

# Solving the Supply Chain Puzzle with SPDX, OpenChain & Hyperledger

Mark Gisi

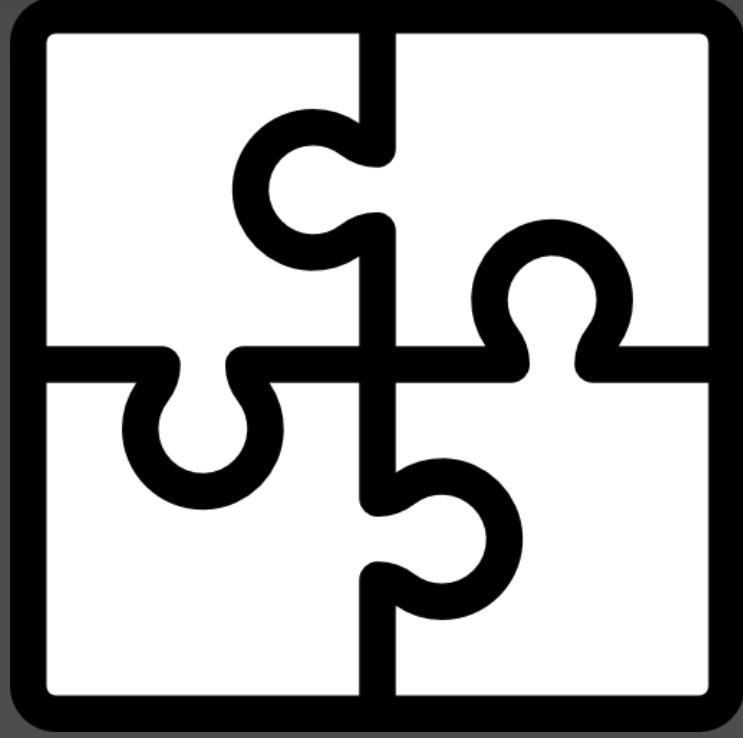
Sameer Ahmed



Open Source Leadership Summit  
February 2017

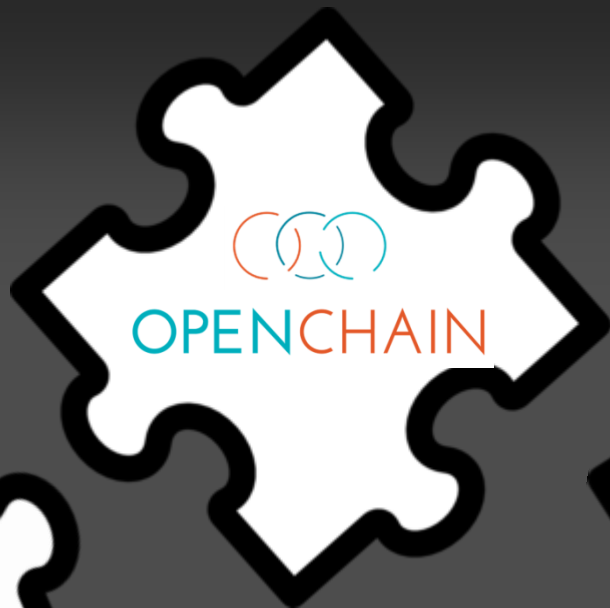


Establish Trust



in using  
Open Source

across the  
Supply Chain



# 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:
  - i. Legal Notices document
  - ii. Obligatory Source Code
  - iii. Licensing data (SPDX)
  - iv. Cryptography info
  - v. Security Vulnerabilities

