivers
- Networking

Agenda

- Describe the open source supply chain challenge
- Discuss why a blockchain ledger provides a good solution
- Present Zephyr Operating system case study
- Summary
- Q & A

Part I: The Challenge

Three Concepts

- Software Parts (tracked on ledger)
- Envelope of Software Artifacts
- Chain of Custody

WIND

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

Artifacts

- Source Code
- Notices
- Open Source BOM
- SPDX data

OPENCHAIN CONFORMANCE 1.1

Security Vulnerabilities

Artifacts

- Open Source BOM
- Vulnerability List

Information Security Management System ISO 27001 Certified

CORE INFRASTRUCTURE INITIATIVE BEST PRACTICES

Safety Certification

Artifacts

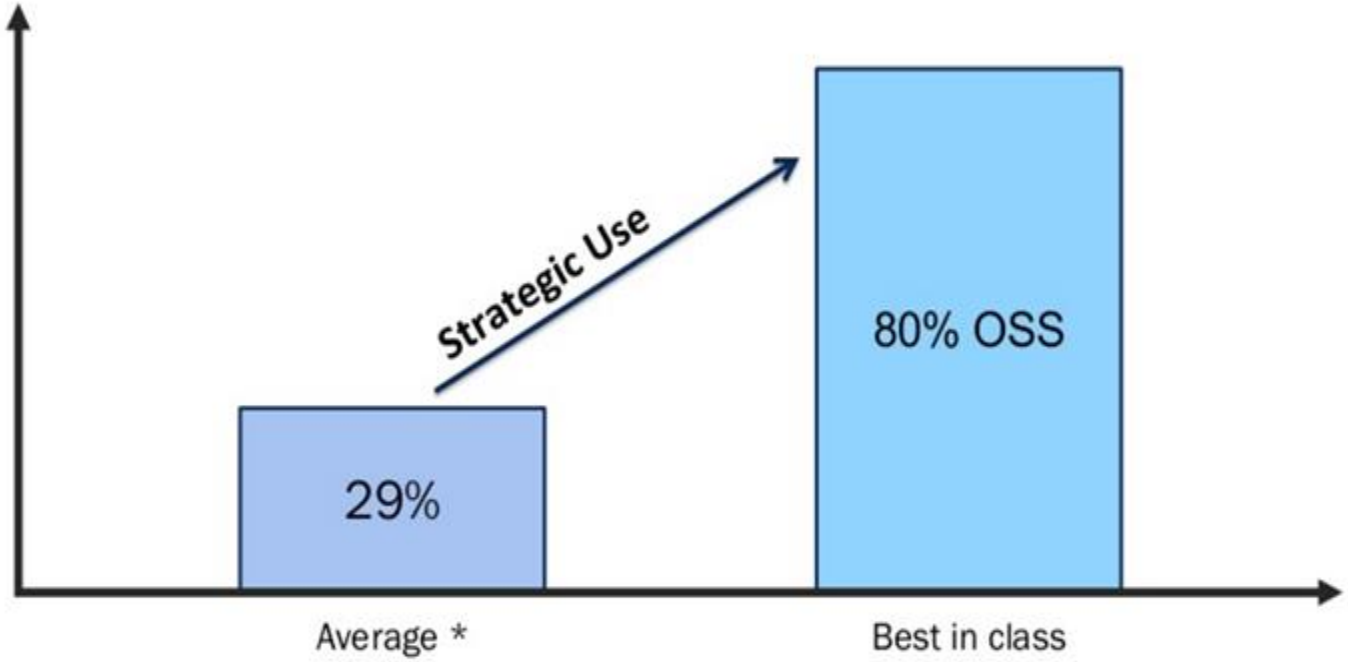
- Open Source BOM
- Certification data

ISO 26262

DO-178 Qualification

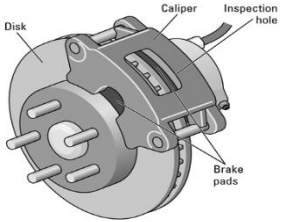
SIL IEC 61508

Moving to Strategic Use of Open Source



* Source: Gartner Group

PARTS



Source file

library

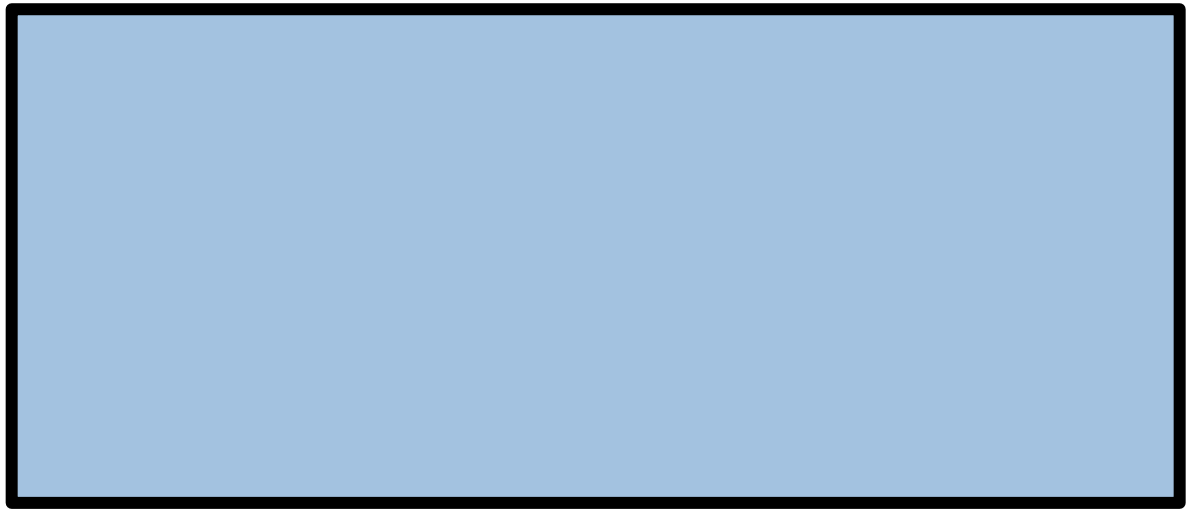
Application

Linux Runtime

Container

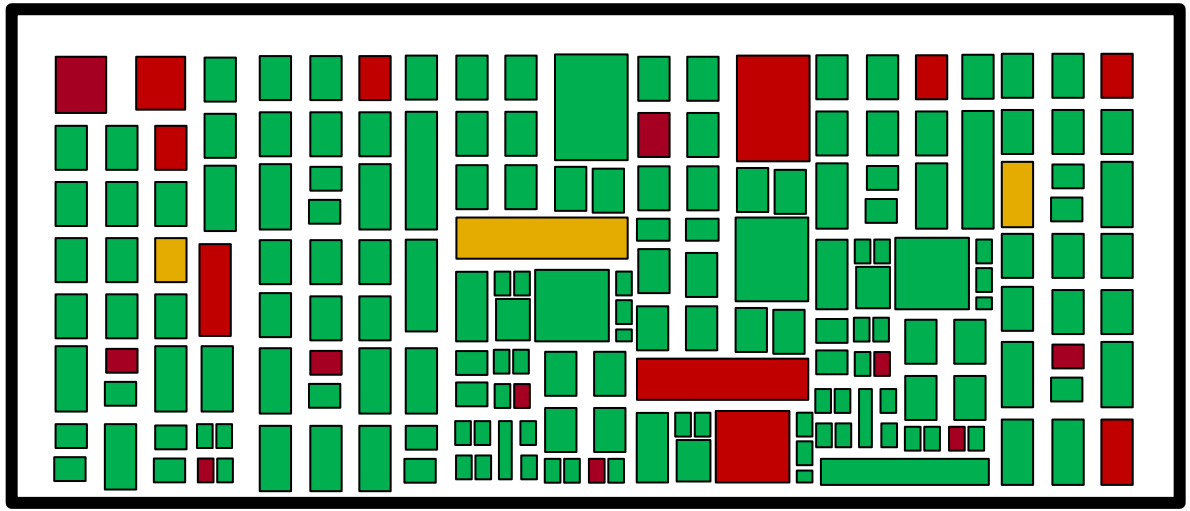
Modern Day Software [2018]

application • library • container • runtime



Modern Day Software [2018]

