Risk Management for the Software Supply Chain

Why the Future will be Federated

Brent Toderash

Who?

b2 user. *(Did I miss anything?)*

• Blogger • Freelancer • Entrepreneur • ISP Owner • Web Host • Agency Owner •
• Web Developer • Project Manager • Open Source Advocate • Writer •

• Iconoclast • Tester of Assumptions • Freelance Thinker •

Linux™   ¡PENGUINISTA!

100 PERCENT WEBHOST.CA

MODERN EARTH

yawp.foo

aspire PRESS

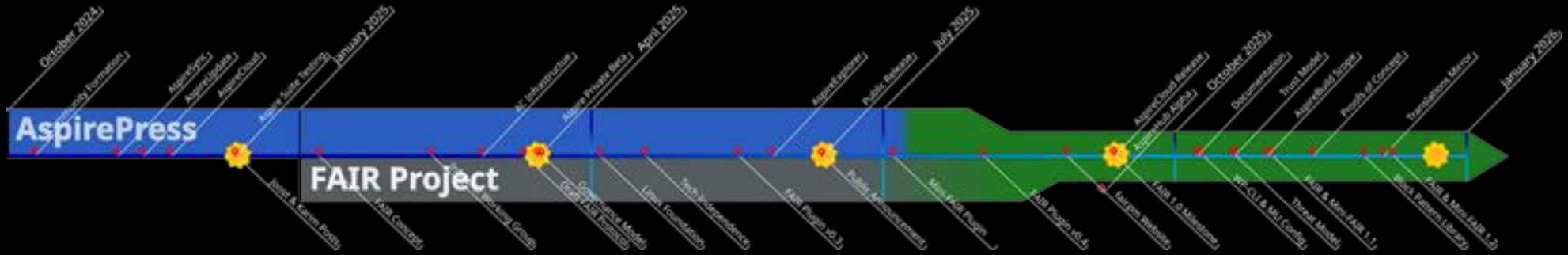
FAIR

I don't always write code, but when I do...

WCEH 2025 CANADA

Brent Toderash

Why I spent the past 12 months working to decentralize WordPress software distribution.



Risk Management Primer

- Pre-Y2K, I held a professional designation in the general insurance industry.
- Risk management principles are transferable.
- The first step in managing risk is identifying it.

Photo by Bernd Dittrich on Unsplash

A Risk Management Primer

Risk Assessment Includes *Measuring* Risk

Photo by capt.sopon on Pexels.com

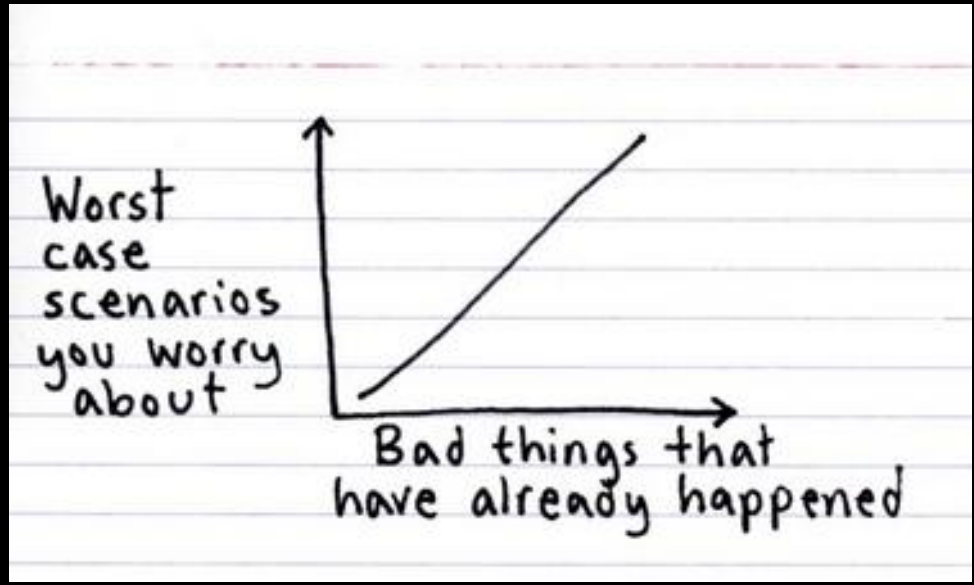
Frequency (Probability)	Severity (Impact)

"What's the Worst that Could Happen?"

Good question for risk managers

Followed by,

"What can we DO about it?"



Source: Jessica Hagy, "Rough habit to have." *Indexed*, thisisindexed.com/2023/06/rough-habit-to-have/

Managing risk starts with mitigation strategies to reduce both the *probability* and *impact* of "Bad Things".

Risk Mitigation

1. Make someone else responsible.

2. **Reduce risk to an acceptable level** by reducing probability, impact, or both.

- Transfer of Risk
  - Insurance
  - Other Contracts
- Reduce Probability
  - Prevention

