SBOM sg #5

What are the challenges that we still have.

OpenChain SBOM study Group

DEFINITIONS and ICONS

ACTION x

SBOM

Software component information

SBOM DOCUMENT

A file that contains software component information in a specific format such as SPDX or CycloneDX.

PUBLIC SOURCE PACKAGE

A source code package whose source code is publicly available on GitHub etc.

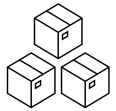
PRIVATE SOURCE PACKAGE

A source code package that is shared only between two or more specific parties, and the source code is not publicly available.

PUBLIC SOURCE PACKAGES

PRIVATE SOURCE PACKAGES

BINARY PACKAGE



BINARY PACKAGES

MODIFY

AGGREGATE

BUILD

outputs

inputs

WHAT IS THE HIGH QUALITY OF ~~SBOM~~ **SBOM DOCUMENT**?

- Proposal
  At SBOM-sg, I’d like to discuss not the quality of the software information being managed during the development, but rather **focus on the quality of the SBOM DOCUMENT** exchanged between two different parties.

WHAT IS THE HIGH QUALITY SBOM DOCUMENT?

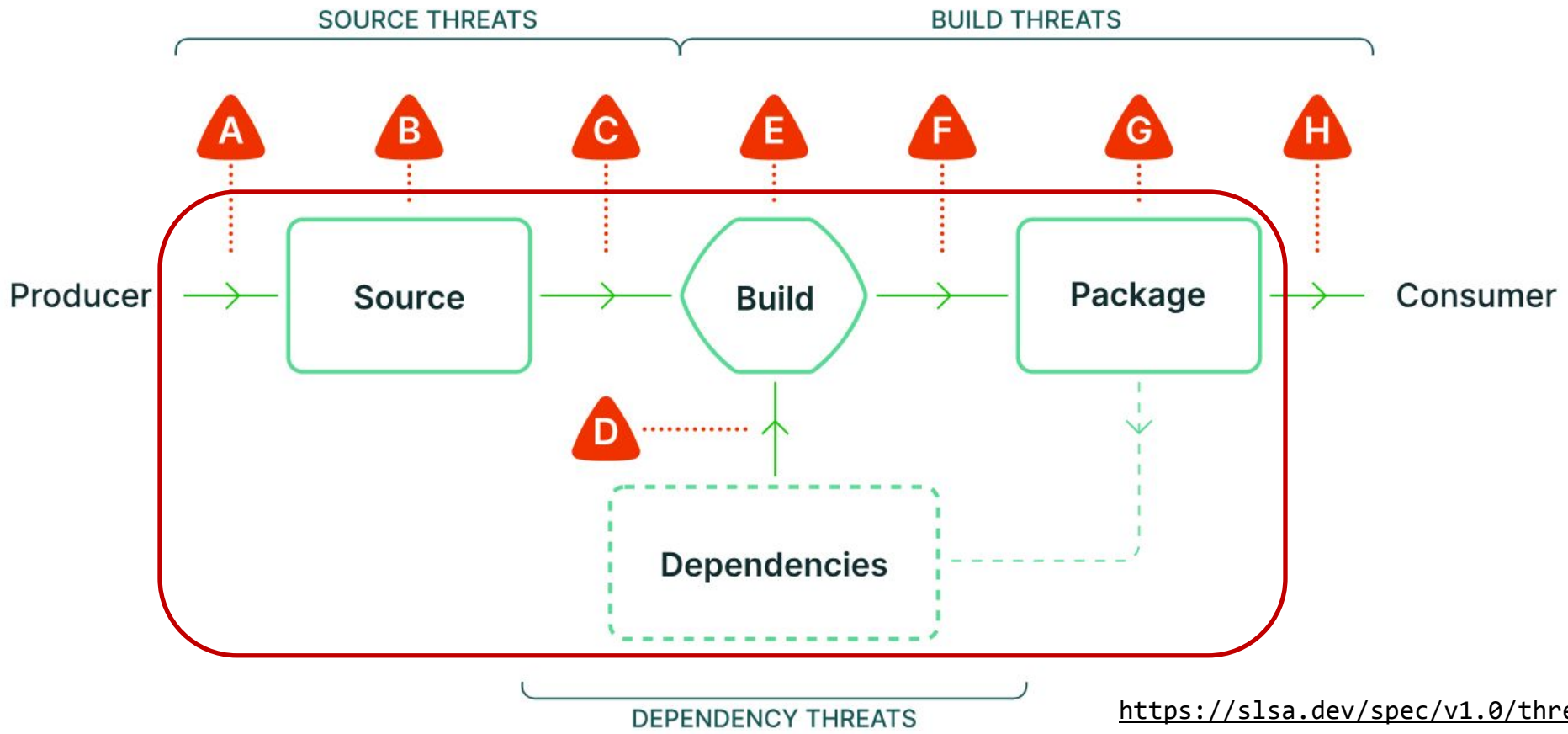
https://github.com/interlynk-io/sbomqs?tab=readme-ov-file#what-is-a-high-quality-sbom

A high quality SBOM should aplly support managing software assets, license information and Intellectual Property as well as provide a base for configuration management, vulnerability handling and incident response.

↓

The quality of the SBOM DOCUMENT depends on whether the SBOM DOCUMENT **contains information that uniquely identifies software, license, intellectual property, and vulnerability information.**

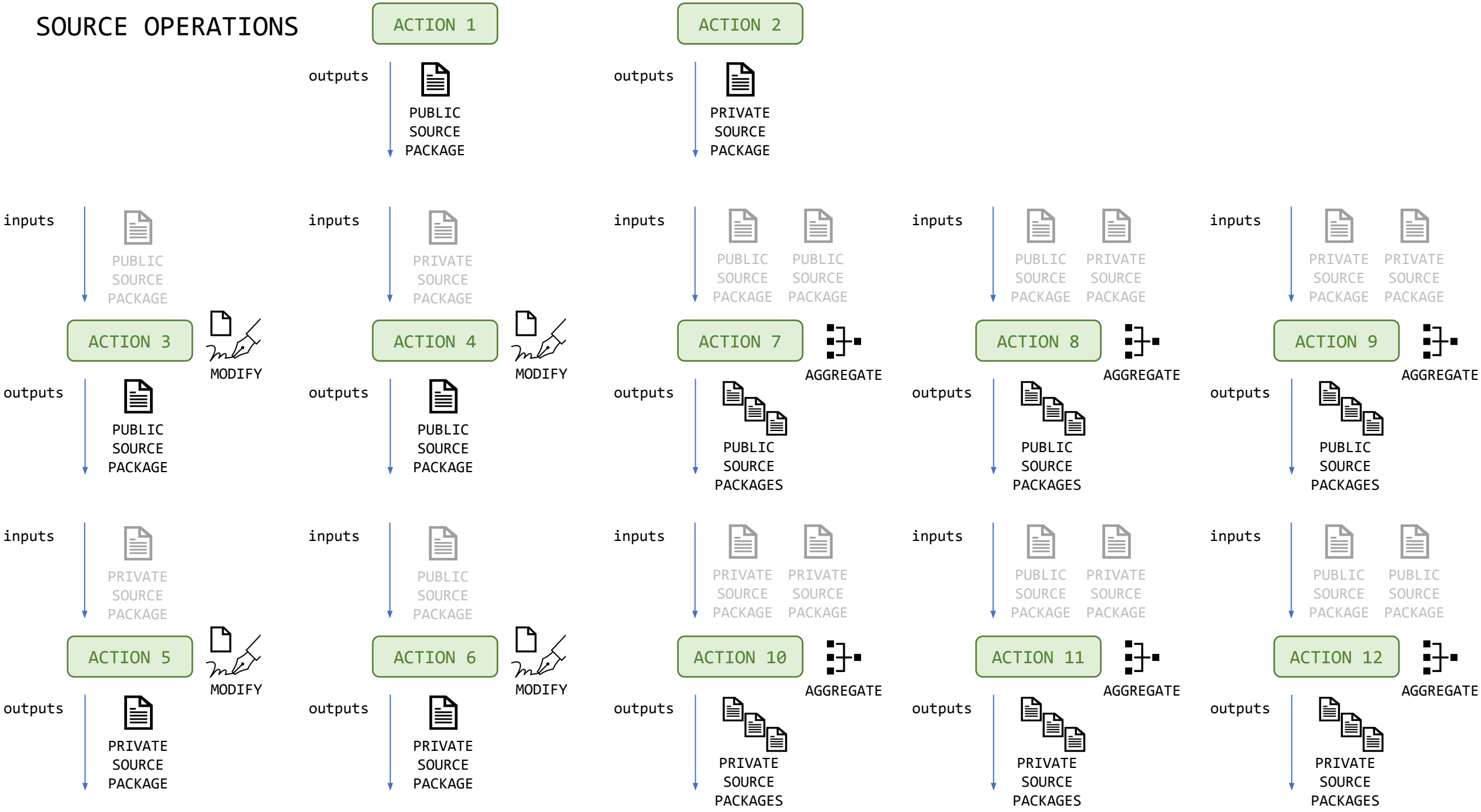
Break down the SLSA software supply chain FROM SOURCE TO BINARY



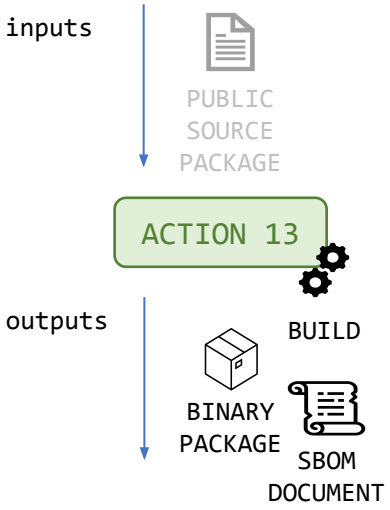
https://slsa.dev/spec/v1.0/threats-overview