application • library • container • runtime

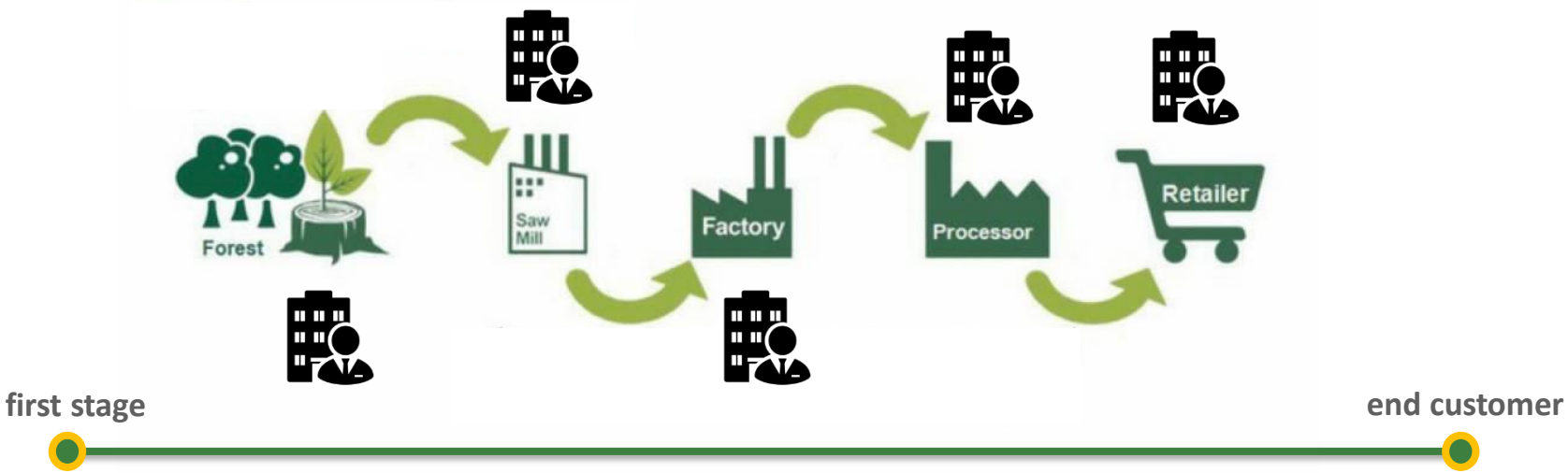


Company IP

Open Source

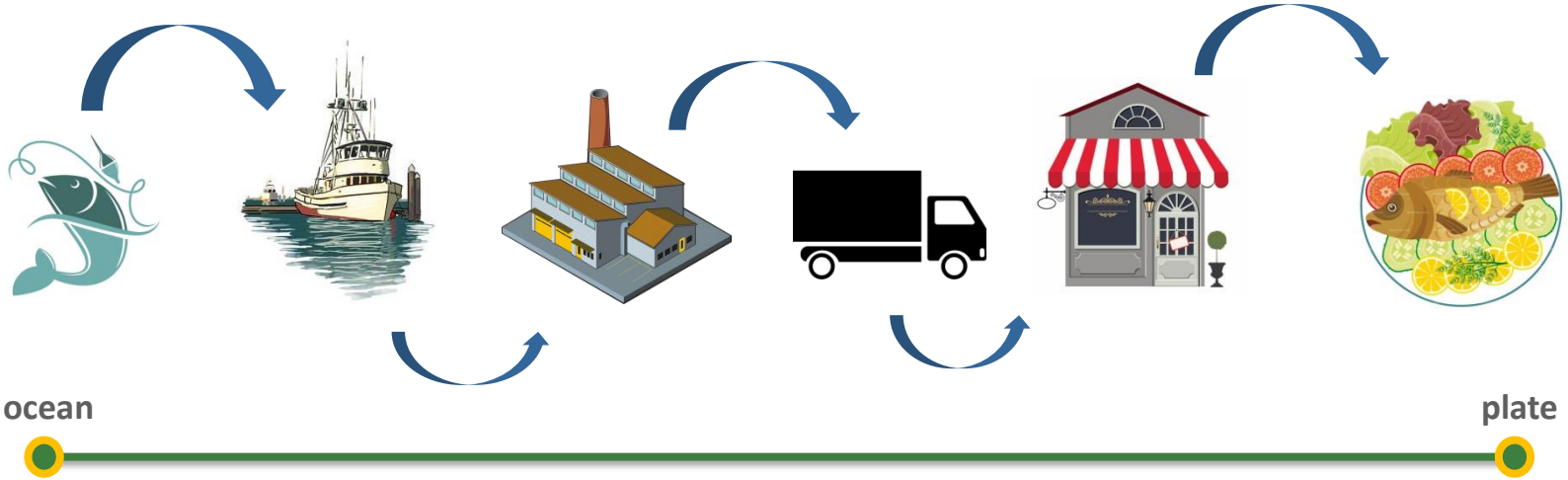
3rd Party Commercial

Chain of Custody

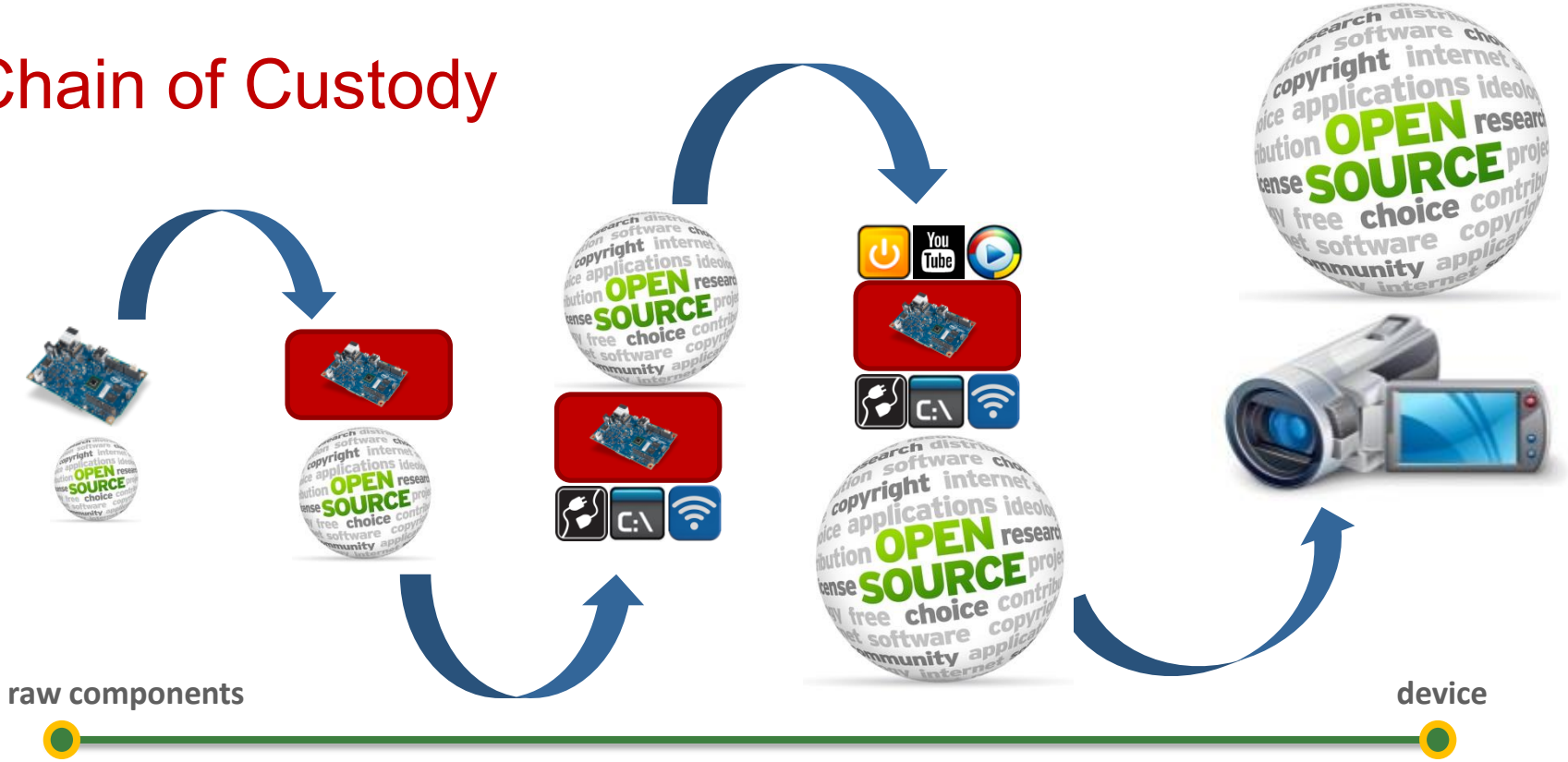


chain of custody - the unbroken path a product takes from the **first stage** in the supply chain to the **end customer** including - raw materials, their conversion, production and along distribution lines

Chain of Custody



Chain of Custody



Open Source Bill of Materials

Open Source BOM

- ☑ async 0.6.2
- ☑ beecrypt 4.2.1
- ☑ busybox 1.22.3
- ☑ core-utils 8.24
- ☑ openSSL 1.0.2d
- ☑ zlib 1.2.8

Open Source Bill of Materials

License Compliance

Open Source BOM

- ☑ async 0.6.2
- ☑ beecrypt 4.2.1
- ☑ busybox 1.22.3
- ☑ core-utils 8.24
- ☑ openSSL 1.0.2d
- ☑ zlib 1.2.8