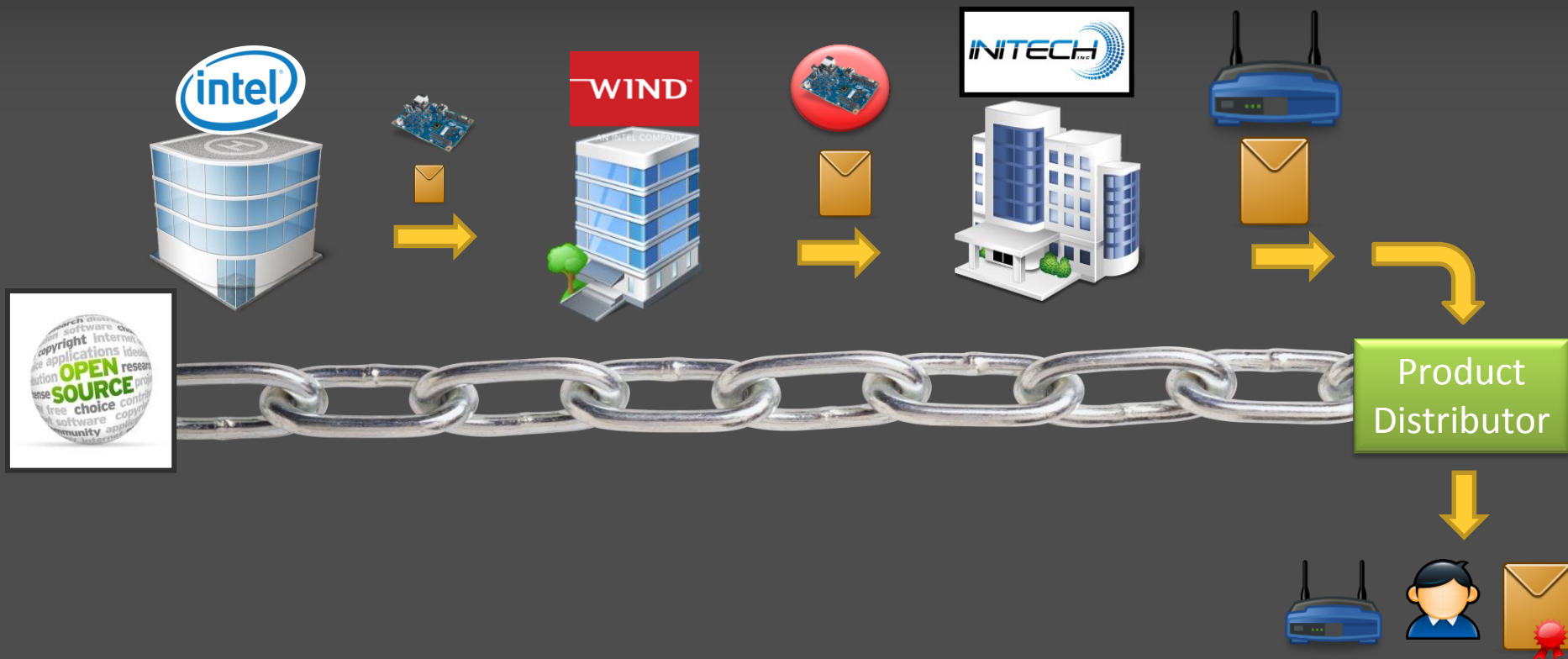
:



## A blue and black wireless router is positioned above a broken metal chain. The chain is composed of several interlocking links, with a noticeable gap in the middle. To the right of the chain, there is a green rectangular box containing the text "Product Distributor" in white. The background is a solid dark gray.



# Software Supply Chain



# IoT/Embedded Device Requirement





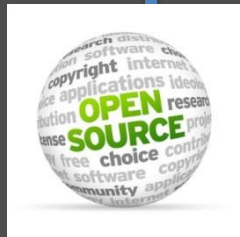




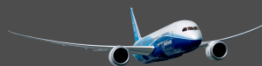
- Linux Foundation's solution to standardize licensing information exchange within the software supply chain
- Format for recording and sharing *licensing* and *copyright* information of a software package

# Software Supply Chain

Open Source  
Projects



Device  
Distributor



# Wind River Delivers SPDX data for Linux



- ✓ **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

# BusyBox

# Files	License
401	GPL-2.0+
265	GPL-2.0
81	GPL 1.0+
40	LGPL-2.1+
41	BSD-3-Clause
27	LGPL 2.0+
21	Public-domain
3	MIT
2	RSA-Security
1	X11-style
1	NTP
1	GPL-2.0+-with-bison-exception
1	Freeware
1	Free-SW
1	BSD-4-Clause-UC



**Document****Package****File****Other Licenses****Relations****Annotations**

```
##-----  
## Document Information  
##-----
```

DataLicense: CC0-1.0

SPDXID: SPDXRef-DOCUMENT

DocumentName: busybox-1.26.1.tar.bz2

DocumentNamespace: <http://spdx.windriver.com/Reports2.0/e7b8b3e2d2c>

DocumentComment: <text>This file contains computer automated SPDX ...