- Reduce Impact
  - Recovery Plan
  - Spread of Risk

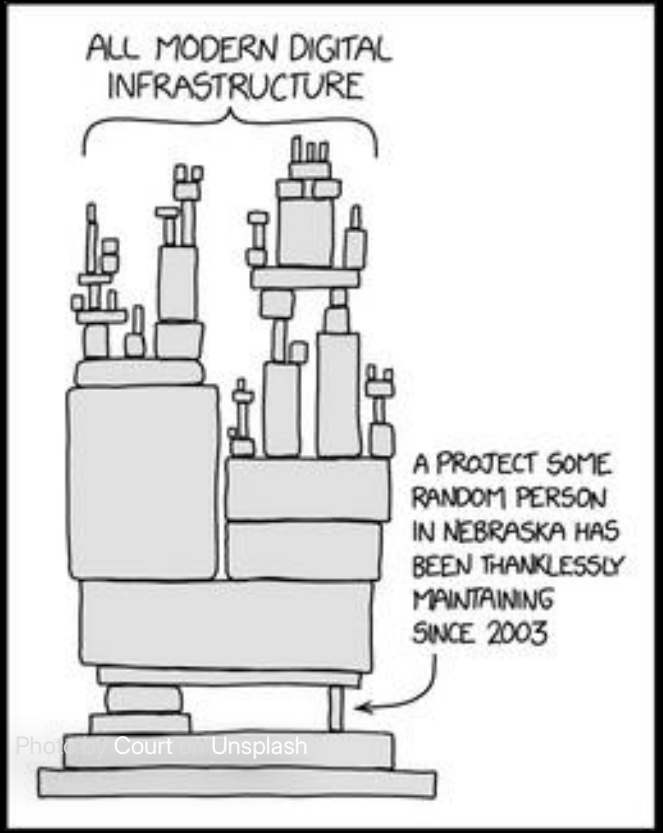
You already understand spread of risk.

- Your mother explained this.
- IT: Single Point of Failure (SPOF)
- Supply Chain: Single-Vendor Risk

Photo by Court on Unsplash

You already understand spread of risk.

- Your mother explained this.
- IT: Single Point of Failure (SPOF)
- Supply Chain: Single-Vendor Risk
- xkcd calls it “Dependency”



Source: xkcd: “Dependency” – xkcd.com/2347

Managing Supply Chain Risk

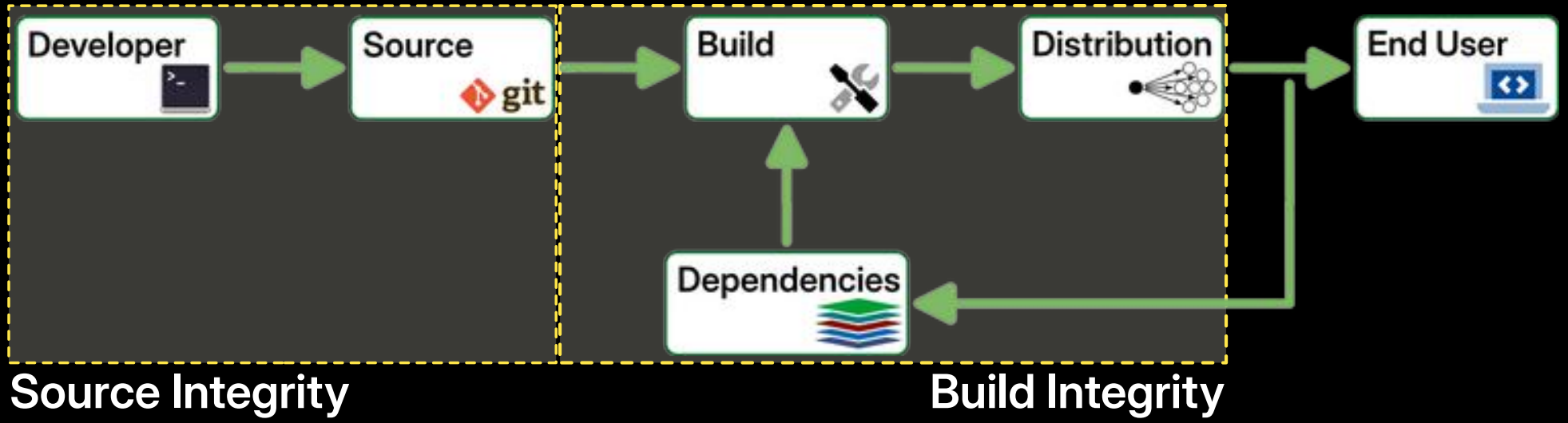
If you're not mitigating risk,
you're not managing it —
you're just accepting it.

Software Supply Chains

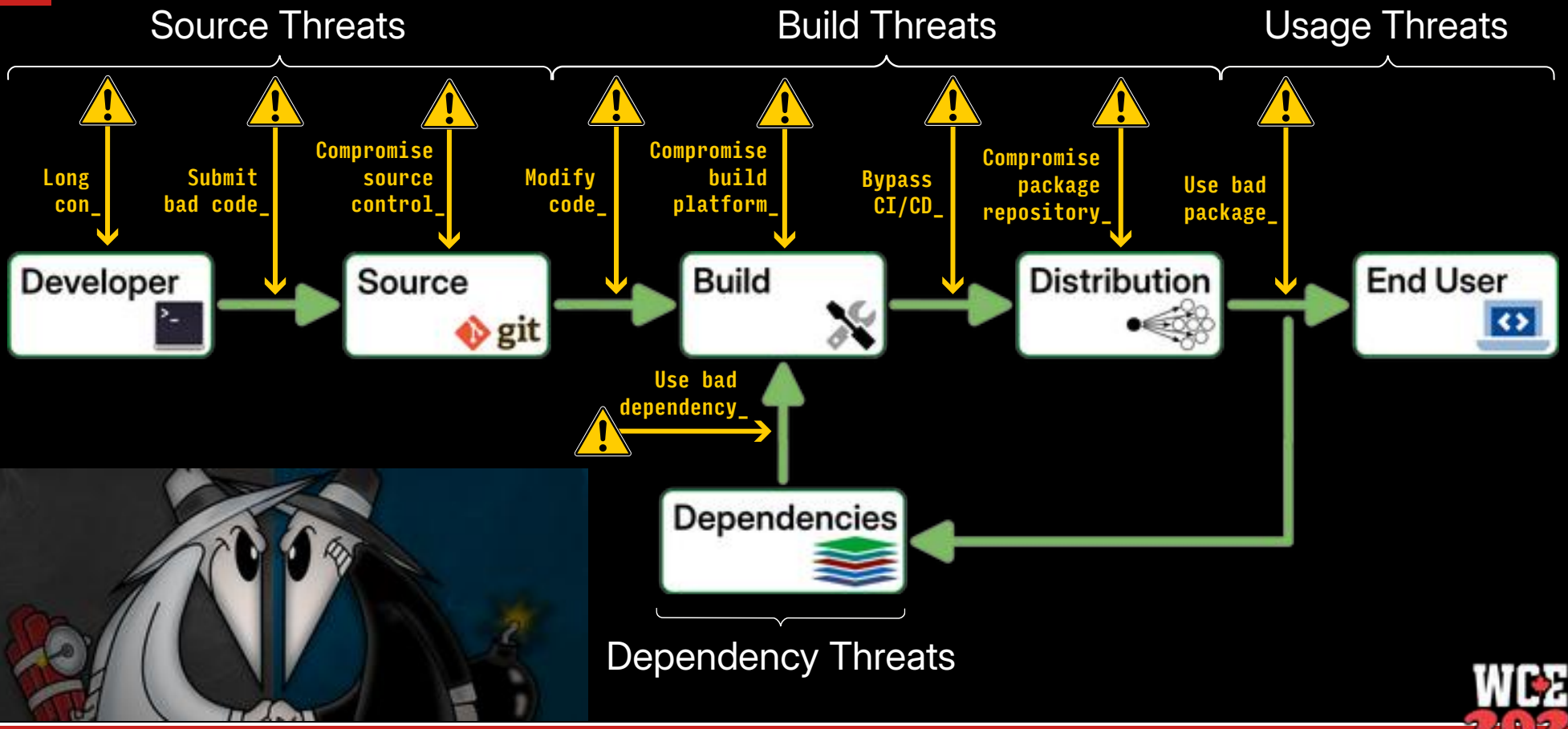
It may not come in a box anymore, but it still has a supply chain.