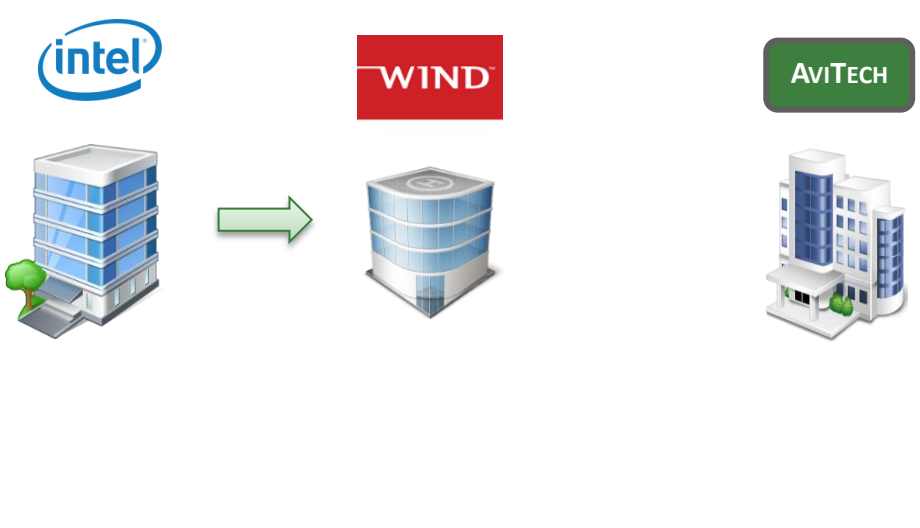
Artifacts

- Source Code
- Notices
- Open Source BOM
- SPDX data

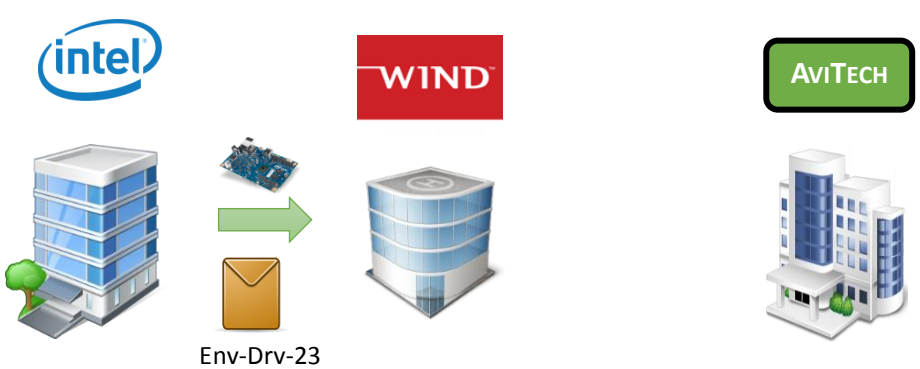
OPENCHAIN CONFORMANCE 1.1

IoT/Embedded Device

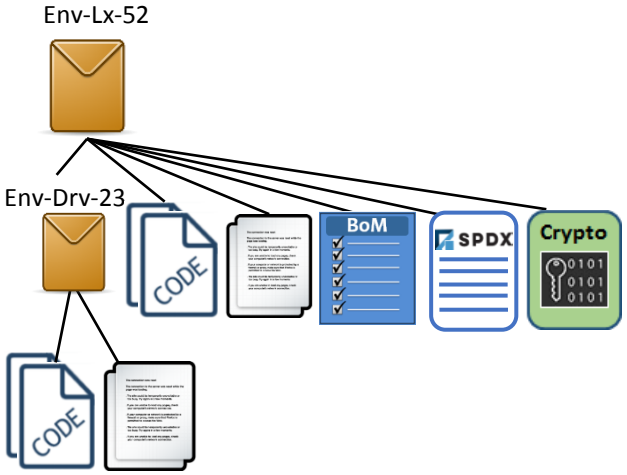
Chain of Custody

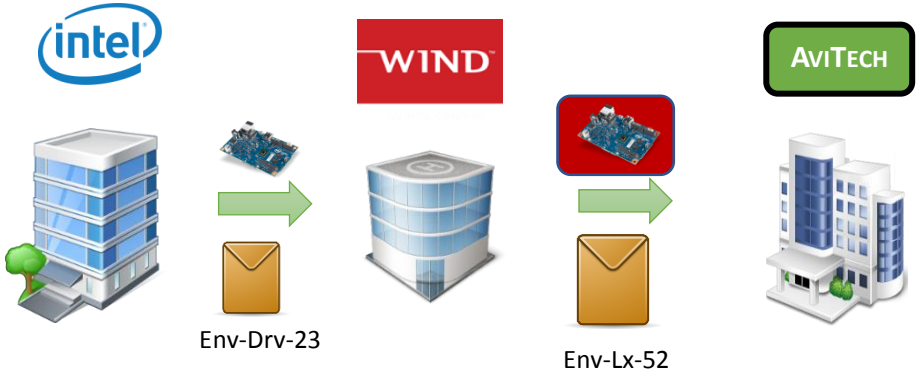


Chain of Custody

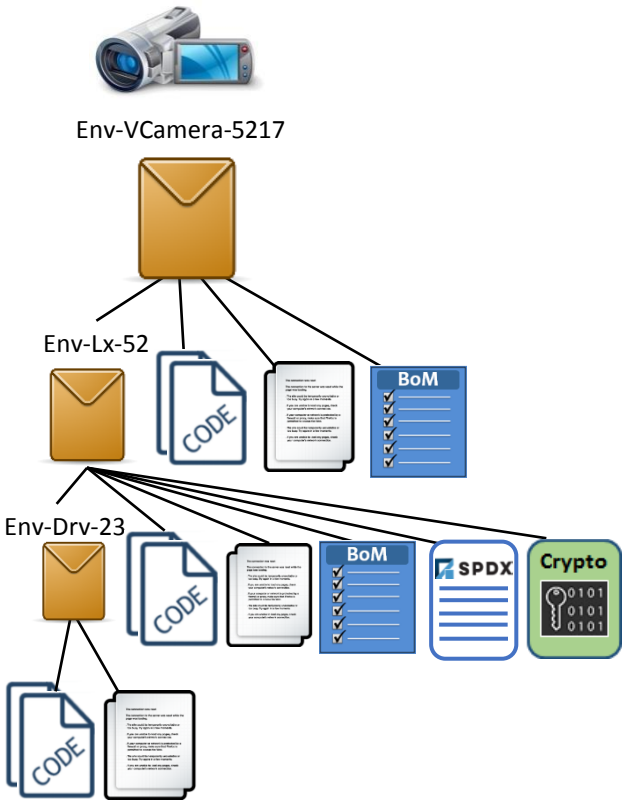


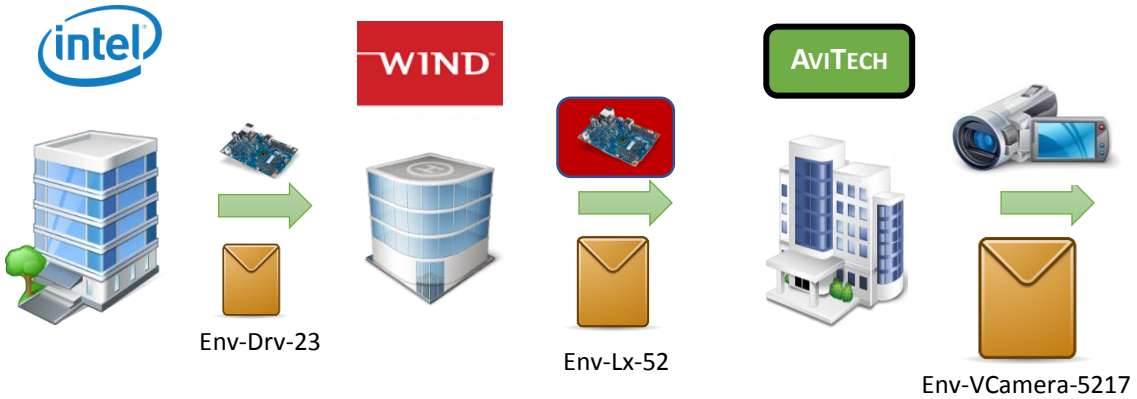
Chain of Custody



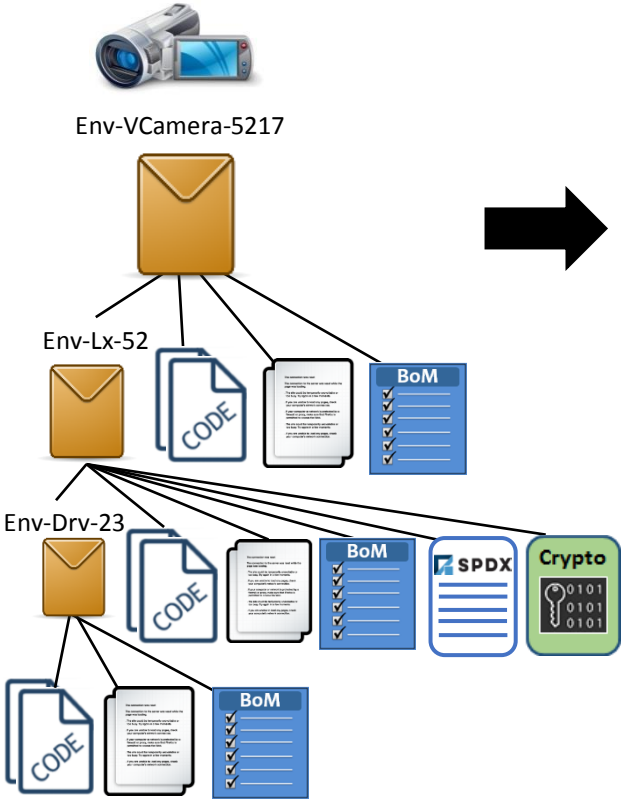


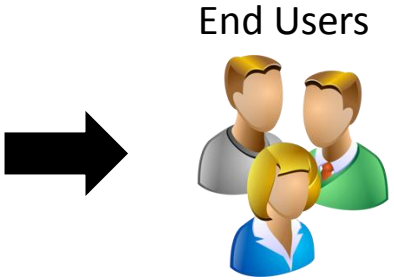