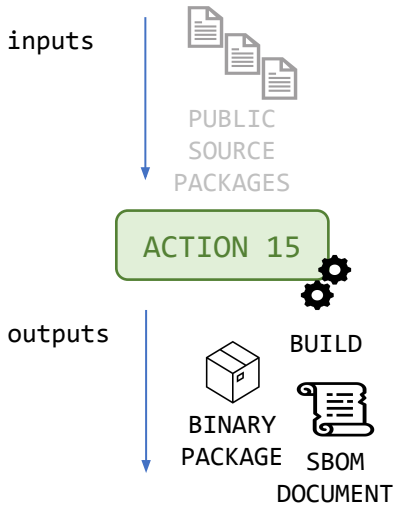
LISTING ALL ACTORS

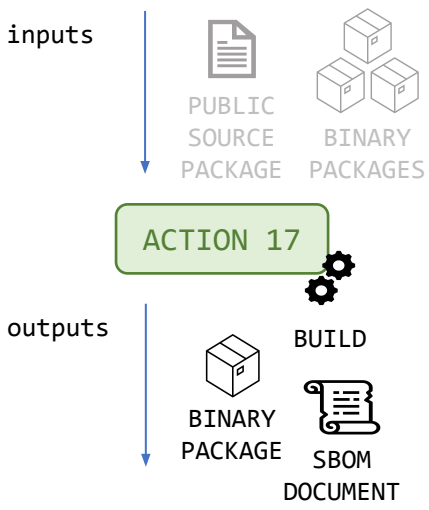
SOURCE OPERATIONS

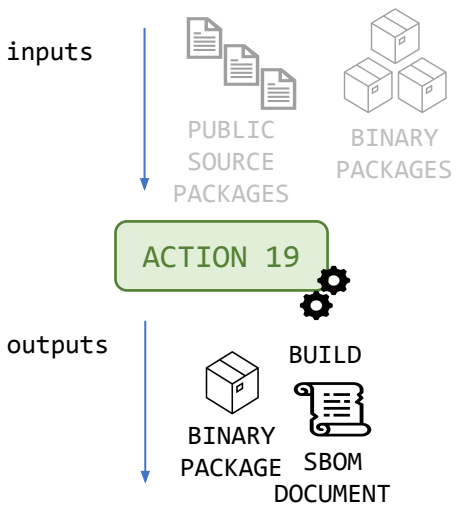


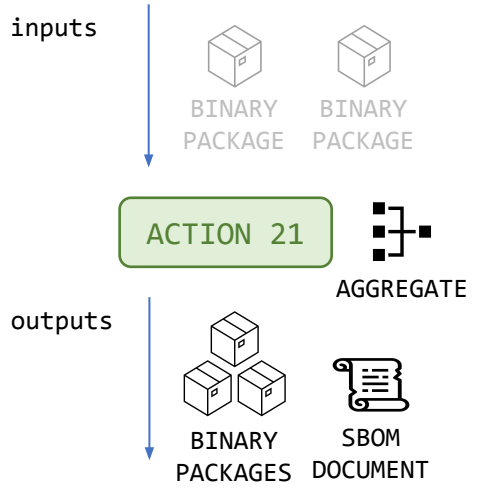
SOURCE TO BINARY OPERATIONS

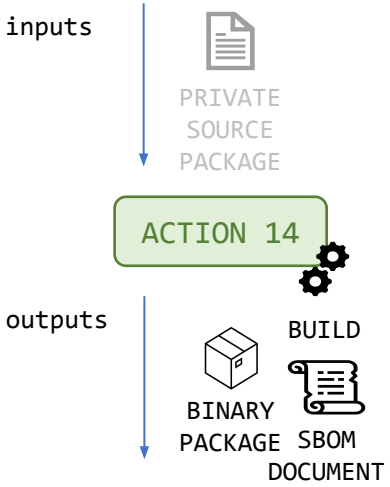


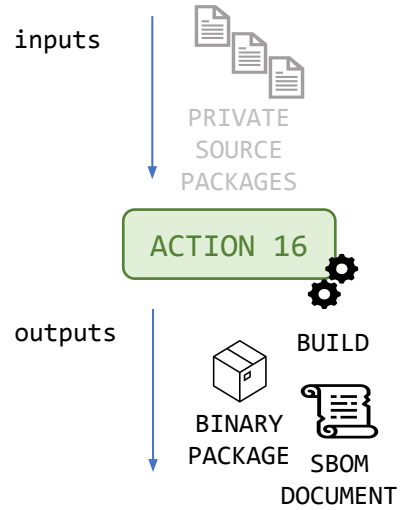


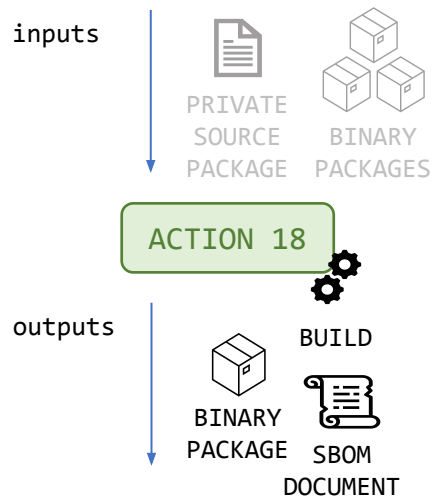


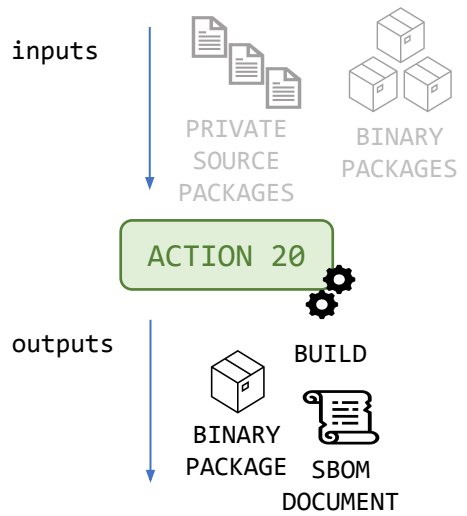




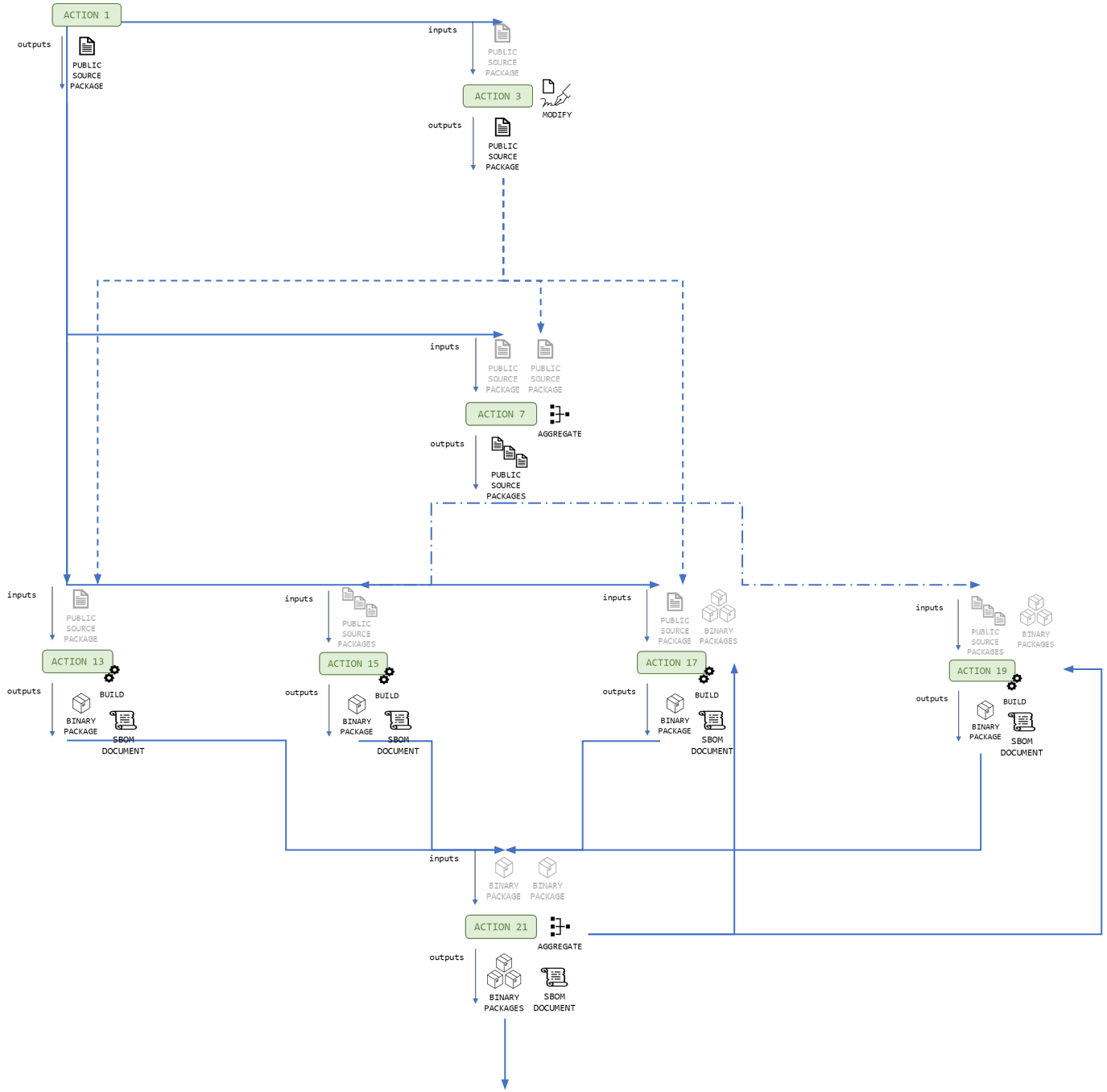