The Software Supply Chain

Digital goods have specialized supply chains for getting products from developers to end users.

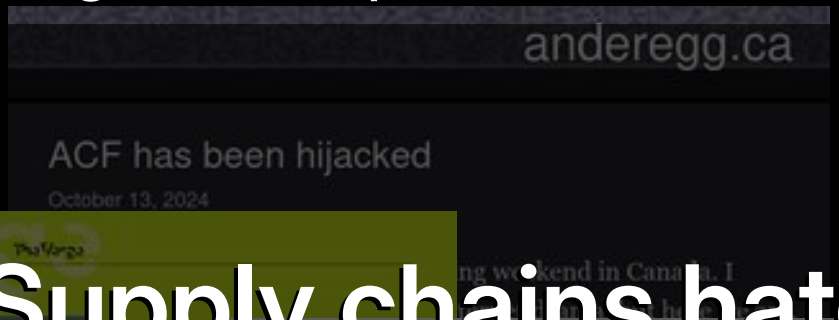


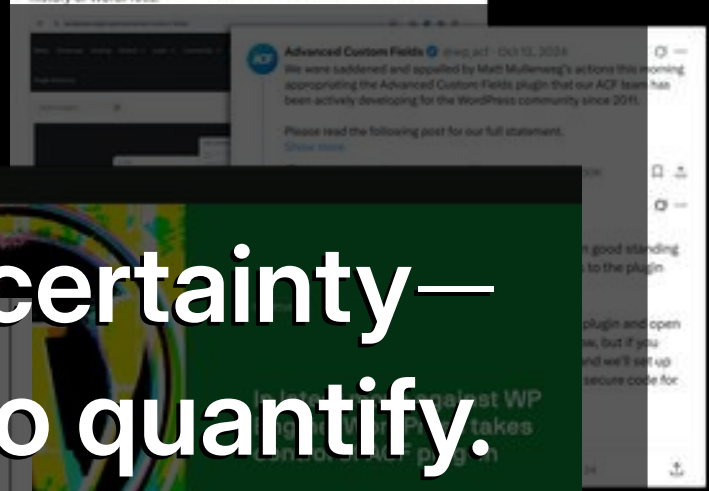
The Software Supply Chain

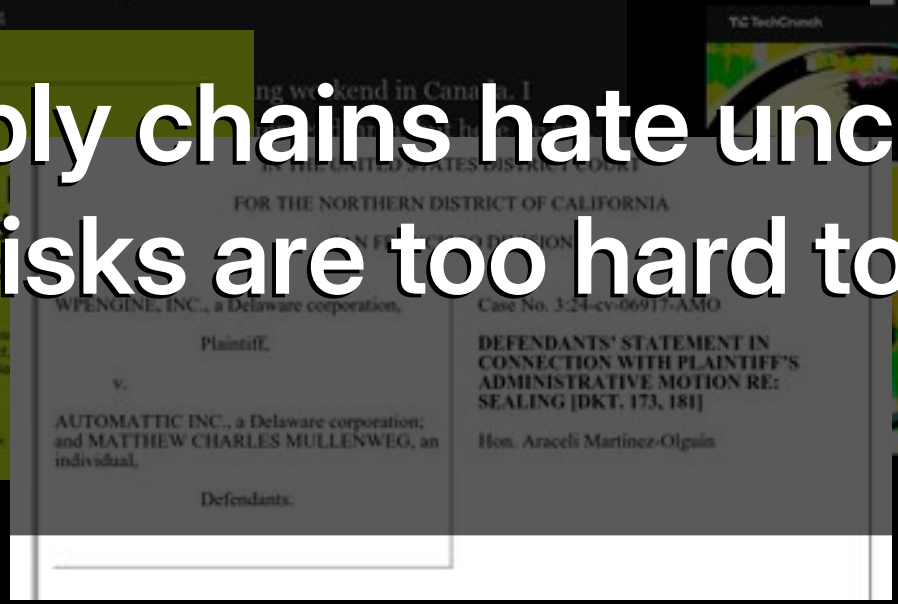


WordPress Supply Chain Risk

Existing Risk Exposed October 2024



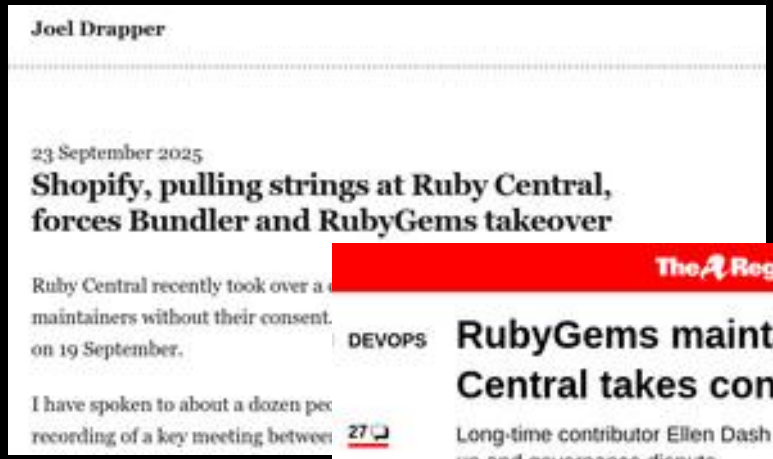




Supply chains hate uncertainty—the risks are too hard to quantify.

And it's Not Just WordPress.

Paralleled in Ruby Community
September 2025

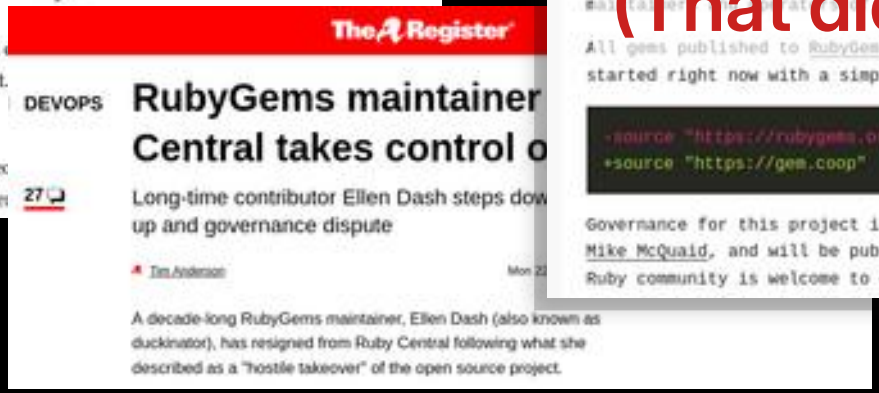

Joel Drapper

23 September 2025

Shopify, pulling strings at Ruby Central, forces Bundler and RubyGems takeover

Ruby Central recently took over a
maintainers without their consent.
on 19 September.

I have spoken to about a dozen pe
recording of a key meeting betwee


The Register

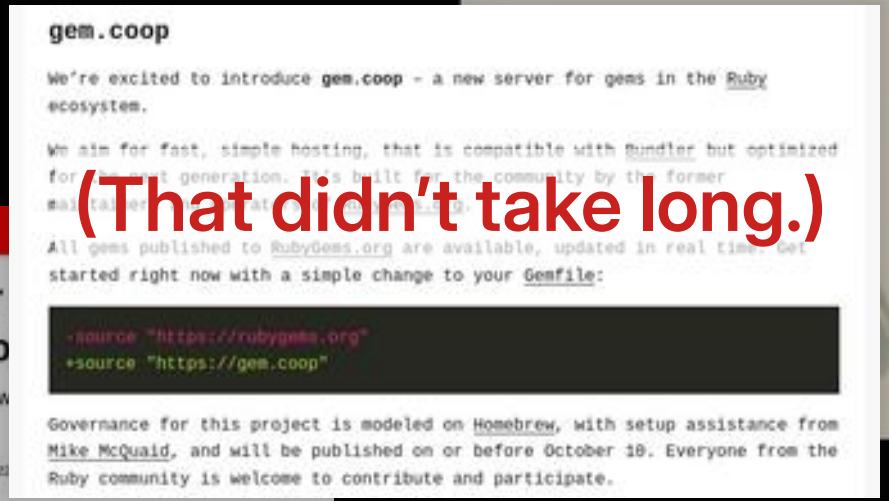
DEVOPS

RubyGems maintainer
Central takes control o

Long-time contributor Ellen Dash steps do
up and governance dispute

Tim Anderson

A decade-long RubyGems maintainer, Ellen Dash (also known as duckinator), has resigned from Ruby Central following what she described as a "hostile takeover" of the open source project.


gem.coop

We're excited to introduce **gem.coop** - a new server for gems in the Ruby ecosystem.

We aim for fast, simple hosting, that is compatible with Bundler but optimized for the next generation. It's built for the community by the former maintainers of RubyGems.org.

All gems published to RubyGems.org are available, updated in real time. Get started right now with a simple change to your Gemfile:

```
-source "https://rubygems.org"
+source "https://gem.coop"
```

Governance for this project is modeled on Homebrew, with setup assistance from Mike McQuaid, and will be published on or before October 10. Everyone from the Ruby community is welcome to contribute and participate.