:



Document

Package

File

Other Licenses

Relations

Annotations

PackageName: busybox-1.26.1.tar.bz2  
SPDXID: SPDXRef-Pkg-busybox-1.26.1.tar.bz2-e7b8b3e2d2e92c09683af...  
PackageFileName: busybox-1.26.1.tar.bz2  
PackageDownloadLocation: NOASSERTION  
PackageVerificationCode: af2c8199559ebe709ebb5e89532900f9da0f7661  
PackageChecksum: SHA1: e7b8b3e2d2373d9e92c09683af7ce52bba2ee93b  
PackageLicenseConcluded: GPL-2.0  
PackageLicenseDeclared: GPL-2.0  
PackageLicenseInfoFromFiles: GPL-1.0+  
PackageLicenseInfoFromFiles: LGPL-2.0+  
PackageLicenseInfoFromFiles: GPL-2.0  
PackageLicenseInfoFromFiles: GPL-2.0+  
PackageLicenseInfoFromFiles: BSD-3-Clause  
PackageLicenseInfoFromFiles: LGPL-2.1+  
PackageLicenseInfoFromFiles: MIT  
:  
:



Document

Package

File

Other Licenses

Relations

Annotations

**FileName:** ./busybox-1.26.1/libbb/change\_identity.c

**SPDXID:** SPDXRef-1515-File-change\_identity.c-e45ff0e65618385496162eb3686...

**FileType:** SOURCE

**FileType:** TEXT

**FileChecksum:** SHA1: e45ff0e65618385496162eb368665c16897fe18a

**LicenseConcluded:** BSD-3-Clause

**LicenseInfoInFile:** BSD-3-Clause

**FileCopyrightText:** <text> copyright 1989 - 1991, julianne frances haugh  
<jockgrrl@austin.rr.com> </text>

:





Document

Package

File

Other Licenses

Relations

Annotations

## ----- License Ref -----

##

**LicenseID:** LicenseRef-6

**ExtractedText:** <text>

/\*

\* Copyright (c) 2002 by David I. Bell  
\* Permission is granted to use, distribute, or modify this source,  
\* provided that this copyright notice remains intact.

\*


\* The "ed" built-in command (much simplified)


\*/ </text>

**LicenseName:** NOASSERTION




# spdx.WindRiver.com

**WIND RIVER**



## SPDX Cloud



We provide a free service that enables you to create SPDX files for your software packages. The server utilizes various algorithms and heuristics to determine licensing information for each file based solely on the information contained in the software package. Upload a package of your choice below and receive a computer generated SPDX file by email. Please send feedback to: [spdx.windriver.com](mailto:spdx.windriver.com).

For uploading a package, acceptable package extensions are "tar.bz2", "tar.gz" and ".zip".

