



Learning Lab: Chainguard Libraries for Python

Patrick Smyth

Queens, New York

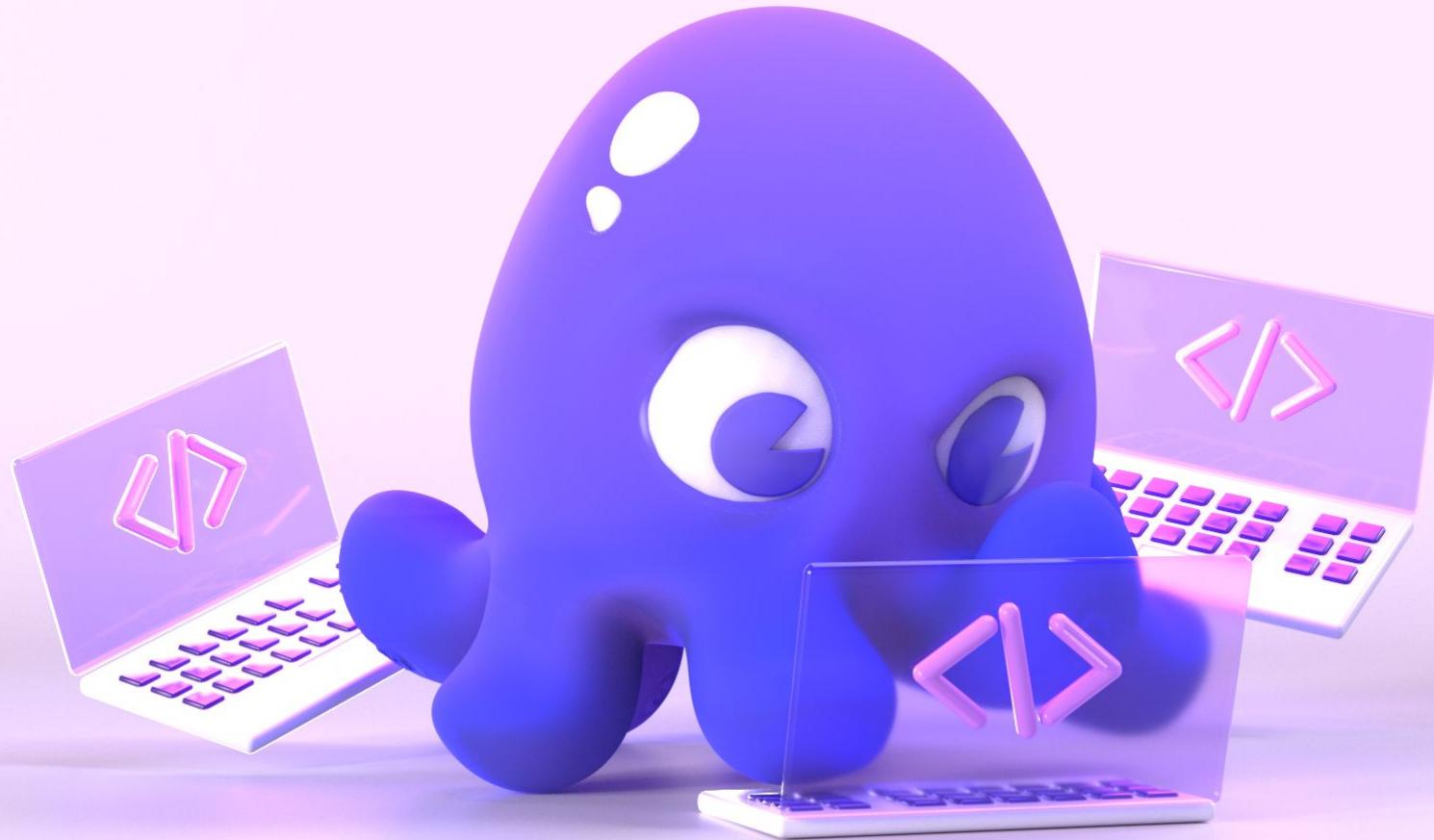
Staff DevRel at Chainguard

Python, Data Science at
James Webb, Columbia

patrick.smyth@chainguard.dev

@psmyth01 on X





Safe Source for Open Source