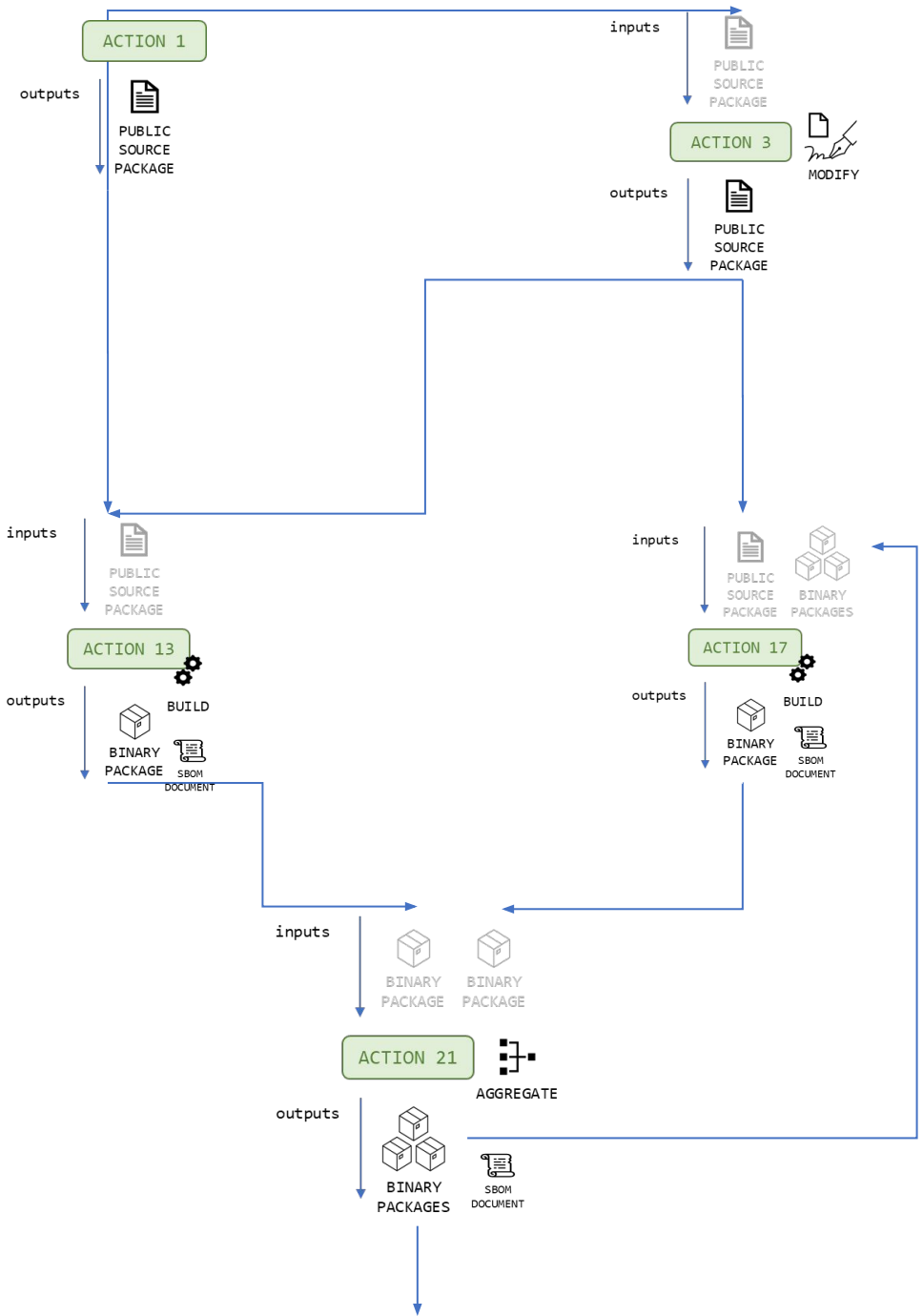




DEVELOP CHAIN FOR PUBLIC SOURCE PACKAGES



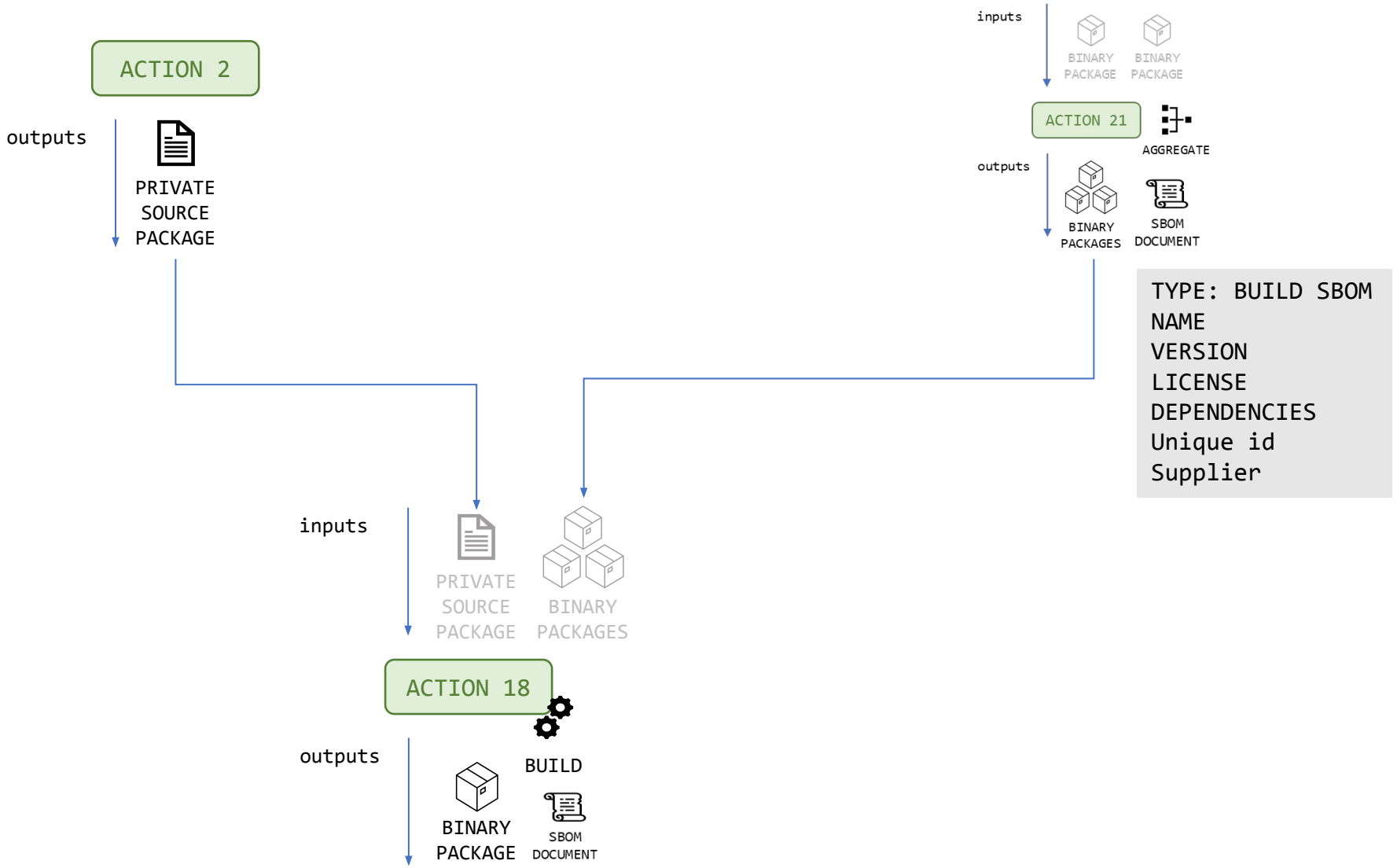
EXAMPLE
OSS PACKAGE DISTRIBUTOR



EXAMPLE

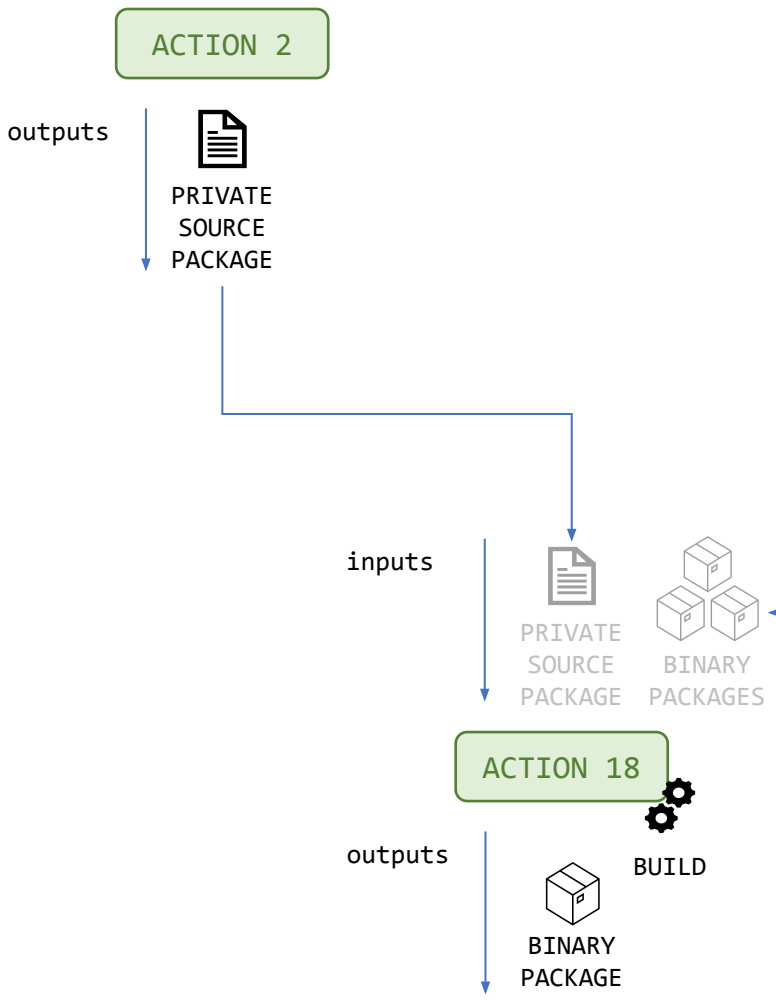
PROPRIETARY APP CREATOR

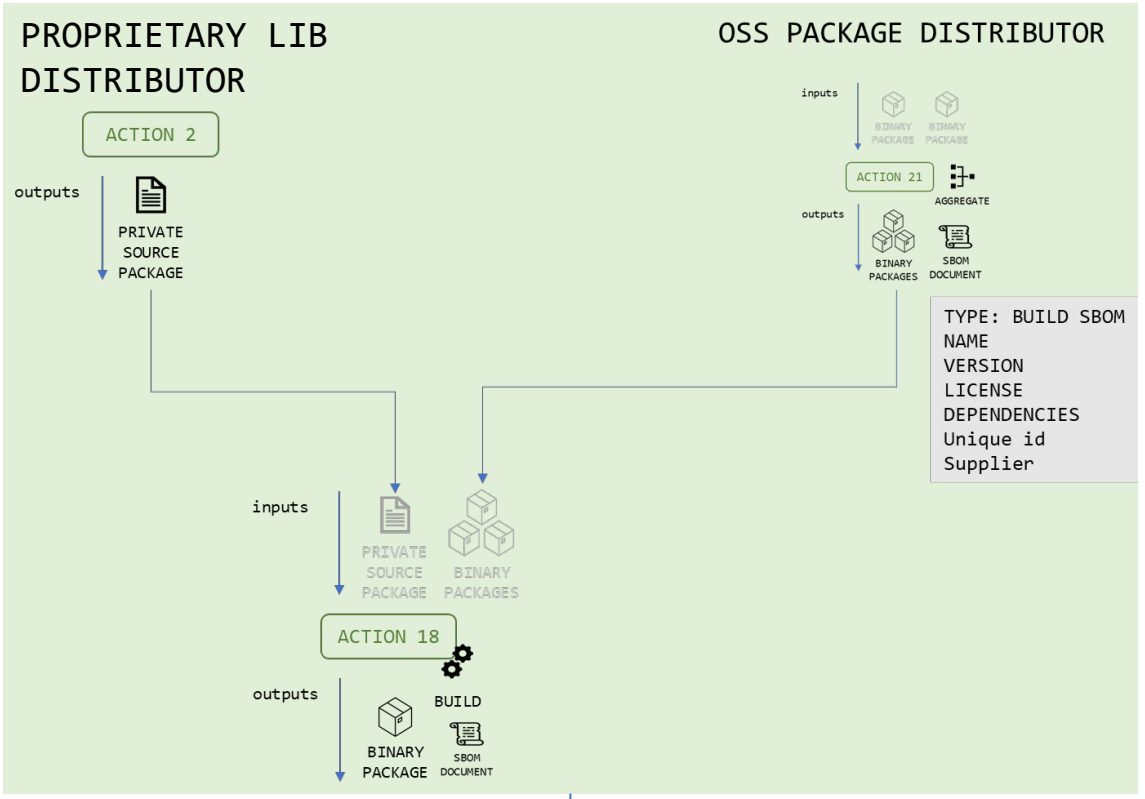
OSS PACKAGE DISTRIBUTOR



CATEGORY	CHALLENGE	SOLUTION IDEA
IDENTITY	Distributors use different names and versions in many cases, and making it difficult to identify the same package.	Use purl?