---

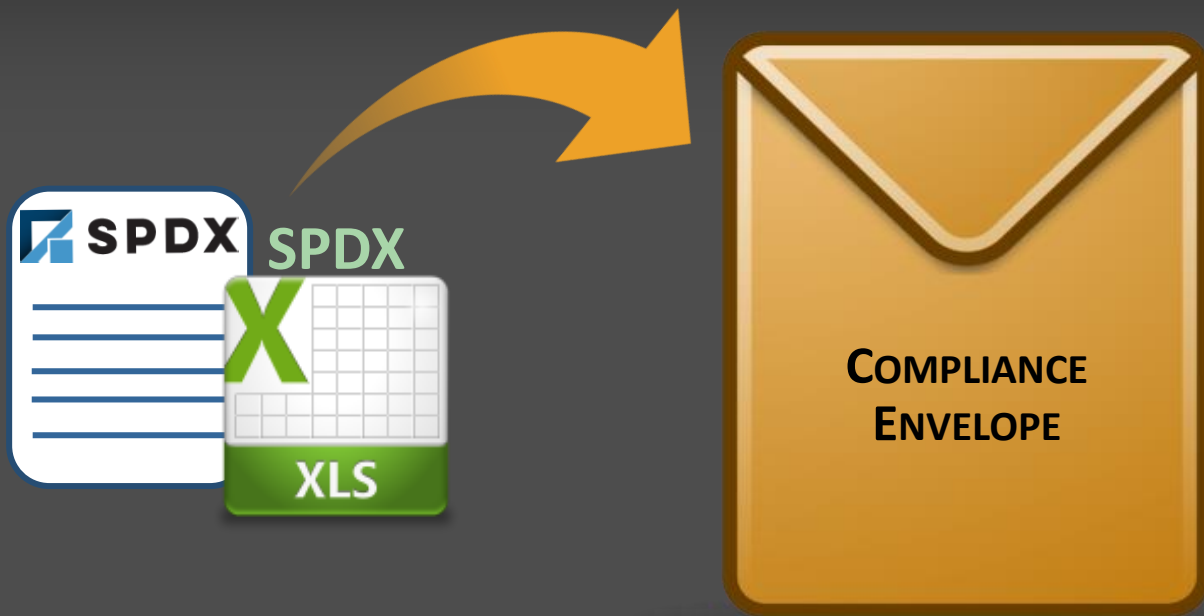
### Option #1: Upload a package

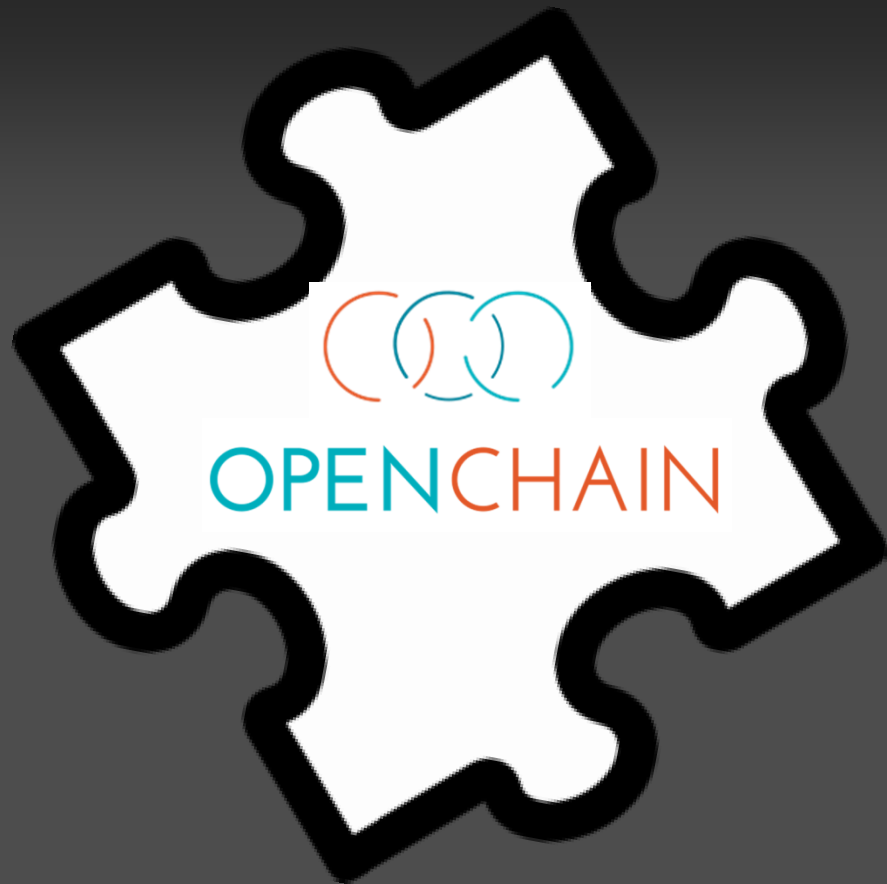
---

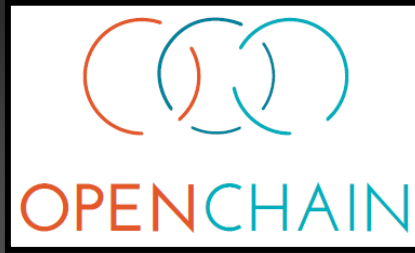
Upload a package:  No file chosen

Email address:

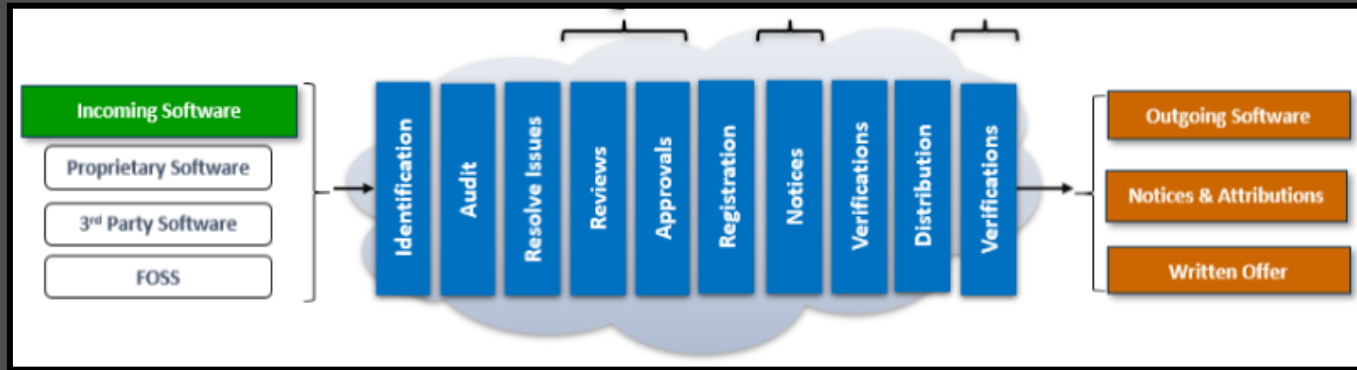
☒ Spreadsheet ☐ Name/Value ☐ SPDX X-ray Viewer





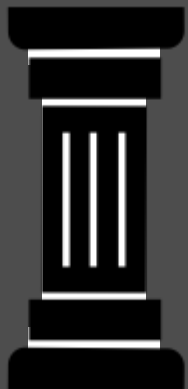


OpenChain is to open source license compliance what ISO 9001 is to software quality



● — Open Source Compliance Management End-to-End — ●

# OpenChain Six Pillars



Policy

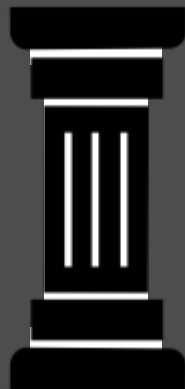
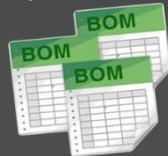


Training

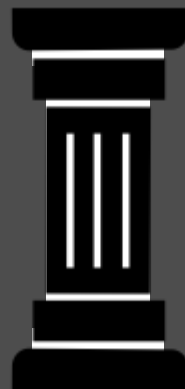
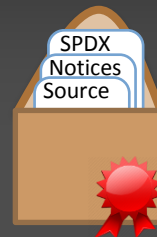


Roles &  
Responsibilities

Open Source



Identify,  
Review,  
Clear, Track

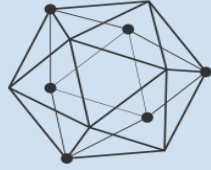


Preparation of  
Compliance  
Artifacts



Community  
Engagement





# HYPERLEDGER

- A Linux Foundation open source initiative
- Infrastructural support for blockchain-based distributed ledgers
- Plumbing analogous to Linux but for distributed ledgers
- Early Stage (one year old)
- A narrow focus – support for a supply chain ledgers





# What is a Ledger?

# Financial Asset Ledgers

[illegible]

# Stock Asset Ledgers

## Trade Record Ledger Summary

Transactions dated from February 1, 2003 to December 31, 2003

Trade Files A021523 through A030033

Trade Number: **A021523**

Address: 32 Winds Drive

Sold Dec. 13, 2002

Closed Feb. 14, 2003

			<u>Pending</u>	<u>Associate</u>	<u>Other Broker</u>	<u>Office</u>	<u>Total</u>	<u>GST</u>
Feb 14.03	Goods & Services Tax	TRS					182.00	
Feb 14.03	Abrams, Emilio	TRS		2,600.00			2,600.00	182.00
Feb 26.03	Sutton Group- Tower Realty Inc.	RCD					(2,782.00)	
Feb 26.03	Abrams, Emilio	PRL	2,600.00	(2,600.00)				
Feb 28.03	Abrams, Emilio	CPR	(2,600.00)					(182.00)
			0.00	0.00	0.00	0.00	0.00	0.00