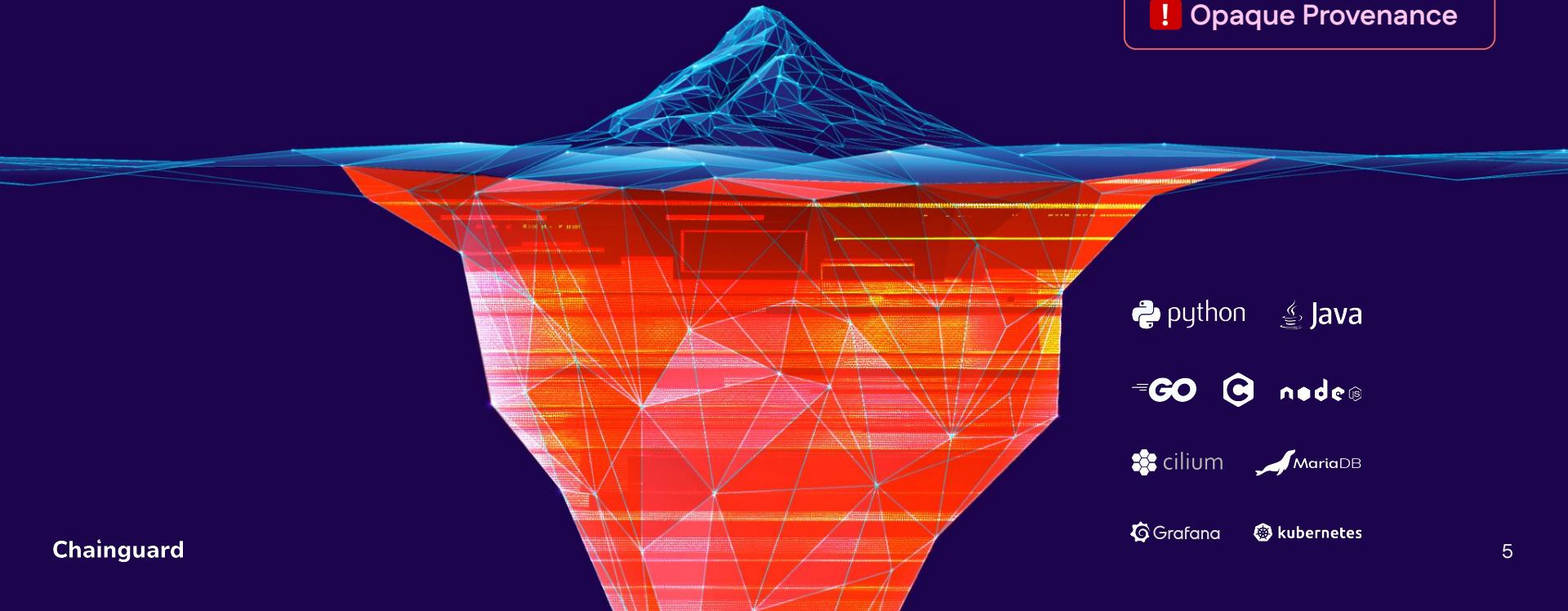
<p>Software</p> <p> </p>	<p>Health & Bio</p> <p> </p>	<p>Security</p> <p> </p>	<p>FinServ</p> <p> </p>
<p>Public Sector</p> <p> </p>	<p>Defense / Safety</p> <p> Booz Allen Hamilton </p>	<p>AI</p> <p> </p>	<p>F500</p> <p> </p>