EXAMPLE
PROPRIETARY APP CREATOR





TYPE: BUILD SBOM
NAME
VERSION
LICENSE
DEPENDENCIES
Unique id
Supplier

... HOW ABOUT PRIVATE SOURCE PACKAGE INFORMATION?

CATEGORY	CHALLENGE	SOLUTION IDEA
IDENTITY	Distributors use different names and versions in many cases, and making it difficult to identify the same package.	Use purl?
DEFINITION	What should we fill the private package information in SBOM DOCUMENT? No third-party verifiable package name, version and no purl	

DISCUSS Challenges with GitHub Discussions

https://github.com/OpenChain-Project/SBOM-sg/discussions/categories/sbom-document-challenges

From the viewpoint of the SBOM DOCUMENT Quality,

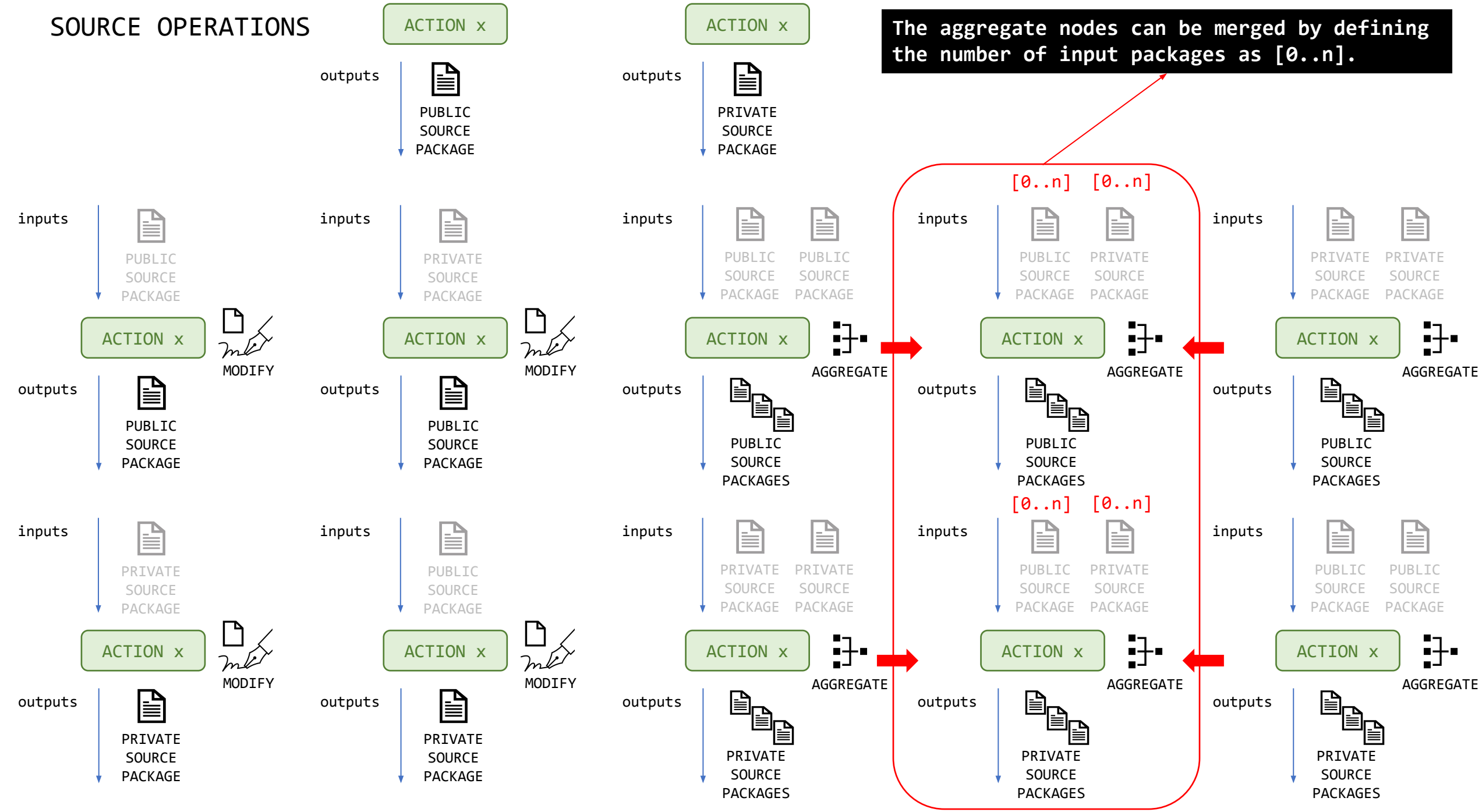
- ✔ Share your challenges in SBOM DOCUMENT Challenges Category.
- ✔ Rate the challenges if you have similar challenges.
- ✔ Share your solution idea in the thread.

Once resolved as a solution, define them as SBOM DOCUMENT quality indicators.

Consider Mergeable ACTIONs

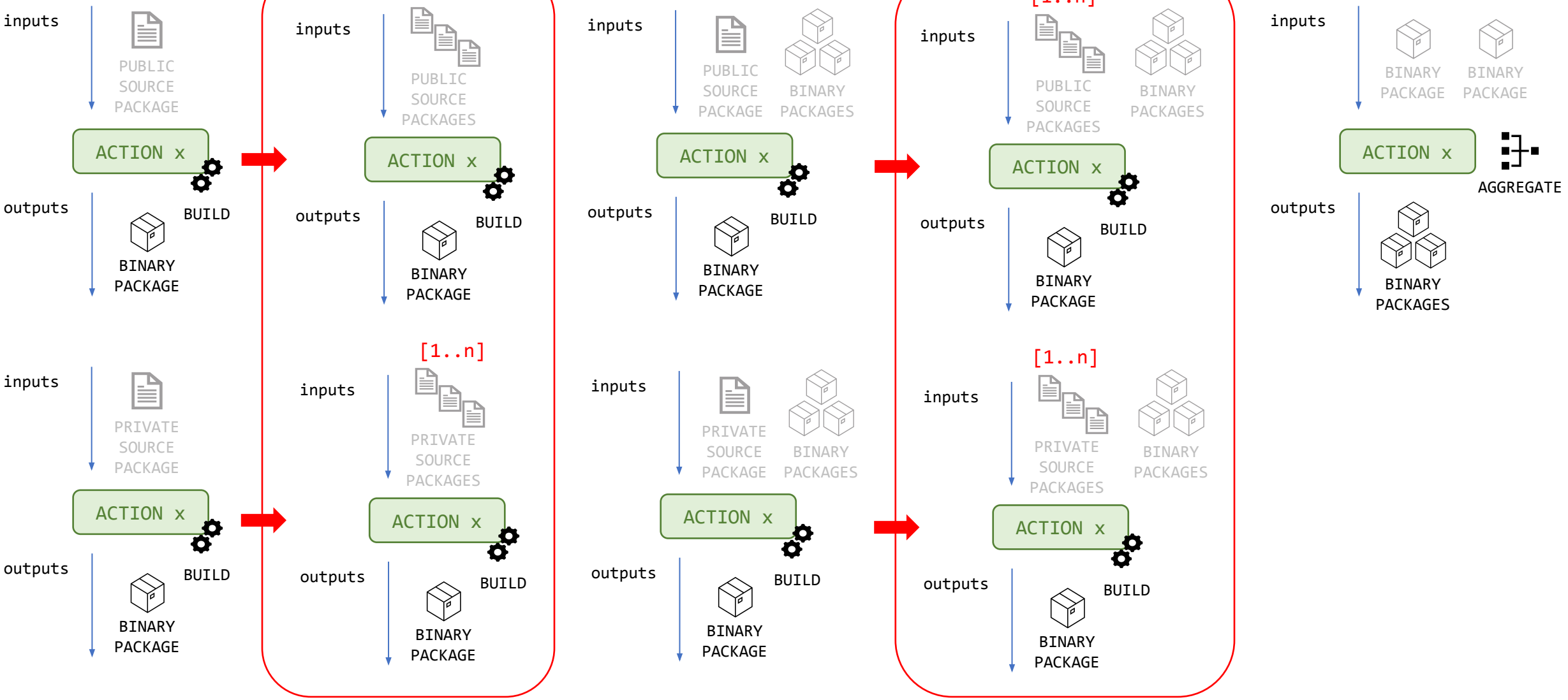
From the viewpoint of Vulnerabilities and License management