Chain of Custody





Chain of Custody Challenge

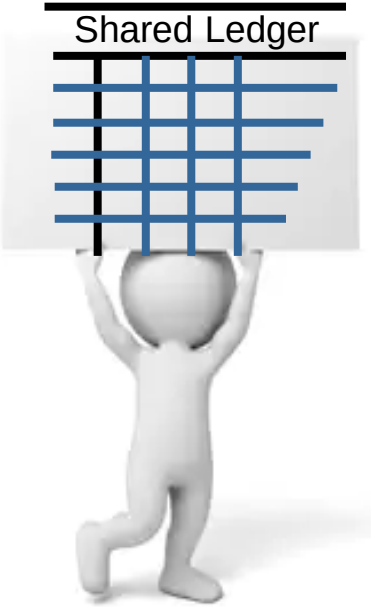




i) ***Accountability*** *- How can we help trust each supplier is preparing the correct artifacts?*

ii) ***Access*** *- How can we facilitate the collection and delivery of all artifacts?*

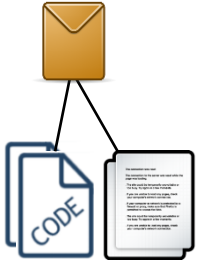
Part II: Solution



Shared Ledger

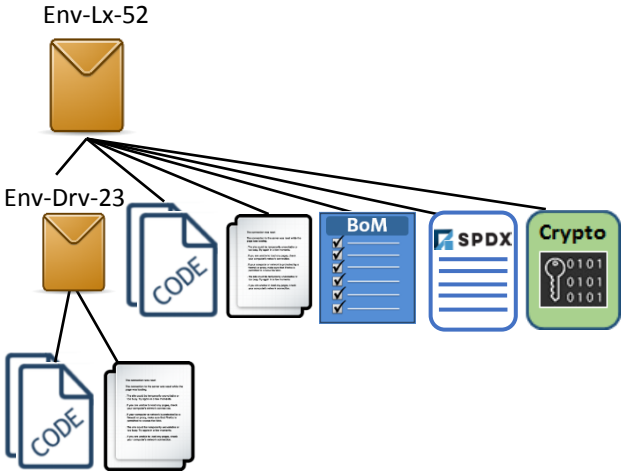
Part/Env ID	Supplier	Action	Artifacts
Env-Drv-23	Intel-ID	add	 