Chainguard Containers

! Persistent CVEs

! Large Attack Surface

! Opaque Provenance



Chainguard Containers

2%
Source Code



98%
Open Source

Chainguard

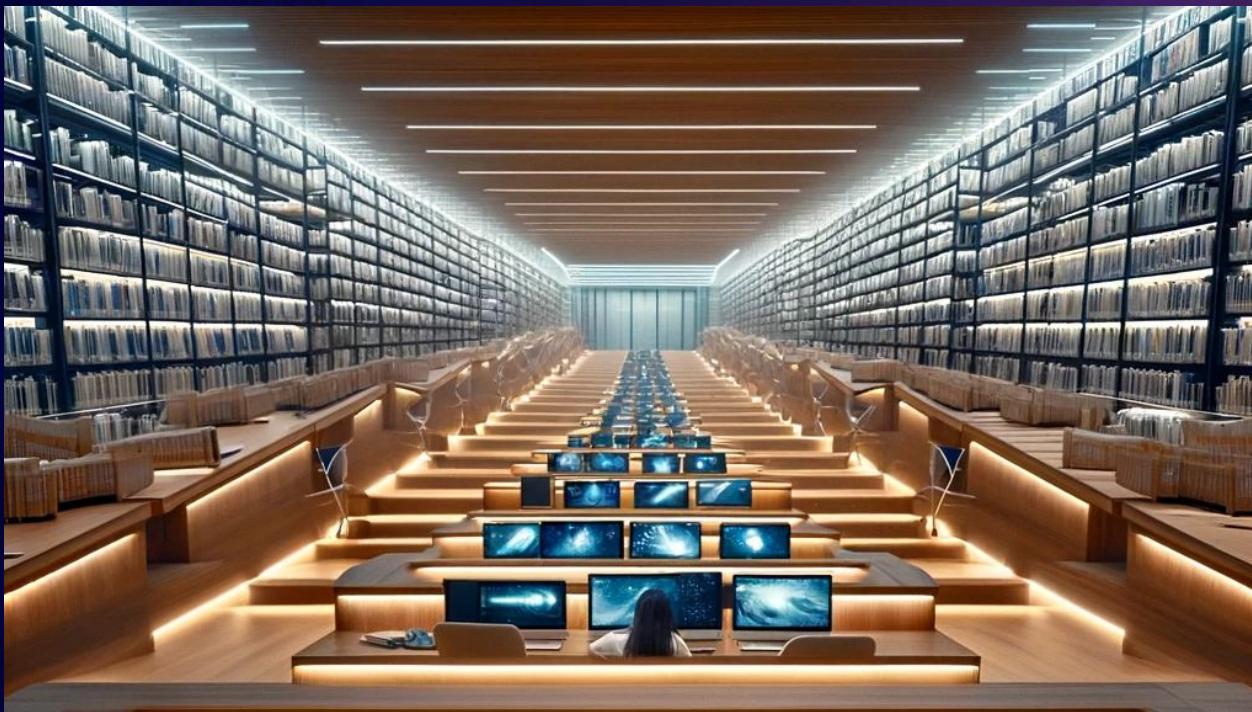