404

How Ruby Went Off the Rails

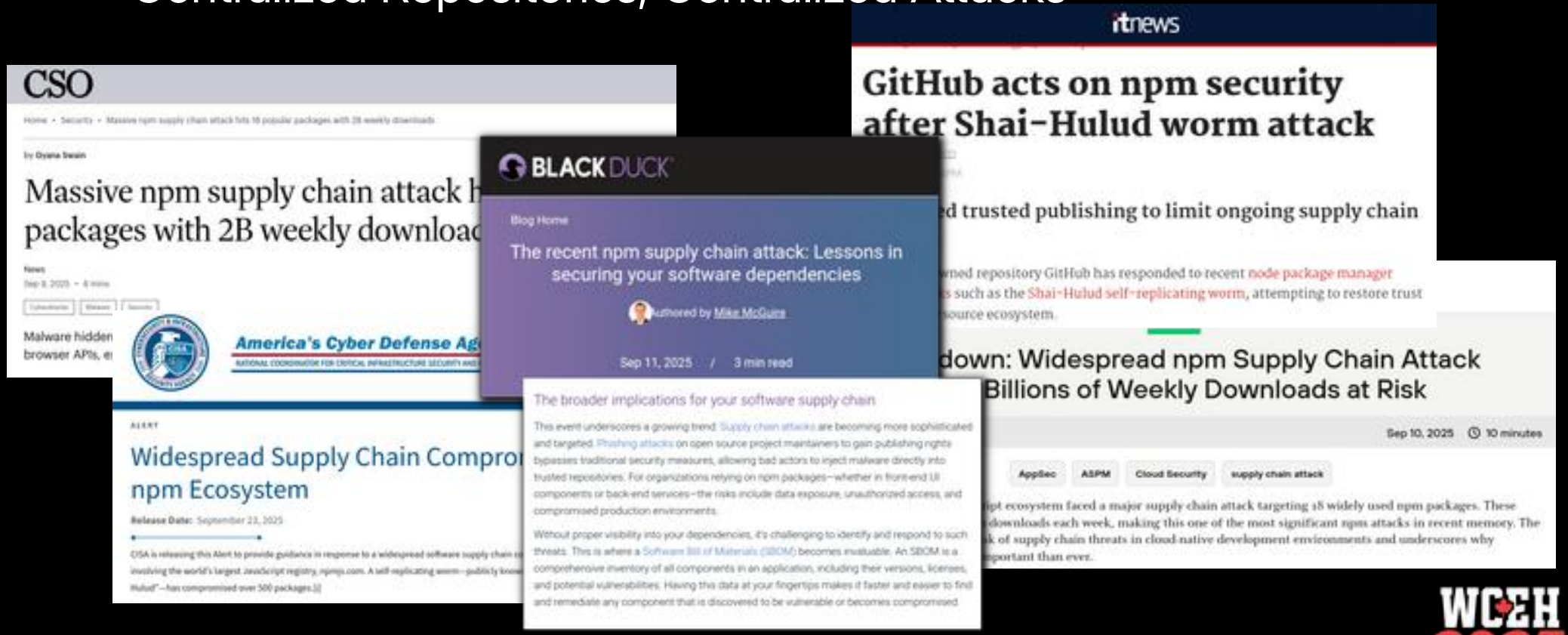
What happened to RubyGems, Bundler, and the Open Source drama that controls the internet infrastructure.

For the past couple of weeks, a community of developers who use the programming language Ruby have been closely following a dramatic change in ownership of some of the most essential tools in its ecosystem with far-reaching

(That didn't take long.)

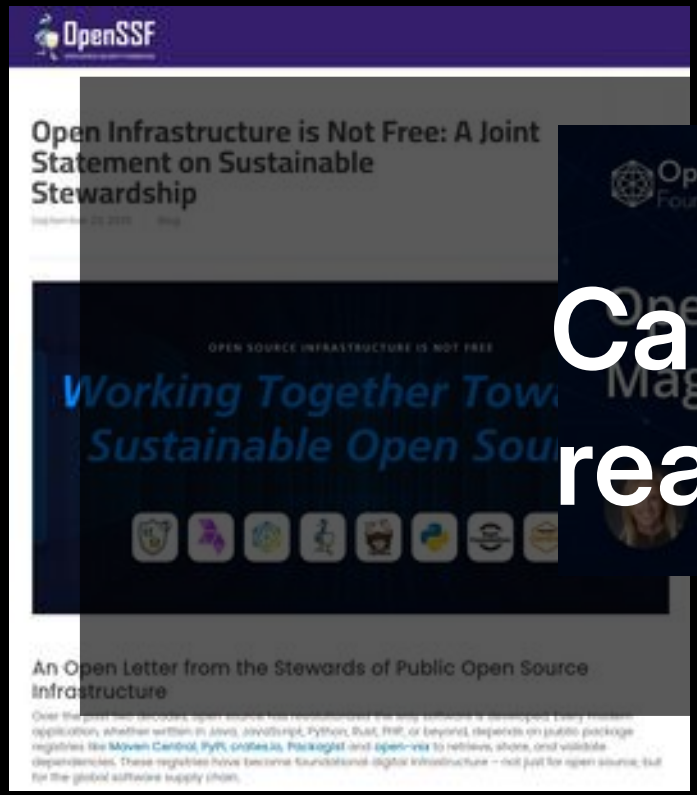
Other Supply Chain Threats

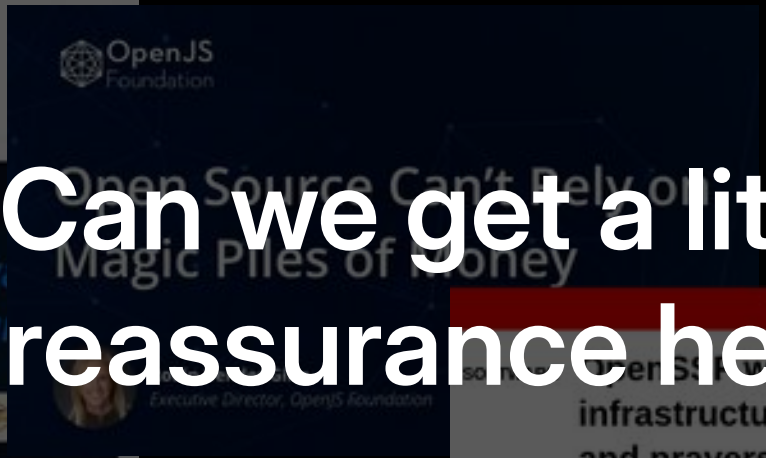
Centralized Repositories, Centralized Attacks