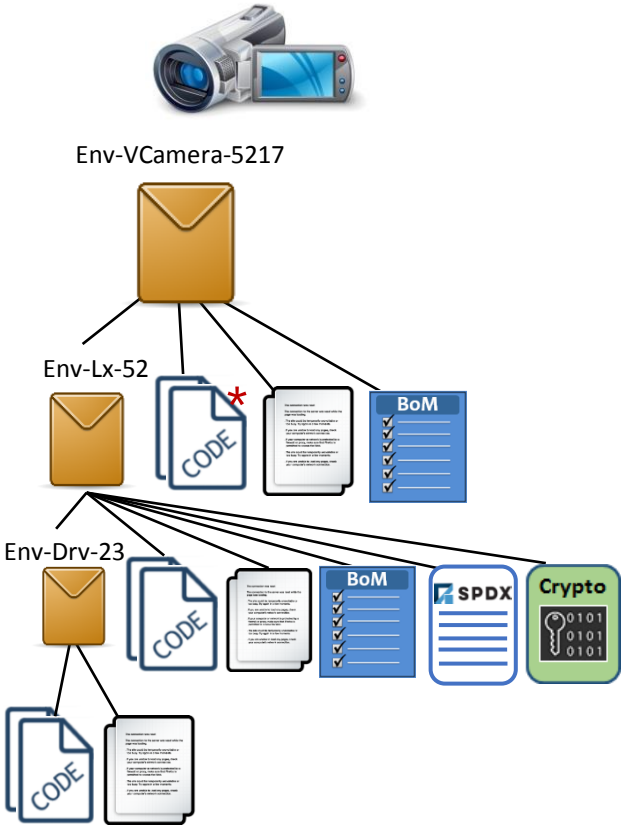
Env-Drv-23



Shared Ledger

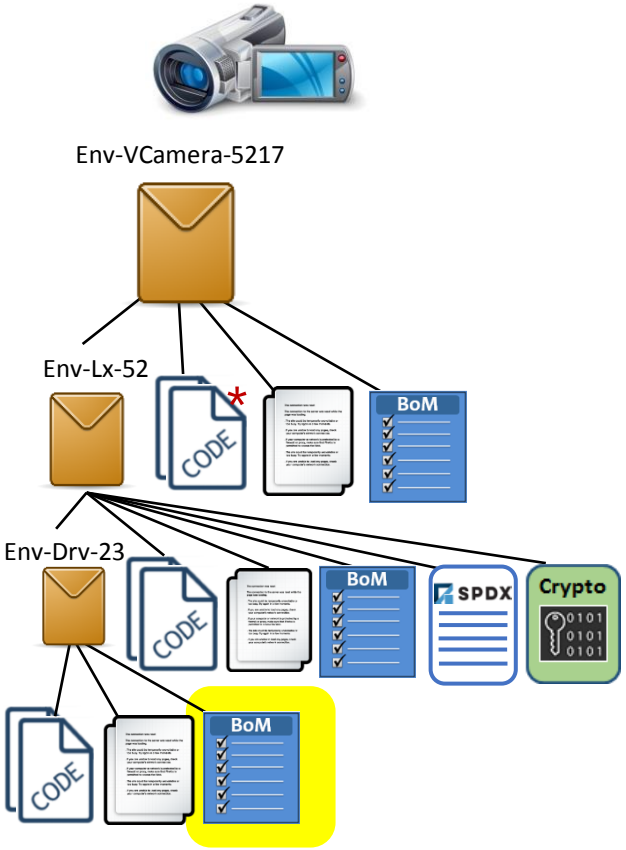
Part/Env ID	Supplier	Action	Artifacts
Env-Drv-23	Intel-ID	add	CODE
Env-Lx-52	WR-ID	add	Env-Drv-23 CODE BoM SPDX Crypto





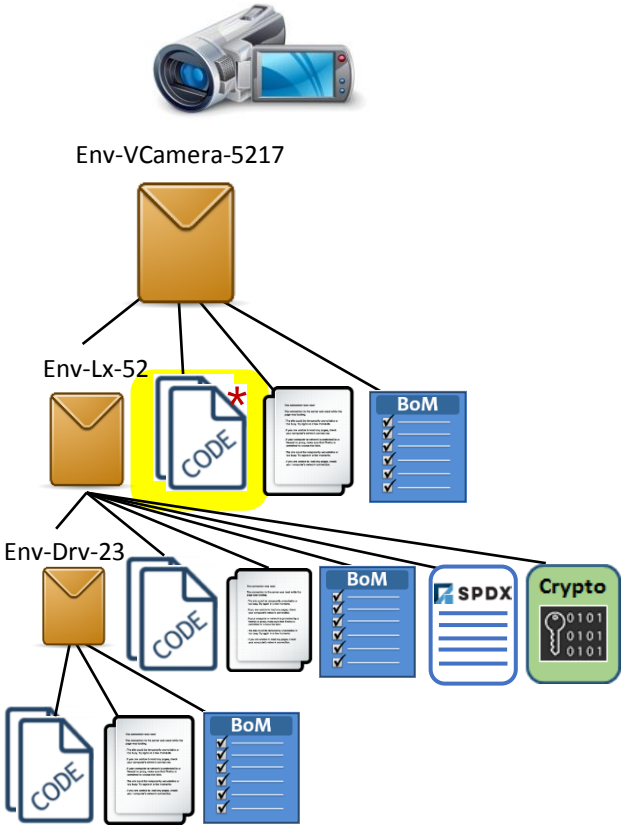
Shared Ledger

Part/Env ID	Supplier	Action	Artifacts
Env-Drv-23	Intel-ID	add	CODE
Env-Lx-52	WR-ID	add	Env-Drv-23 CODE BoM SPDX Crypto
Env-VCam-5217	AvTec-ID	**add**	Env-Lx-52 CODE BoM