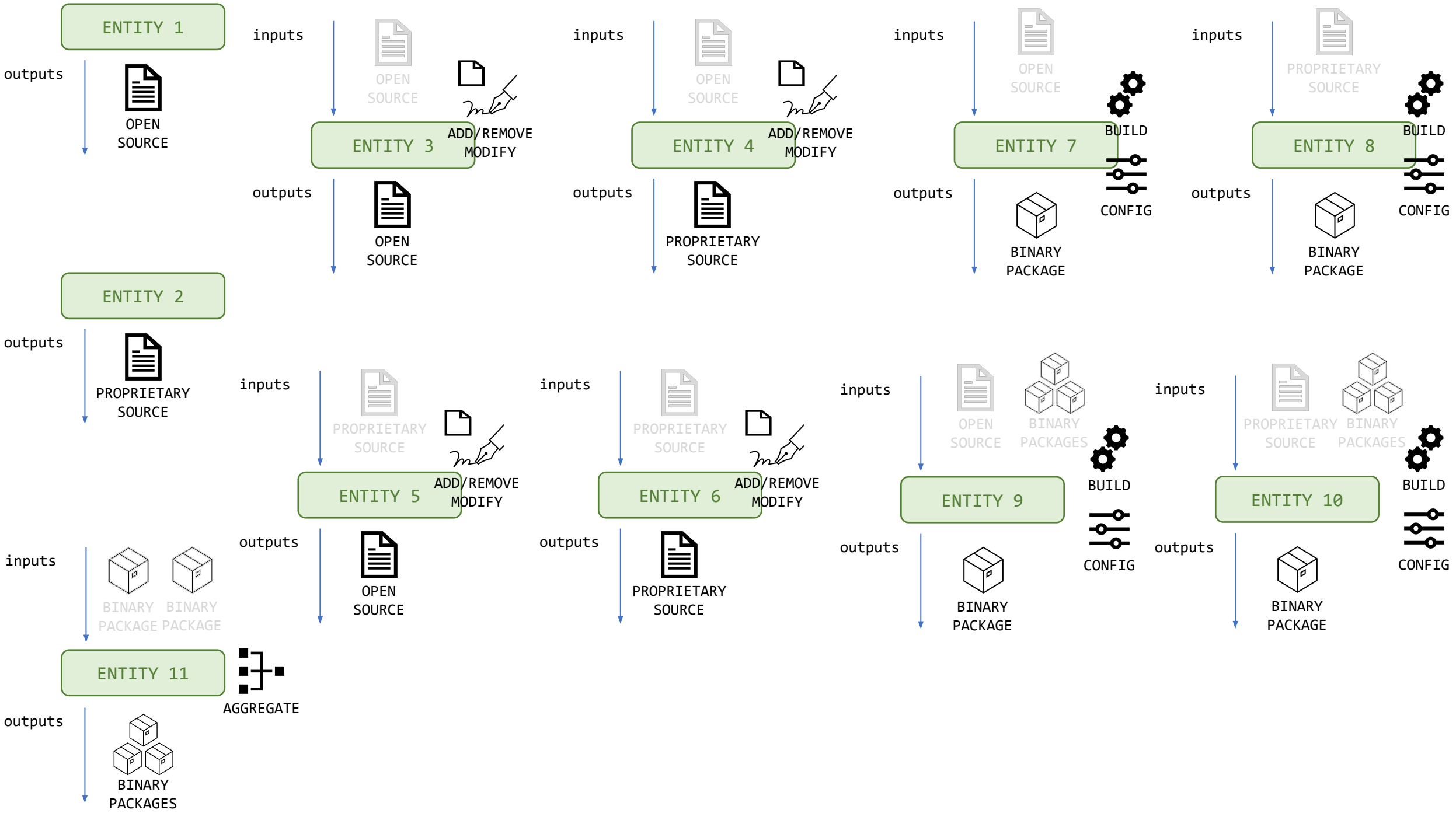
SOURCE OPERATIONS

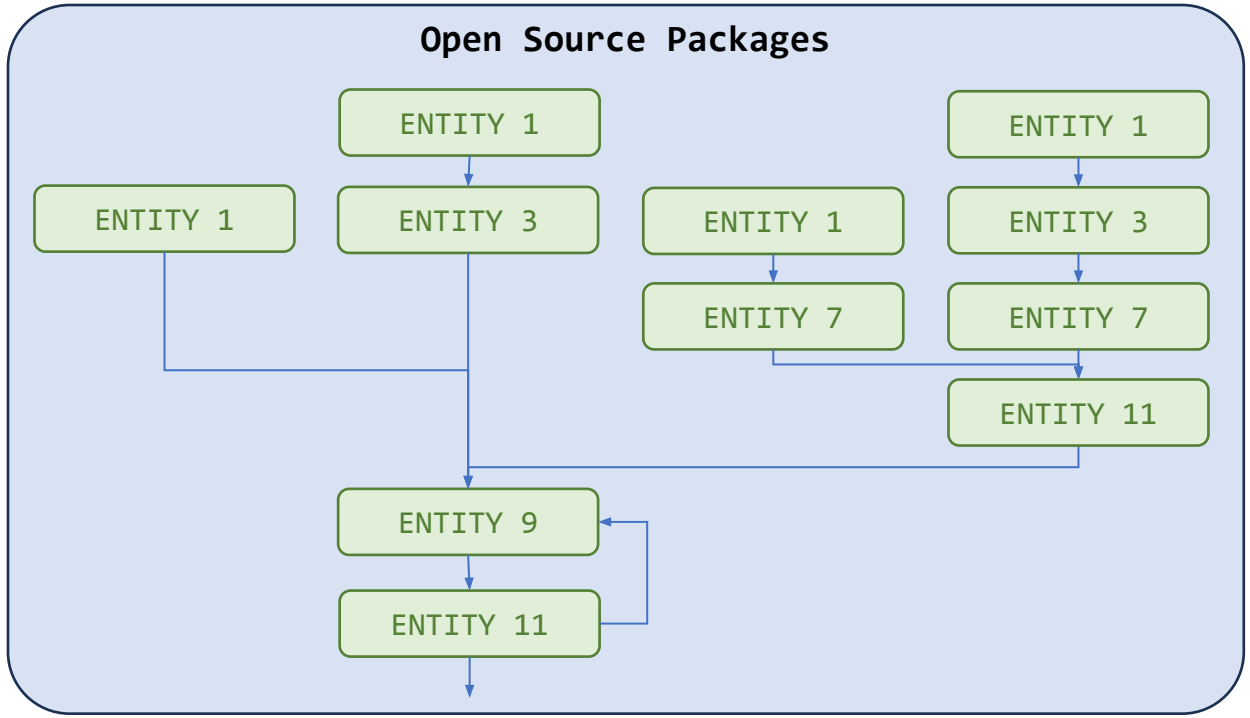


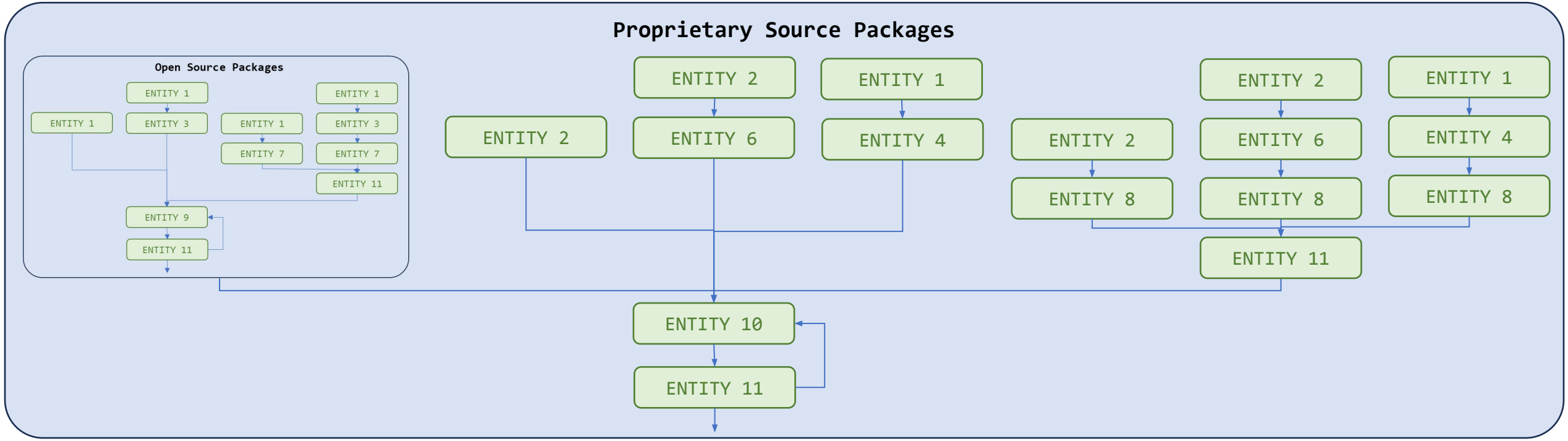
SOURCE TO BINARY OPERATIONS

The build nodes can be merged by defining the number of input packages as [1..n].




ENTITY 1
outputs
OPEN SOURCE
inputs
OPEN SOURCE
ADD/REMOVE MODIFY
ENTITY 3
outputs
OPEN SOURCE
inputs
OPEN SOURCE
ADD/REMOVE MODIFY
ENTITY 4
outputs
PROPRIETARY SOURCE
inputs
OPEN SOURCE
BUILD
ENTITY 7
CONFIG
outputs
BINARY PACKAGE
inputs
PROPRIETARY SOURCE
BUILD
ENTITY 8
CONFIG
outputs
BINARY PACKAGE
ENTITY 2
outputs
PROPRIETARY SOURCE
inputs
PROPRIETARY SOURCE
ADD/REMOVE MODIFY
ENTITY 5
outputs
OPEN SOURCE
inputs
PROPRIETARY SOURCE
ADD/REMOVE MODIFY
ENTITY 6
outputs
PROPRIETARY SOURCE
inputs
OPEN SOURCE
BINARY PACKAGES
BUILD
ENTITY 9
CONFIG
outputs
BINARY PACKAGE
inputs
PROPRIETARY SOURCE
BINARY PACKAGES
BUILD
ENTITY 10
CONFIG
outputs
BINARY PACKAGE
inputs
BINARY PACKAGE
BINARY PACKAGE
ENTITY 11
AGGREGATE
outputs
BINARY PACKAGES