Trade Number: **A021533**

Address: 135 Hardwood Boulevard

Sold Dec. 10, 2002

Closed Feb. 14, 2003

			<u>Pending</u>	<u>Associate</u>	<u>Other Broker</u>	<u>Office</u>	<u>Total</u>	<u>GST</u>
Feb 14.03	Goods & Services Tax	TRS					543.90	
Feb 14.03	Gibbons, Ed	TRS		7,770.00			7,770.00	543.90
Feb 25.03	Homelife Gold Pacific Realty	RCD					(8,313.90)	
Feb 25.03	Gibbons, Ed	PRL	7,770.00	(7,770.00)				
Feb 28.03	Gibbons, Ed	CPR	(7,770.00)					(543.90)
			0.00	0.00	0.00	0.00	0.00	0.00

Trade Number: **A030033**

Address: 45 Yellow Road

Sold Jan. 8, 2003

Closed Feb. 12, 2003

			<u>Pending</u>	<u>Associate</u>	<u>Other Broker</u>	<u>Office</u>	<u>Total</u>	<u>GST</u>
Feb 12.03	Goods & Services Tax	TRS					388.50	
Feb 12.03	Henderson, Erin	TRS		5,550.00			5,550.00	388.50
Feb 25.03	Homelife/Chimman Real Estate	RCD					(5,938.50)	
Feb 25.03	Henderson, Erin	PRL	5,550.00	(5,550.00)				
Feb 28.03	Henderson, Erin	CPR	(5,550.00)					(388.50)
			0.00	0.00	0.00	0.00	0.00	0.00

## RENTAL VEHICLE LOG BOOK

VEHICLE CHASSIS NUMBER

VEHICLE REGISTRATION PLATE NUMBER:

### Detail of costs

[illegible]

# Hours Worked Ledgers

ID	Employee Name	Reg Hours Worked	Vacation Hours	Sick Hours	Overtime Hours
1001	Tony Smith	50	5	1	
1002	David Jones	40			
1003	Denise Smith	35	3		
1008	Sebastien Motte	50	5	1	
1011	Isabelle Scemia	40			2
1012	David Bristol	40	5	1	
1025	Anne Weiler	36		2	1
1032	Luka Abrus	40	5	1	
1049	David Ludwig	40	1		
1003	Denise Smith	35	3		
1008	Sebastien Motte	50	5	1	
1011	Isabelle Scemia	40			2
1012	David Bristol	40	5	1	
1025	Anne Weiler	36		2	1
1032	Luka Abrus	40	5	1	
1049	David Ludwig	40	1		
1003	Denise Smith	35	3		
1008	Sebastien Motte	50	5	1	
1011	Isabelle Scemia	40			2
1012	David Bristol	40	5	1	
1025	Anne Weiler	36		2	1
1032	Luka Abrus	40	5	1	
1049	David Ludwig	40	1		
Totals	9	371	24	#REF!	3

# Land Acquisition



# BlockChain Ledger Benefits

- Disintermediation - exchange w/o need of third party
- High quality data - complete, consistent, timely, accurate, & widely available
- Transparency and immutability - publicly viewable, transactions are immutable
- Durability, reliability, and longevity – no central point of failure, long lived
- Highly Secure