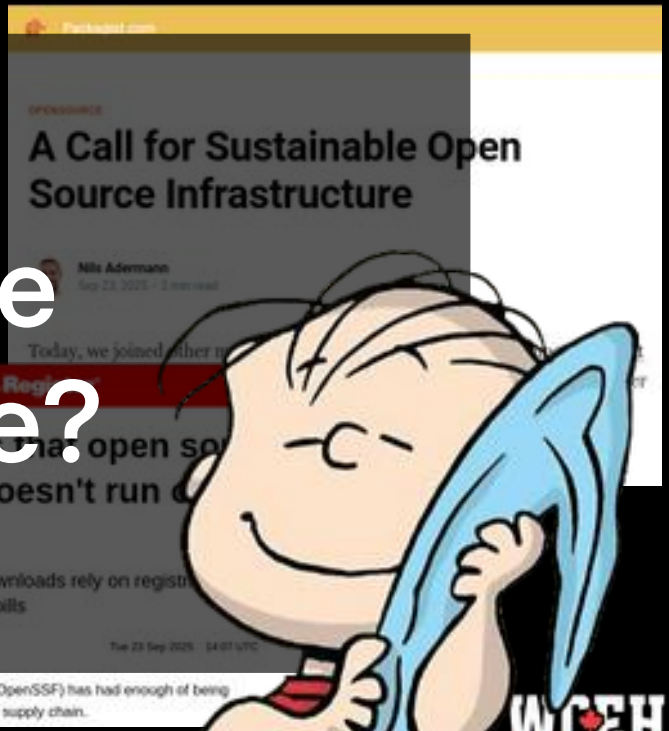


Warning Signs

Centralized Repositories May not be Sustainable: September 2025

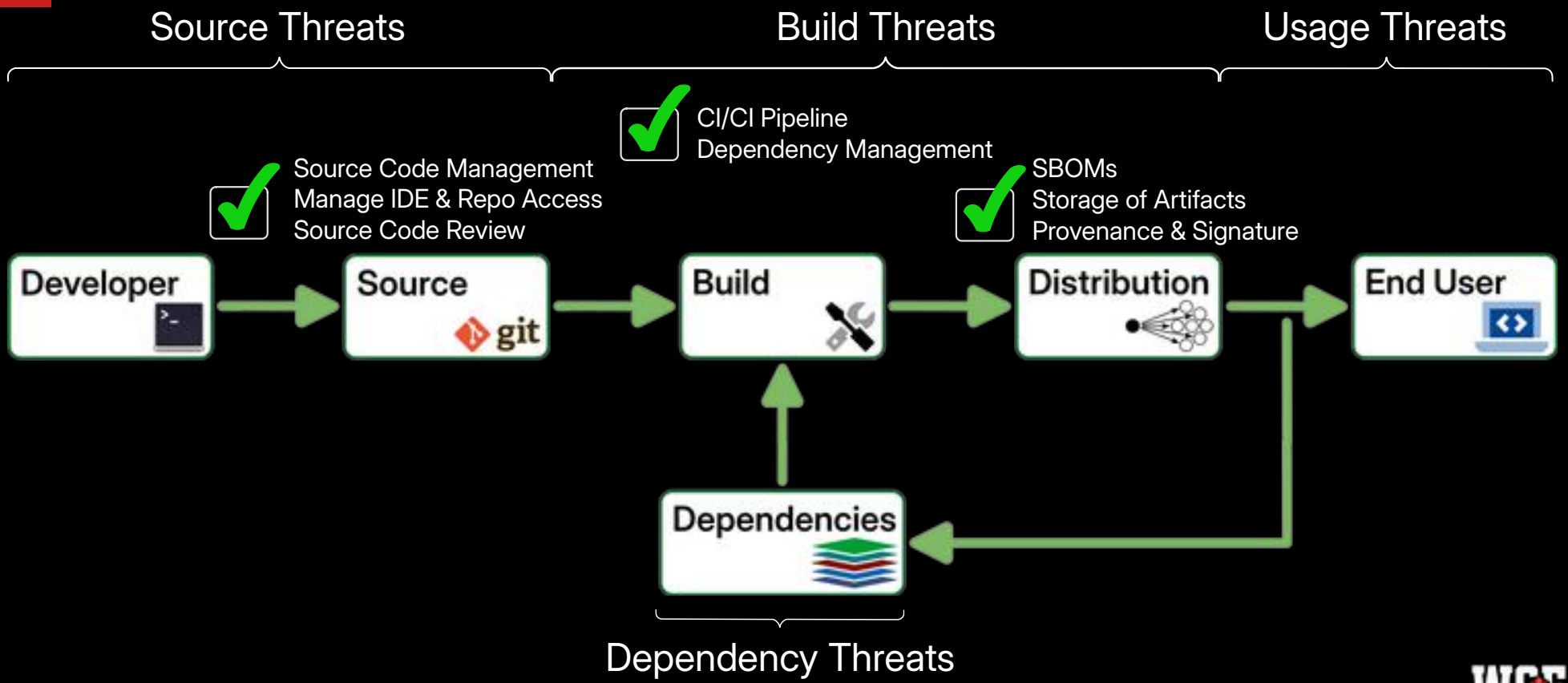






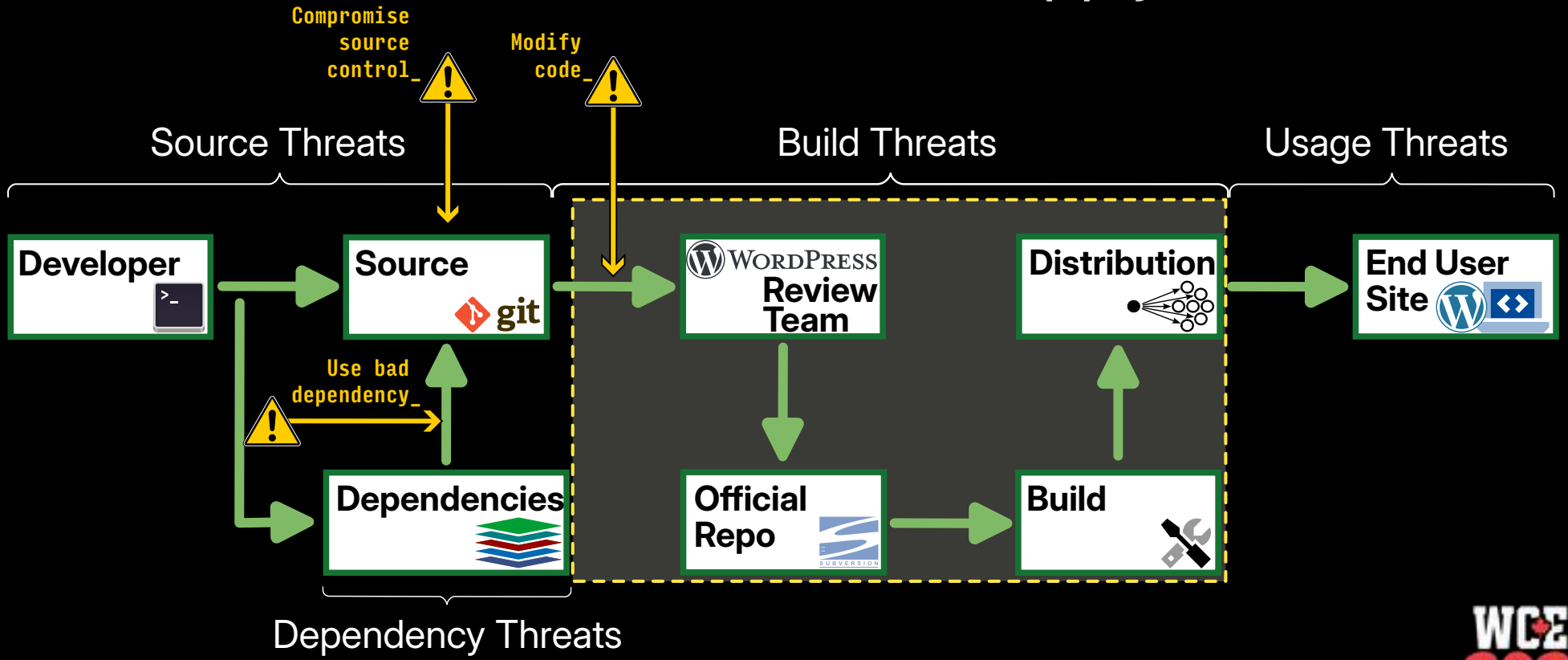