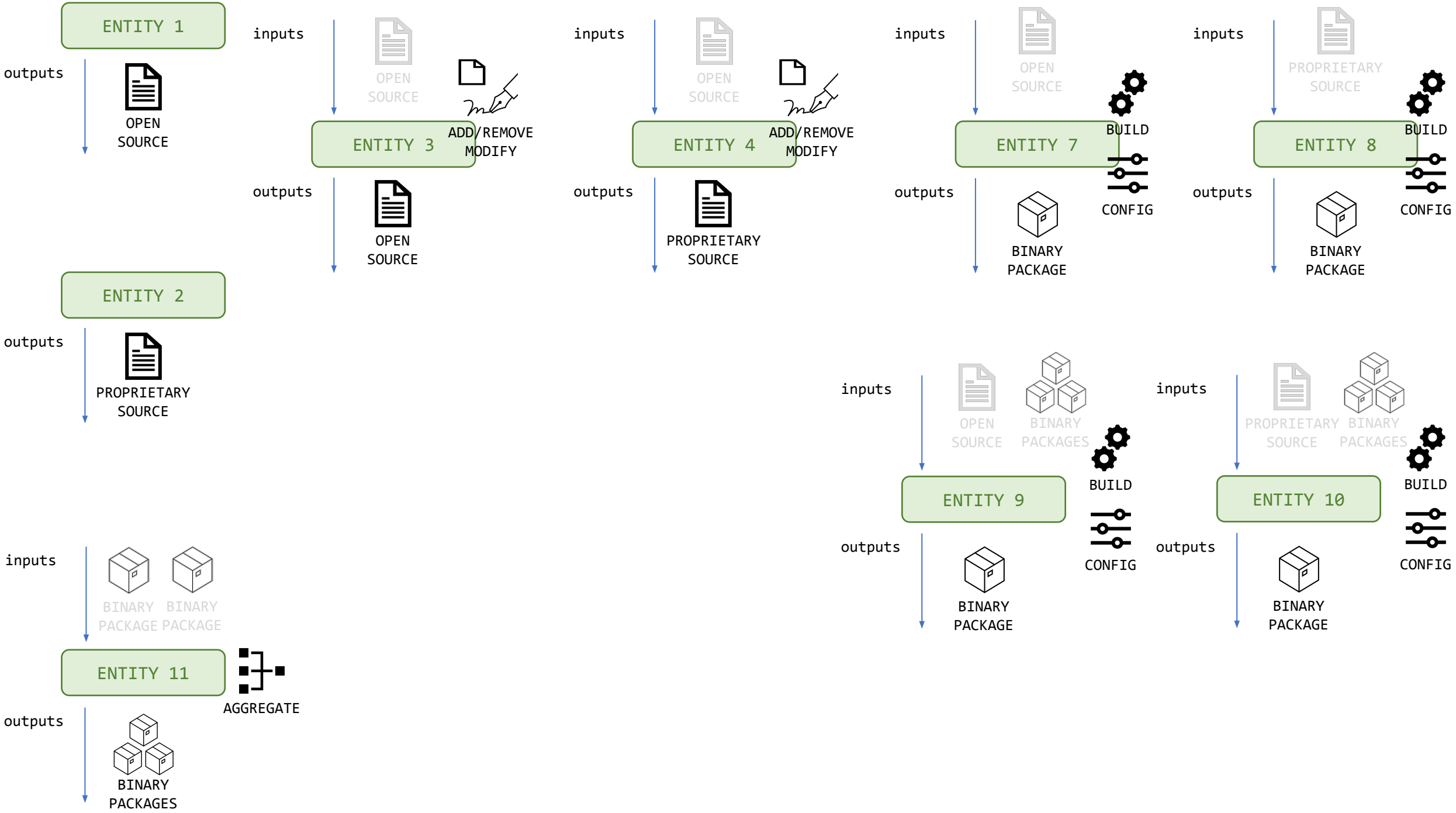

Open Source Packages
ENTITY 1
ENTITY 1
ENTITY 1
ENTITY 1
ENTITY 3
ENTITY 1
ENTITY 3
ENTITY 7
ENTITY 7
ENTITY 11
ENTITY 9
ENTITY 11

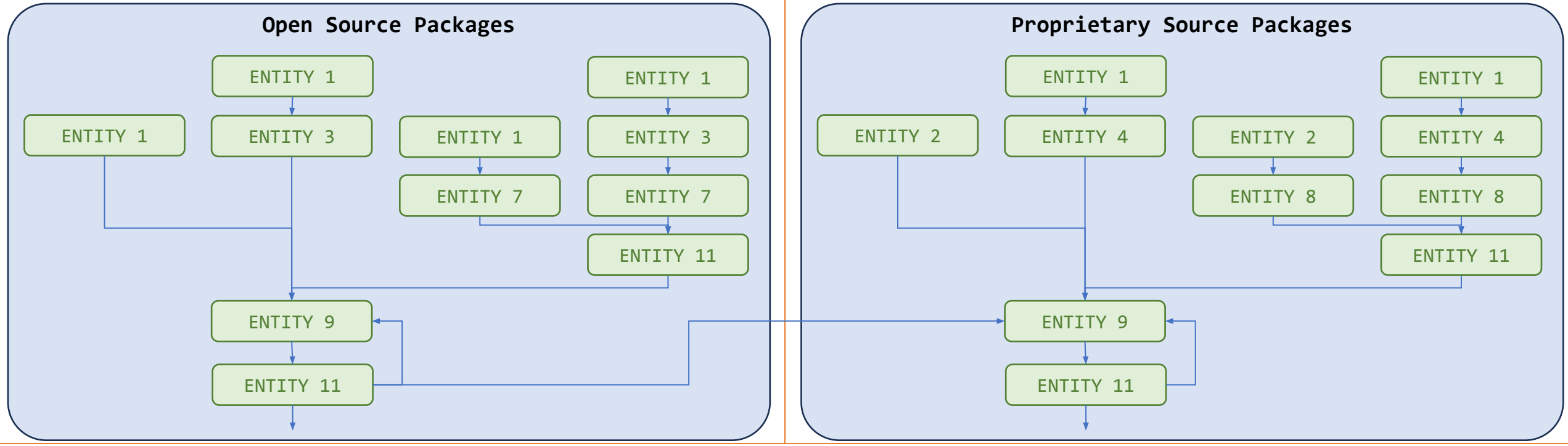

Proprietary Source Packages
Open Source Packages
ENTITY 1
ENTITY 1
ENTITY 3
ENTITY 1
ENTITY 1
ENTITY 3
ENTITY 7
ENTITY 7
ENTITY 11
ENTITY 9
ENTITY 11
ENTITY 2
ENTITY 1
ENTITY 2
ENTITY 6
ENTITY 4
ENTITY 2
ENTITY 2
ENTITY 1
ENTITY 8
ENTITY 6
ENTITY 4
ENTITY 8
ENTITY 8
ENTITY 11
ENTITY 10
ENTITY 11

Simplify

In terms of whether the “SOURCE” has a globally unique ID such as purl.

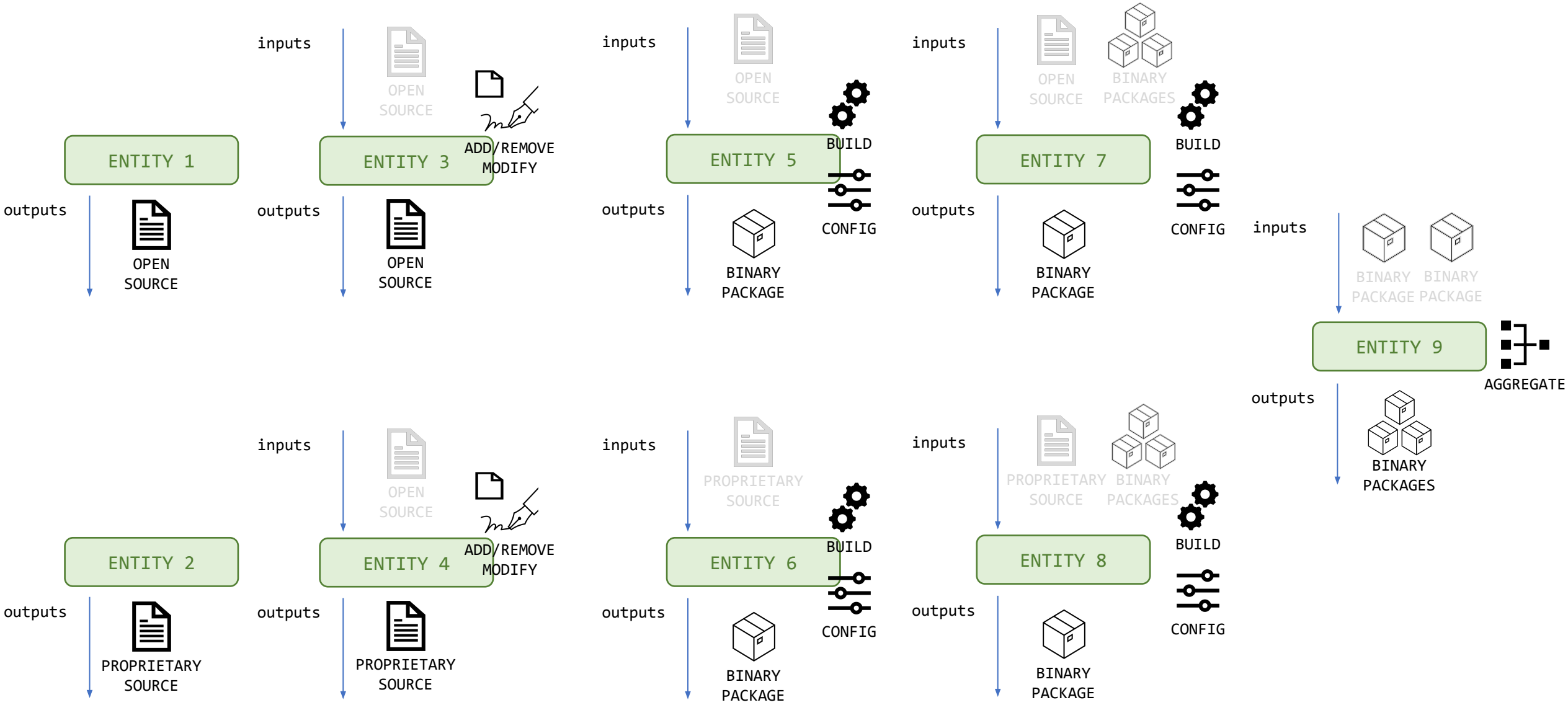
- ENTITY 5 is equivalent to ENTITY 1 or ENTITY 3.
- ENTITY 6 is equivalent to ENTITY 2 or ENTITY 4.