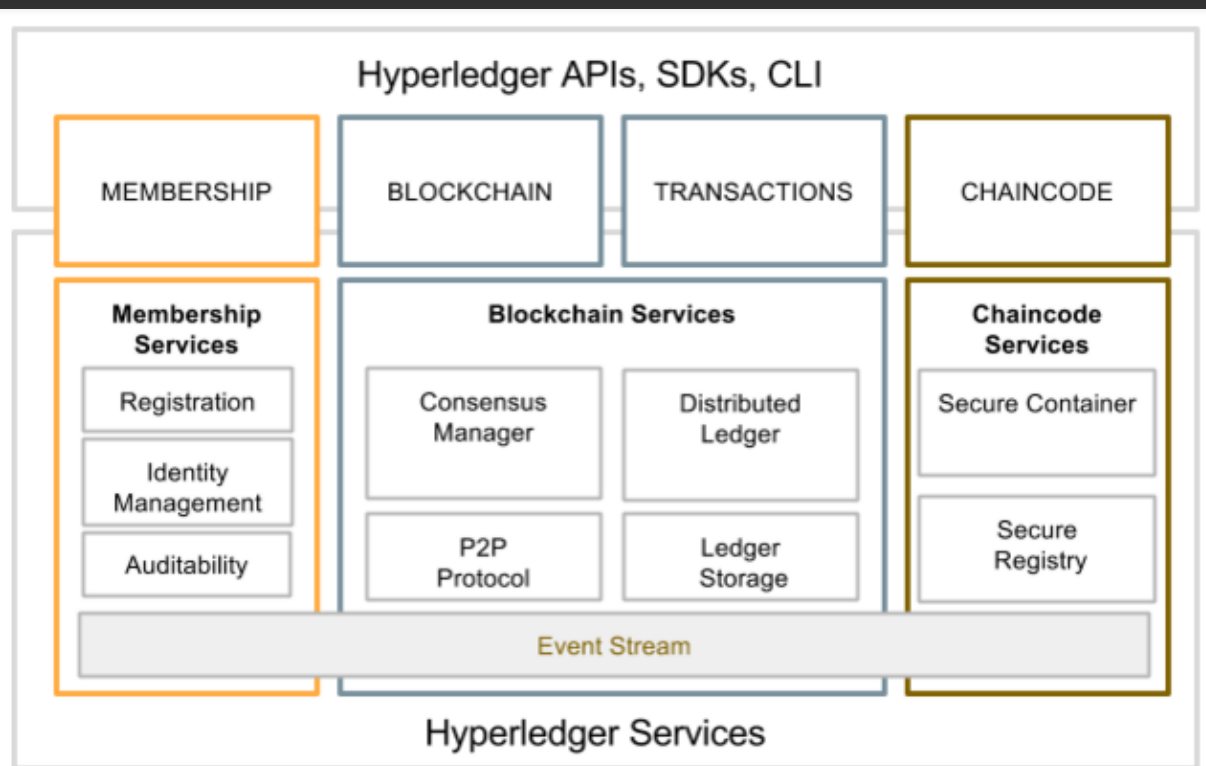


Figure 2: Hyperledger reference architecture



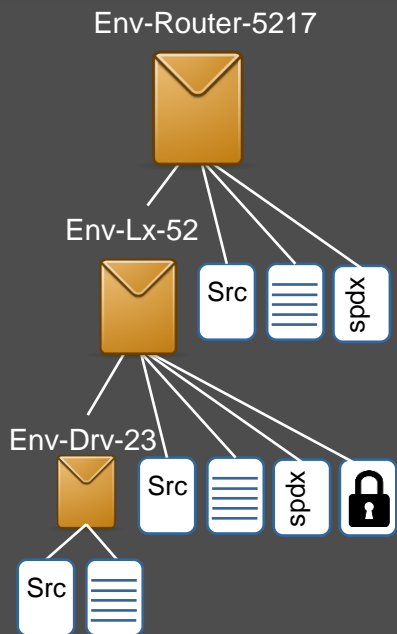
# HyperLedger

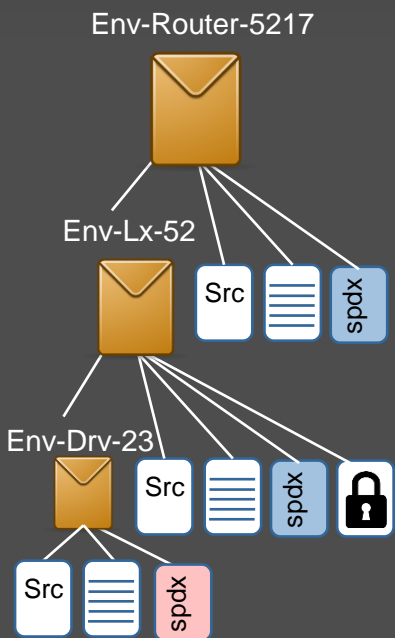


## HYPERLEDGER



# Compliance Ledger



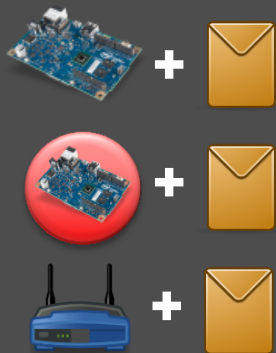








## Envelope Ledger

Envelope ID	Org	Action	Artifacts
Env-Drv-23	Intel-ID	create	Src
Env-Lx-52	WR-ID	create	Src  spdx
Env-Router-5217	ITech-ID	create	Src  spdx
Env-Drv-23	WR-ID	add	spdx

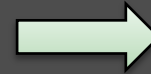
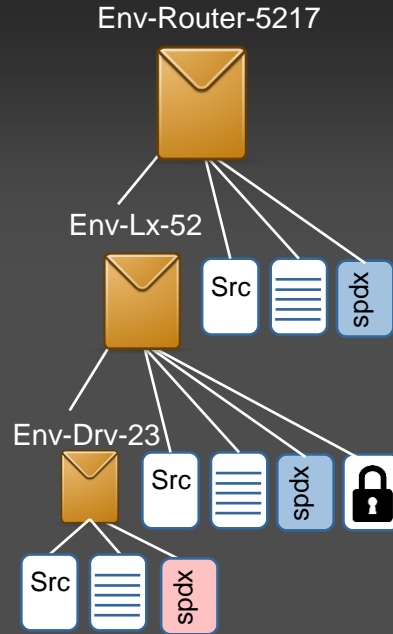