Can we get a little reassurance here?

Securing the Supply Chain



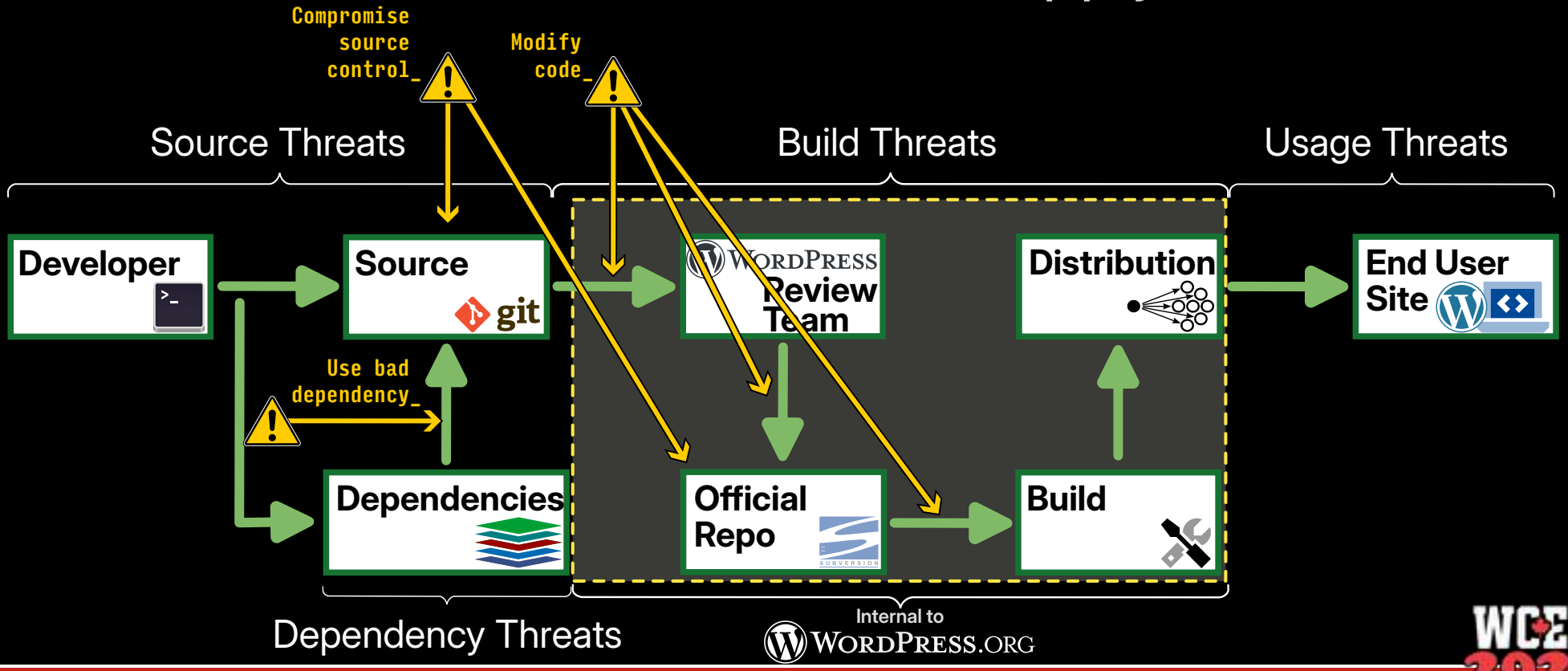
The WordPress Supply Chain

WordPress has a modified supply chain.