python Java

GO C node.js

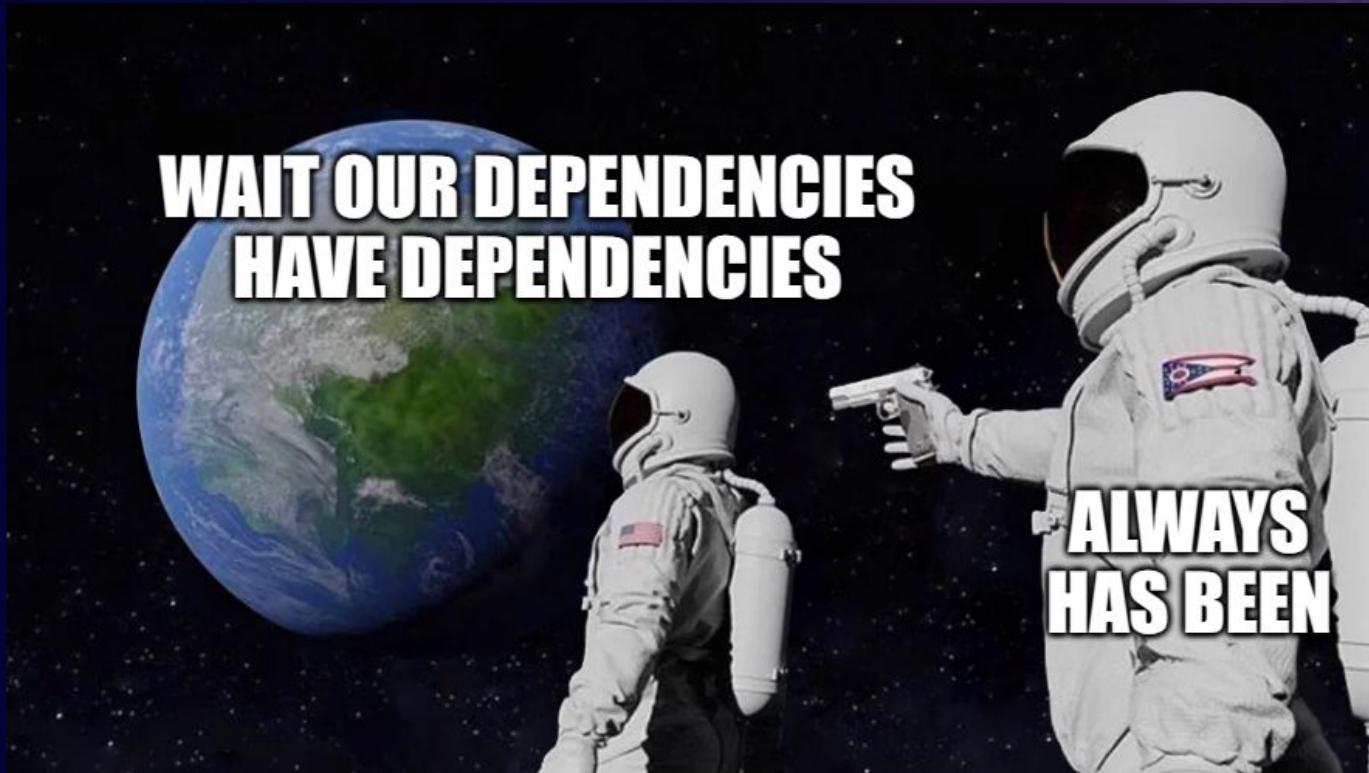
cilium MariaDB

Grafana kubernetes

What's a Library?



Transitive Dependencies



What is PyPI?