# Compliance Ledger

## Compliance Ledger



Dist-ID	Org	Action	Software ID	Envelope ID	QR Code
	Intel-ID	release	X-Driver 2.1	Env-Drv-23	
	WR-ID	release	WR Lx 9	Env-Lx-52	
	ITech-ID	release	Router 5217	Env-Router-5217	

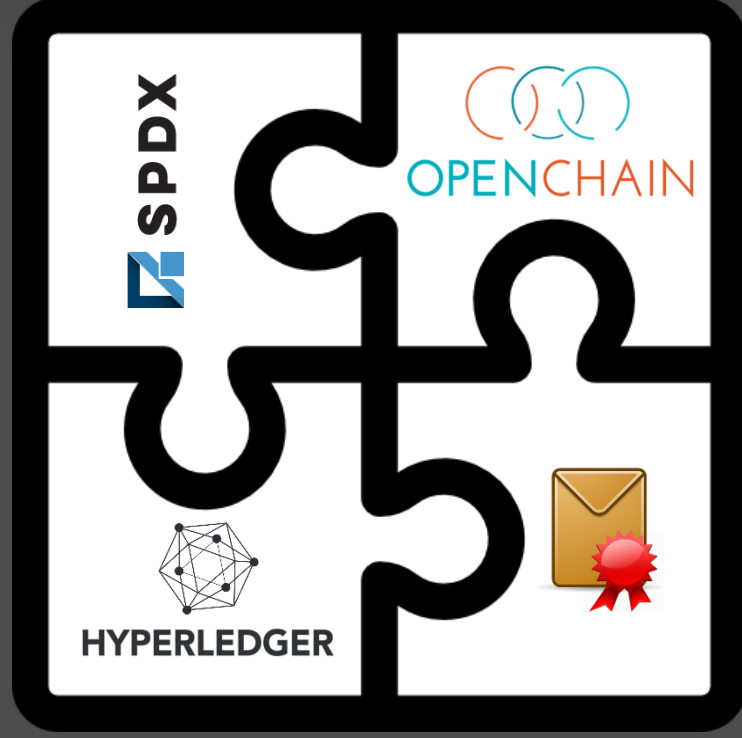
## IniTech 5217 Router



Product  
Distributor



Establish Trust



using  
Open Source

across the  
Supply Chain

Q & A

A hand holding a piece of white chalk, positioned below the 'Q & A' text on a blackboard.

# Contact



Mark.Gisi@WindRiver.com