ENTITY 1
outputs
OPEN SOURCE
inputs
OPEN SOURCE
ADD/REMOVE MODIFY
ENTITY 3
outputs
OPEN SOURCE
inputs
OPEN SOURCE
ADD/REMOVE MODIFY
ENTITY 4
outputs
PROPRIETARY SOURCE
inputs
OPEN SOURCE
BUILD
ENTITY 7
CONFIG
outputs
BINARY PACKAGE
inputs
PROPRIETARY SOURCE
BUILD
ENTITY 8
CONFIG
outputs
BINARY PACKAGE
ENTITY 2
outputs
PROPRIETARY SOURCE
inputs
OPEN SOURCE
BINARY PACKAGES
BUILD
ENTITY 9
CONFIG
outputs
BINARY PACKAGE
inputs
PROPRIETARY SOURCE
BINARY PACKAGES
BUILD
ENTITY 10
CONFIG
outputs
BINARY PACKAGE
inputs
BINARY PACKAGE
BINARY PACKAGE
ENTITY 11
AGGREGATE
outputs
BINARY PACKAGES

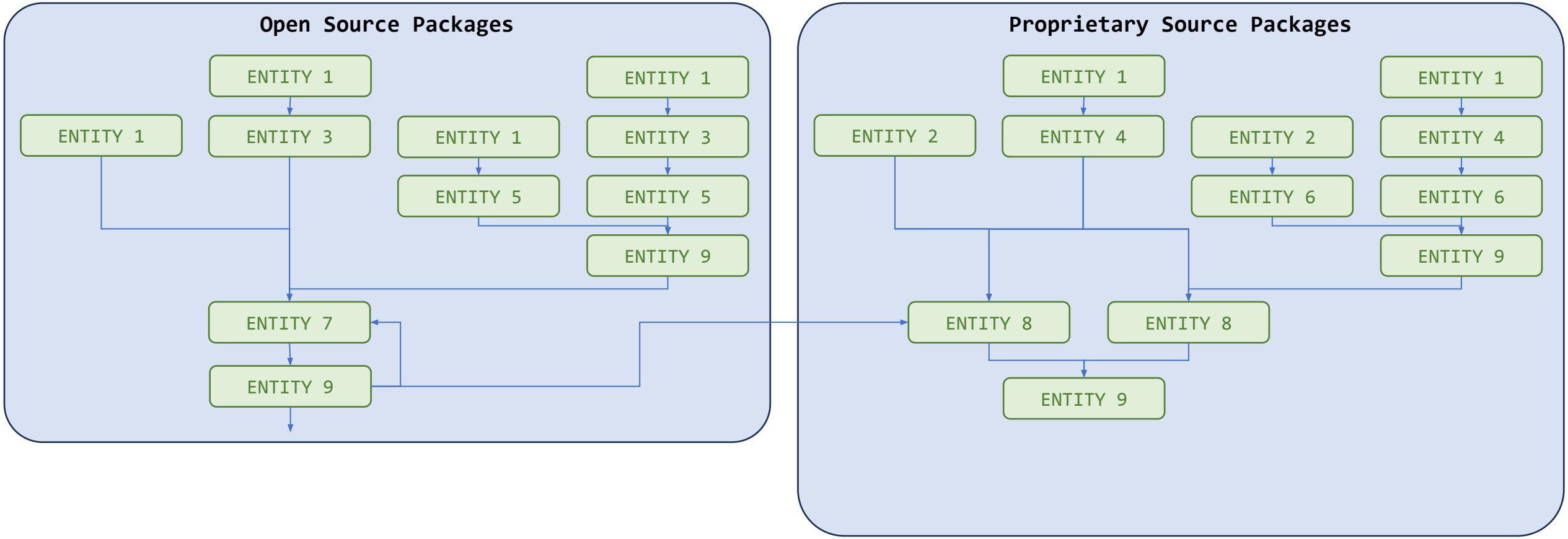

Open Source Packages
ENTITY 1
ENTITY 1
ENTITY 1
ENTITY 1
ENTITY 3
ENTITY 3
ENTITY 7
ENTITY 7
ENTITY 11
ENTITY 9
ENTITY 11
Proprietary Source Packages
ENTITY 1
ENTITY 1
ENTITY 2
ENTITY 4
ENTITY 2
ENTITY 4
ENTITY 8
ENTITY 8
ENTITY 11
ENTITY 9
ENTITY 11

Re-numbering

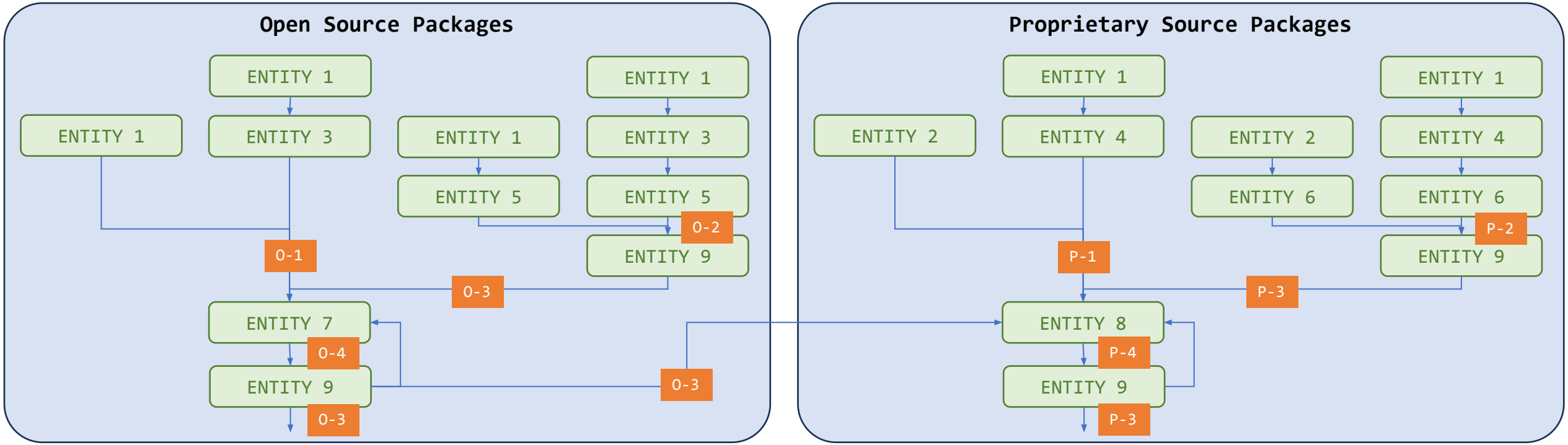
QUESTION:
Does this extract all the necessary entities for software development?



※ Here, “PROPRIETARY SOURCE” means source code that cannot be represented by the globally unique ID such as purl in SBOMs.

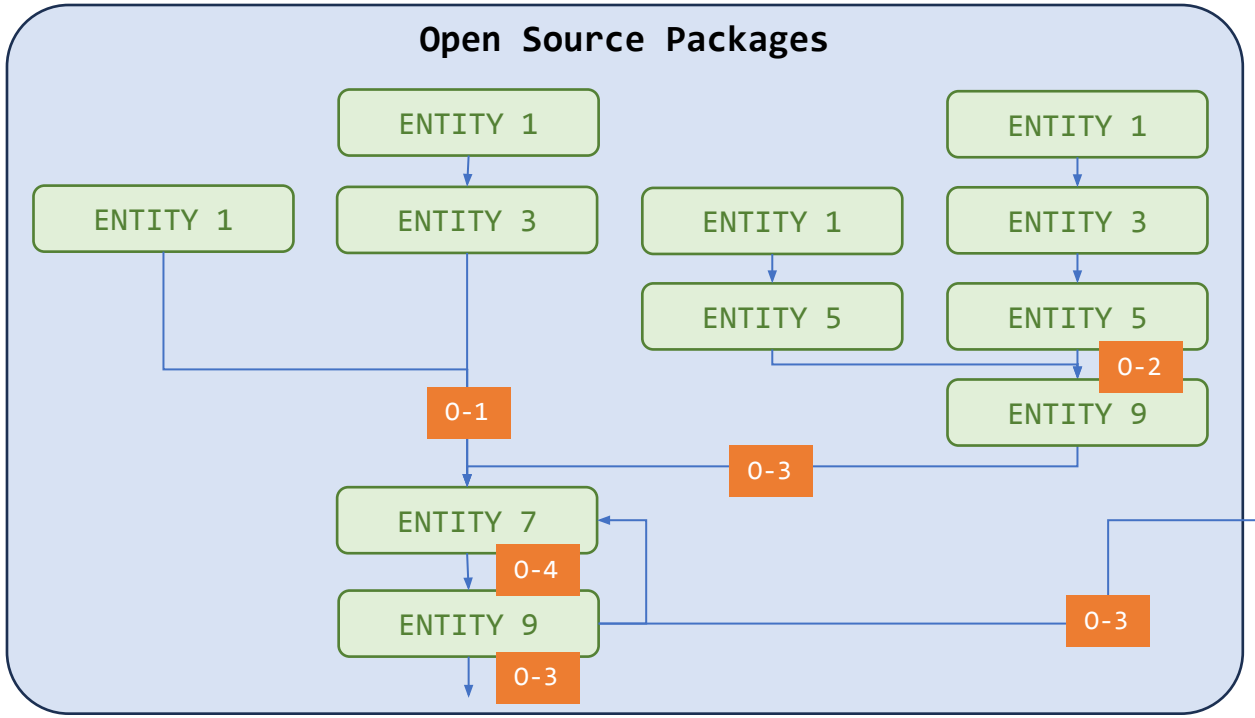


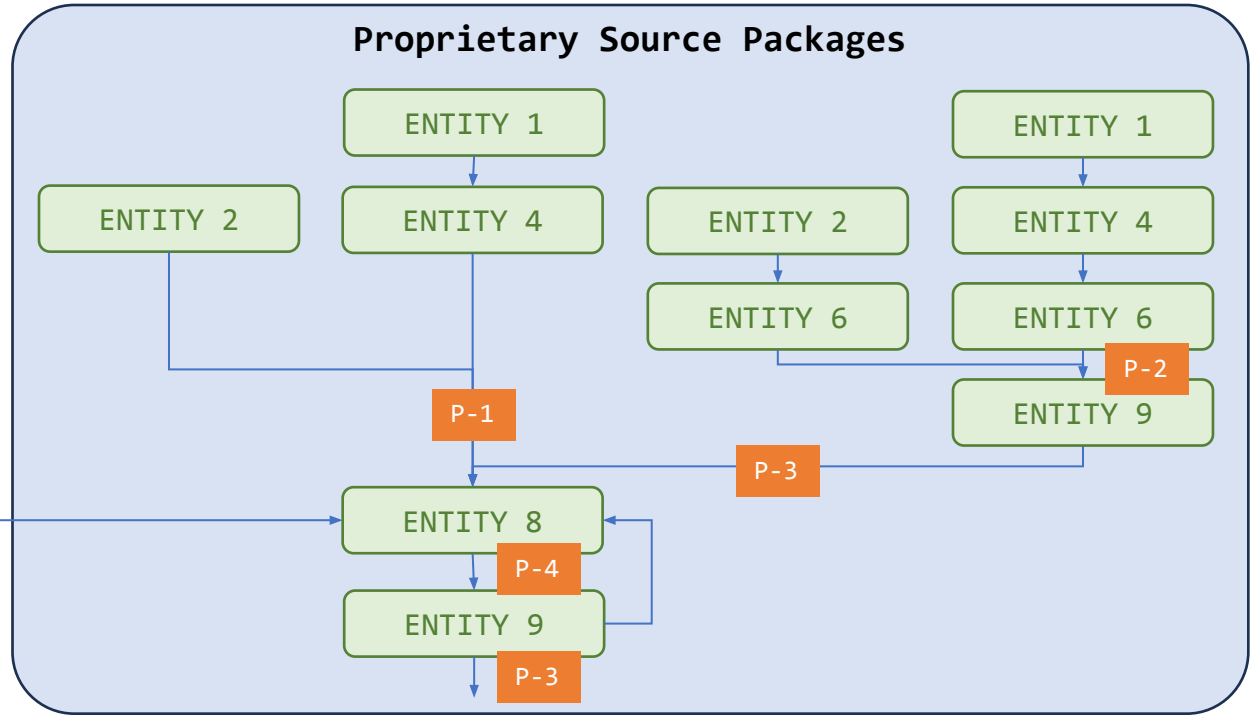
QUESTION:
Does this flow chart represent the entire software development and supply chain for the software development?