PyPI / Warehouse



- 634,879 projects
- 1,580,910,735 daily downloads
- 27.4 TB
- Checked 5/12/25

We Got a Problem



Attack Every Month

2025

JANUARY 	FEBRUARY 	MARCH 	APRIL 
MAY 	JUNE 	JULY	AUGUST

Software Supply Chain Speedrun

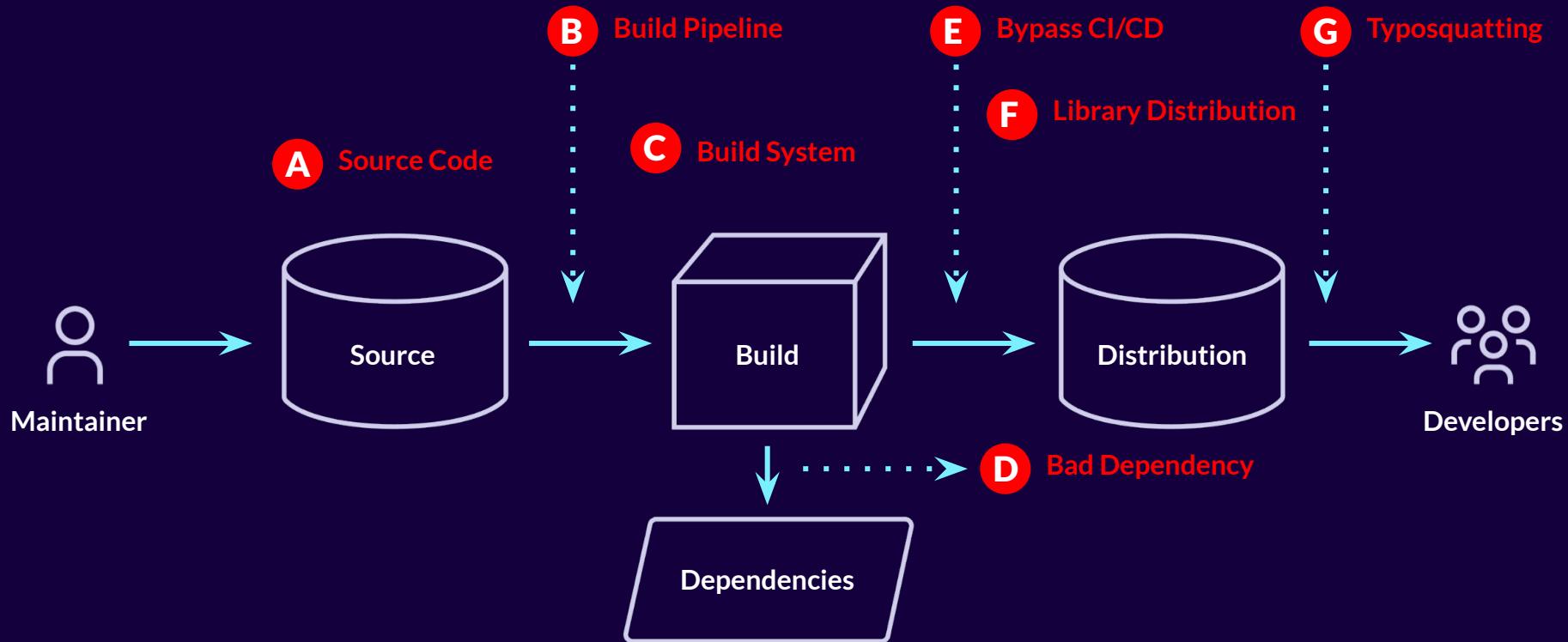
- Raw materials to finished product
- Complex network
- Many actors, many steps