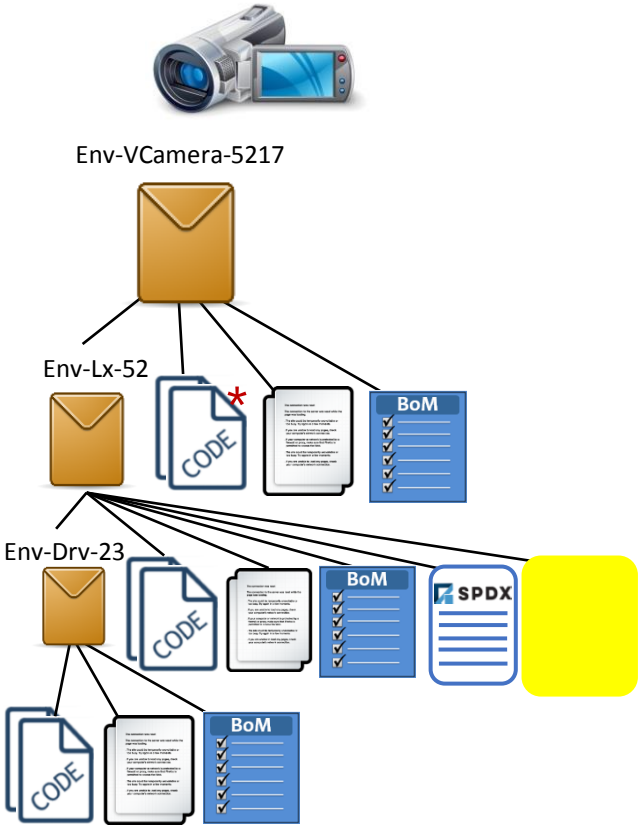
Shared Ledger

Part/Env ID	Supplier	Action	Artifacts
Env-Drv-23	Intel-ID	add	CODE
Env-Lx-52	WR-ID	add	Env-Drv-23, CODE, BoM, SPDX, Crypto
Env-VCam-5217	AvTec-ID	add	Env-Lx-52, CODE, BoM
Env-Drv-23	WR-ID	**add**	BoM



Shared Ledger

Part/Env ID	Supplier	Action	Artifacts
Env-Drv-23	Intel-ID	add	CODE
Env-Lx-52	WR-ID	add	Env-Drv-23 CODE BoM SPDX Crypto
Env-VCam-5217	AvTec-ID	add	Env-Lx-52 CODE BoM
Env-Drv-23	WR-ID	add	BoM
Env-VCam-5217	AvTec-ID	update	CODE



Shared Ledger

Part/Env ID	Supplier	Action	Artifacts
Env-Drv-23	Intel-ID	add	CODE
Env-Lx-52	WR-ID	add	Env-Drv-23, CODE, BoM, SPDX, Crypto
Env-VCam-5217	AvTec-ID	add	Env-Lx-52, CODE, BoM
Env-Drv-23	WR-ID	add	BoM
Env-VCam-5217	AvTec-ID	update	CODE
Env-Lx-52	WR-ID	**delete**	Crypto

ID	Org	Artifact
233	WR	source
491	WR	notice
524	Intel	source
901	Intel	SPDX

ID	Org	Artifact
233	WR	source
491	WR	notice
524	Intel	source
901	Intel	SPDX

ID	Org	Artifact
233	WR	source
491	WR	notice
524	Intel	source
901	Intel	SPDX

ID	Org	Artifact
233	WR	source
491	WR	notice
524	Intel	source
901	Intel	SPDX

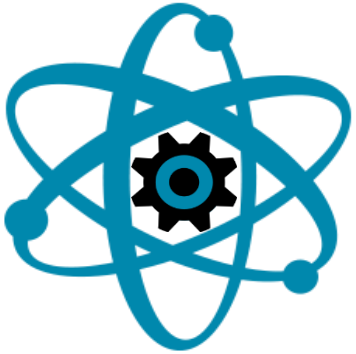
Consensus

ID	Org	Artifact
233	WR	source
491	WR	notice
524	Intel	source
901	Intel	SPDX

ID	Org	Artifact
233	WR	source
491	WR	notice
524	Intel	source
901	Intel	SPDX

ID	Org	Artifact
233	WR	source
491	WR	notice
524	Intel	source
901	Intel	SPDX

Technology



Blockchain

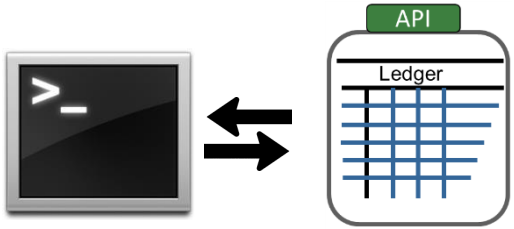
- A digital ledger that maintains a historical record of executed transactions
- Like a database it can record information of various types (e.g., artifacts:)
- Unlike databases it uses cryptography to ensure each record is **immutable**
- Data is replicated across a network of servers (ledger nodes)
- Eliminates dependence on a central authority/agent

HYPERLEDGER Sawtooth

SParts Project

SPARTS
Software Parts Ledger

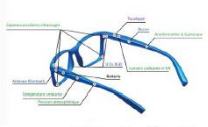
- SParts - Provides free digital ledger to track open source artifacts across a supply chain
- Blockchain platform: Hyperledger Sawtooth
- Source code:
  https://github.com/hyperledger-labs/SParts/
- Three components
  - Ledger (container)
  - Command Line Interface
  - Supply Chain network directory (www.spartshub.com)
- Documentation:
  - https://sparts.readthedocs.io/en/latest/
  - Ledger API:
    https://sparts.readthedocs.io/en/latest/web/ledger/api.html



Part III: Use Case

Zephyr Project

- **Zephyr** is a small real-time operating system for connected, resource-constrained devices
- Under the Apache License 2.0
- Supports multiple architectures (100+ boards)
- Examples:



Ellcie-Healthy Smart Connected Eyewear

ProGlove Scanning Gloves

Intellinium Safety Shoes

Rigado IoTGateway

Grush Gaming Toothbrush

hereO Smartwatch

Blocks Modular Smartwatch

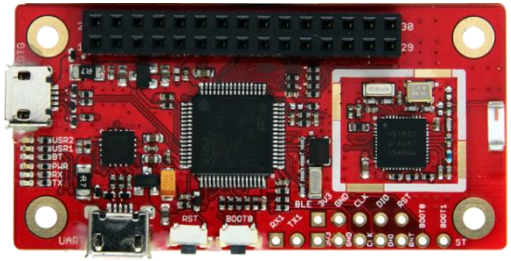
Antmicro Badge

GNARBOX 2.0 SSD

Zephyr Project

- **Zephyr** is a small real-time operating system for connected, resource-constrained devices
- Under the Apache License 2.0
- Supports multiple architectures (100+ boards)
- Demo: 96boards Carbon

Smart Solar Panel (SSP)



+

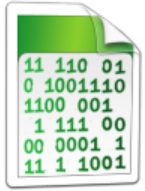
Zephyr™

+

apps

=

SSP-Z96



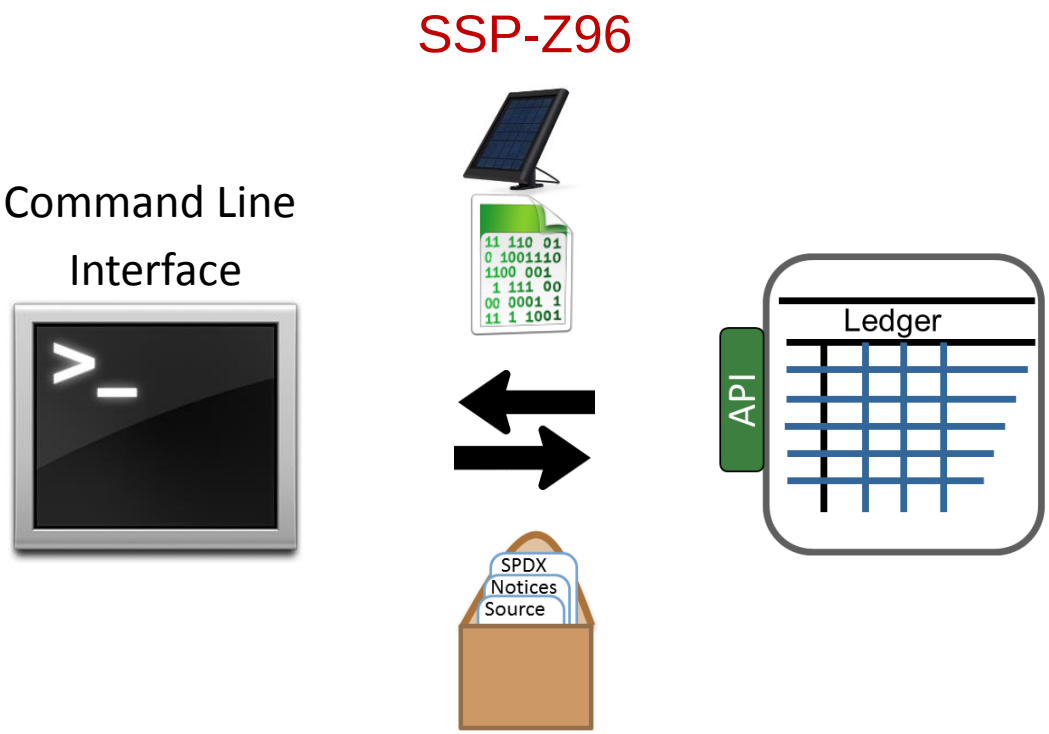
Smart Solar Panel runtime

Part IV: Demo

SPARTS
Software Parts Ledger

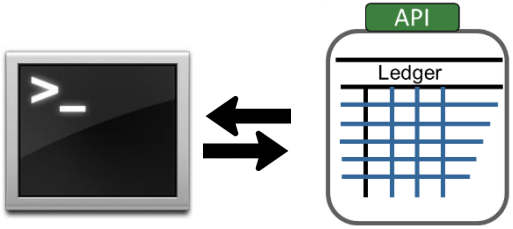
An open shared ledger used to track software part compliance artifacts across the supply chain

Demo



SParts Project

- Hyperledger lab project under Apache 2.0
- Blockchain platform: Hyperledger Sawtooth
- Source code:
  https://github.com/hyperledger-labs/SParts/
- Three components
  - Ledger (container)
  - Command Line Interface
  - Network Directory look up (www.spartshub.com)

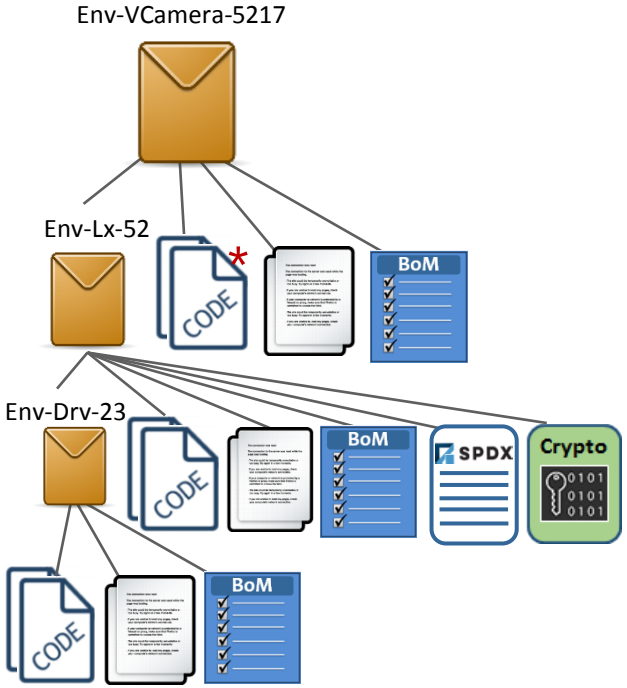


Summary

- SParts – Free and Open Ledger - track open source components and their meta data of IoT devices
- Code is available under the Apache-2.0
- Looking for contributors:
  - Ledger development
  - Web UI for end users and admins
- Useful internally to track 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