O-1 - O-4 , P-1 - P-4 Points at which SBOMs are distributed.

QUESTION:
Is there any other points where SBOMs may be distributed?



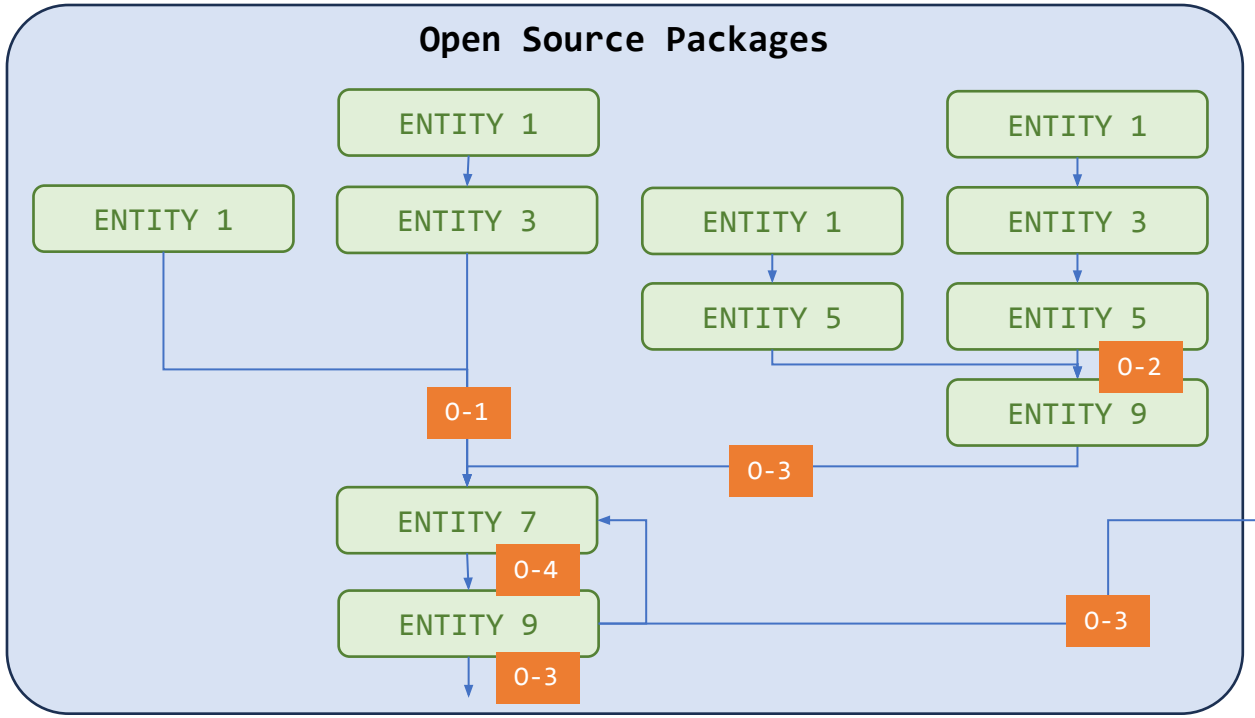


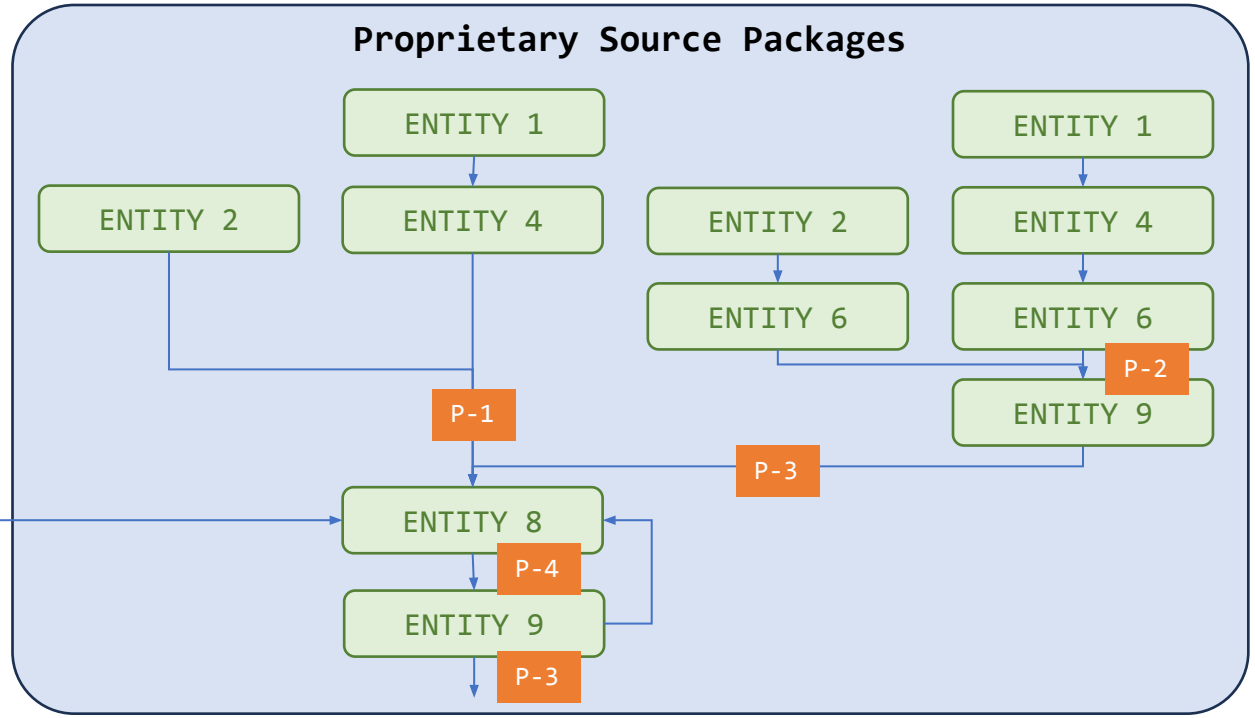
O-1 - O-4 , P-1 - P-4 Points at which SBOMs are distributed.

For ENTITY 1, 3 at O-1:
- What information can be provided?
- What type of SBOMs can be provided?
- When can the SBOMs be provided?
- What should ENTITY 1 and 3 do to do the above?

ENTITY 5, 7 ask ENTITY 1, 3 at O-1:
- What information will be needed?
- What type of SBOMs is ideal?
- When do they want the SBOMs to be provided?
- What should ENTITY 5 and 7 do to do the above?

Question:
Are there any other items required for each point, for each entity other than the question on the left?





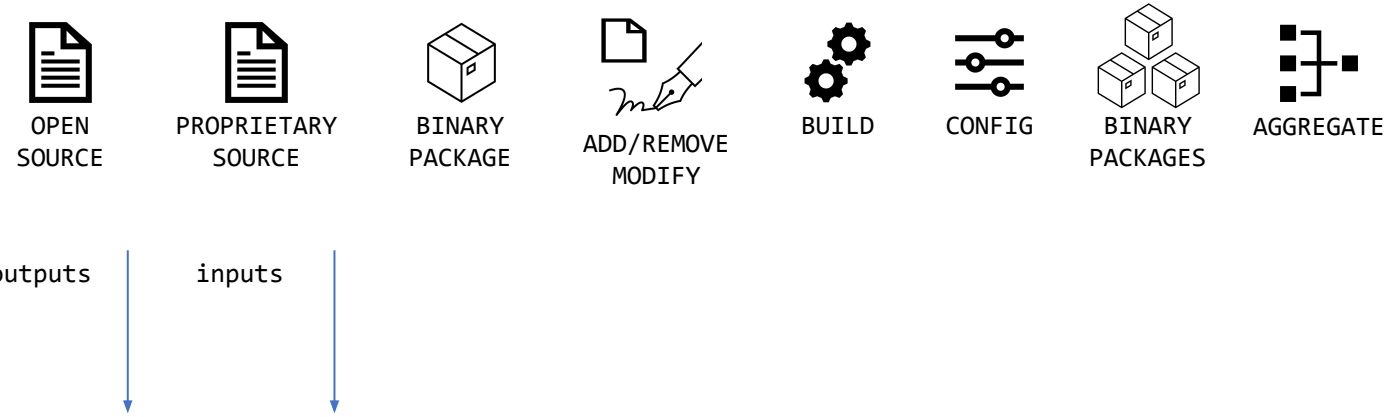
O-1 - O-4 , P-1 - P-4 Points at which SBOMs are distributed.

For ENTITY 1, 3 at O-1:
- What information can be provided?
- What type of SBOMs can be provided?
- When can the SBOMs be provided?
- What should ENTITY 1 and 3 do to do the above?

ENTITY 5, 7 ask ENTITY 1, 3 at O-1:
- What information will be needed?
- What type of SBOMs is ideal?
- When do they want the SBOMs to be provided?
- What should ENTITY 5 and 7 do to do the above?

TASK:
At each point, at each entity, please summarize the same information as the question on the left.

ACTION x


OPEN SOURCE
PROPRIETARY SOURCE
BINARY PACKAGE
ADD/REMOVE MODIFY
BUILD
CONFIG
BINARY PACKAGES
AGGREGATE
outputs
inputs