Stuff Flows Downhill



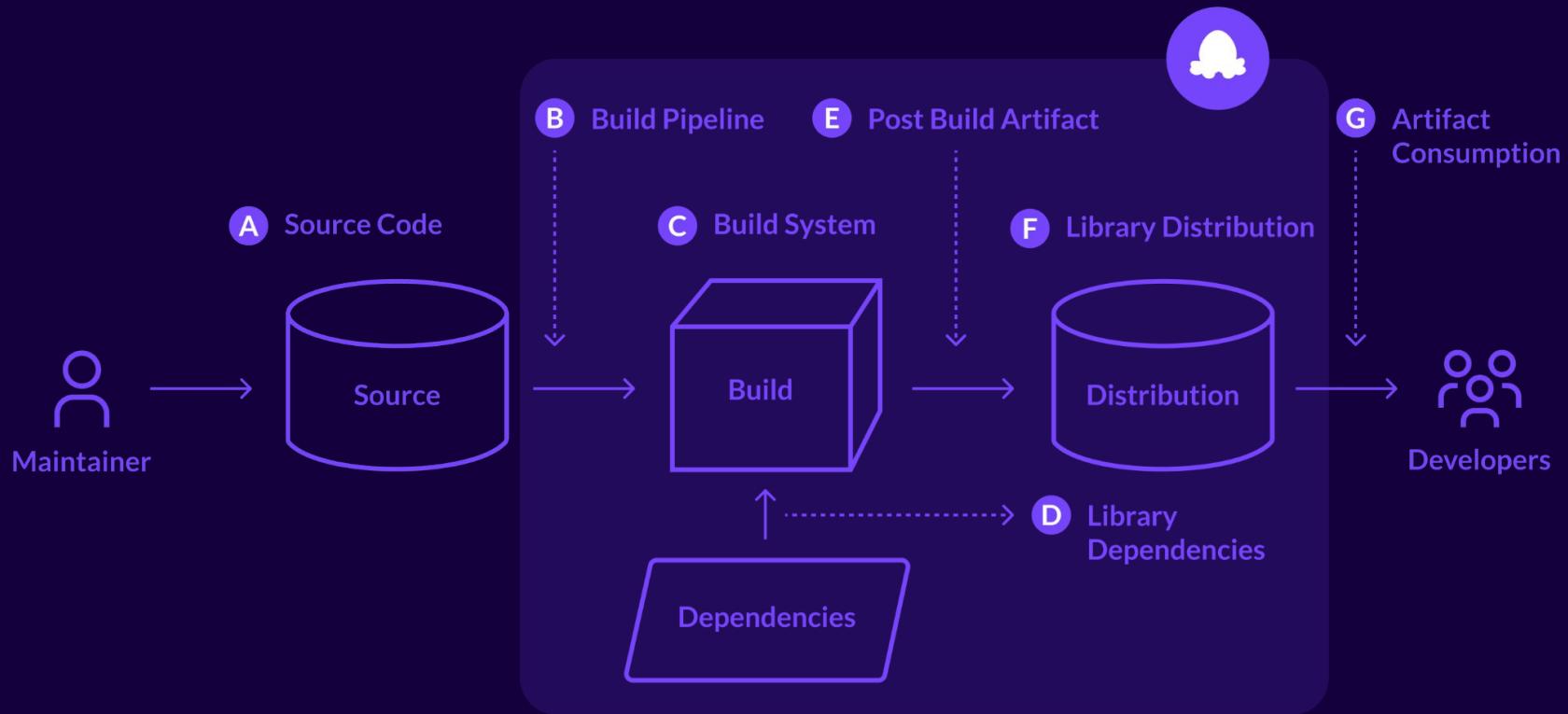
Points of Failure



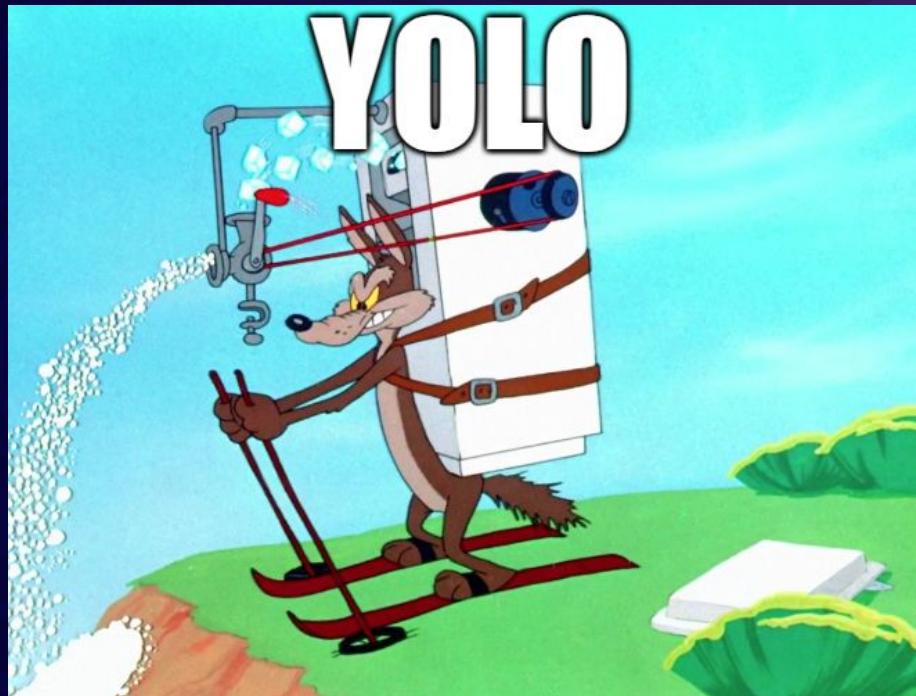
Chainguard Libraries



Source > Chainguard Factory > You



Ultralytics YOLO Attack



Chainguard Factory



Chainguard Factory

- What is it?
- Fitting into the supply chain landscape
- Python ecosystem and Dark Matter



DE MO

Chainguard Libraries



chainguard.dev/libraries



A close-up photograph of a bright orange fish, possibly a damselfish or wrasse, swimming away from a light-colored, textured rock surface. The fish is angled upwards and to the right, with its body curved. Its fins are slightly spread, and it appears to be moving quickly. The background is blurred, emphasizing the fish.

Goodbye!