The WordPress Supply Chain

WordPress has a modified supply chain.



Where Did We Get this Model?

This is really more of a *"when"* question.

Circa 2004...

- Software distribution was centralized on trusted download sites
- Software was transferred by FTP
- Subversion was dominant (until 2010)
- Agile had yet to gain much adoption
- Broadband use was just passing dialup

Blogging was in the *Zeitgeist*.

Back when b2 begat WordPress...

An Abbreviated Timeline

- May 2003: First release (v 0.7)
- May 2004: Plugin support (v 1.2)
- January 2005: Official plugin repository at wp-plugins.org
- February 2005: Theme support (v 1.5)
- February 2005: Official plugin directory
- The “Wild West” of Plugins was ending.

Of necessity, the repository and directory took a centralized approach.

Can we decentralize without unleashing the “Wild West” again?

Verdict on Our Supply Chain?

- Doing nothing is always an option.

...though typically not the *best* option.

Source: KC Green, "The pills are working" – Gunshow #648 gunshowcomic.com/648

It's time to shift.

Photo by Pixabay.com

Doing nothing accepts too much risk.

Response Began October 2024

AspirePress – Federated & Distributed Repositories

- Founded by Sarah Savage
- People asking the right questions
- Software suite
- Standing up infrastructure
- Version 1.0 launched June 6, 2025 at AltCtrl.org in Basel, Switzerland

A FAIR Response

Federated
And
Independent
Repositories

- Formation talks in early 2025
- Linux Foundation (Around 1,000 Projects)
- Coordinated announcement with AspirePress June 6th at AltCtrl.org in Basel
- FAIR Plugin for Technical Independence

AspirePress & FAIR Announcement, Basel, Switzerland, June 2025

Source: Joost de Valk & Karim Marucchi, Presentation at Linux Foundation's Open Source Summit North America, June 2025

A FAIR & Aspirational Response

- Decentralize & federate software distribution for WordPress.
- Devise a method for other software projects & digital goods.

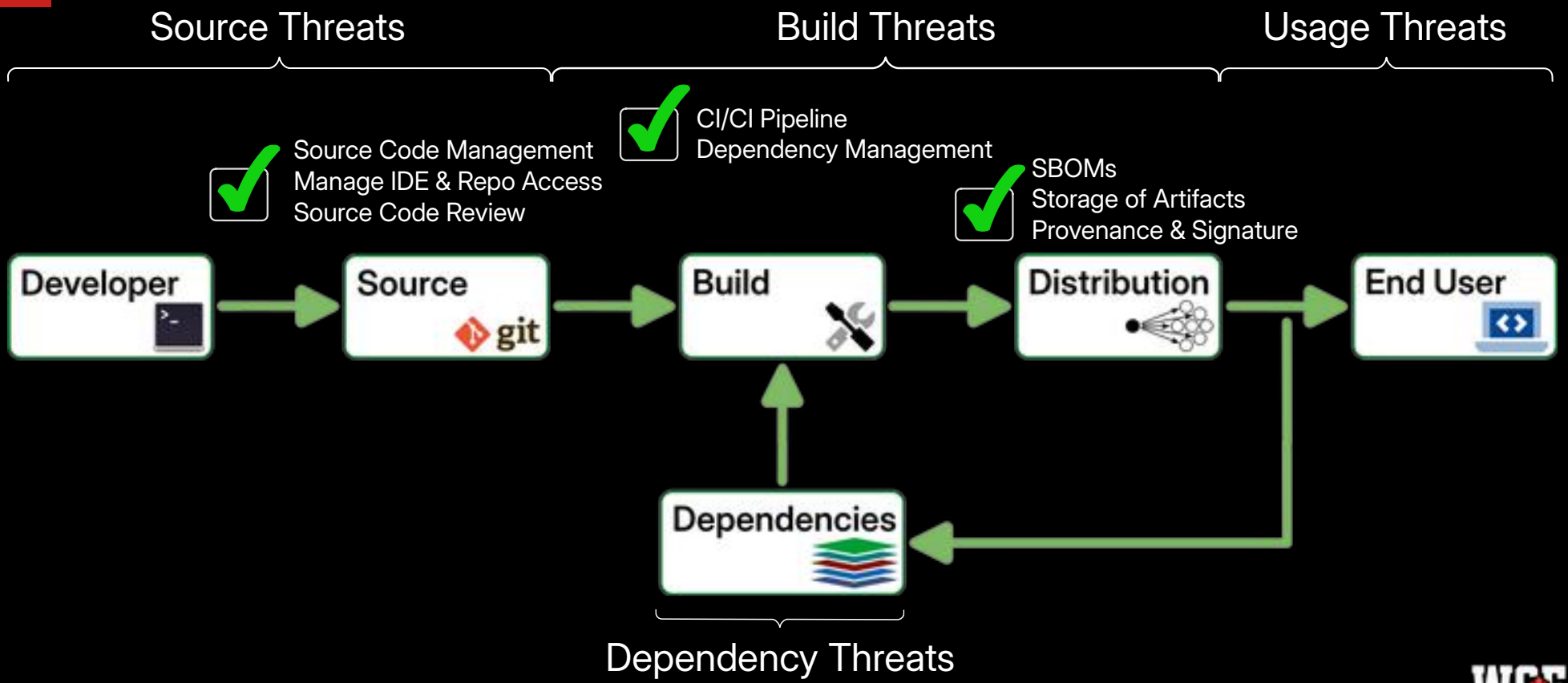
Federated
And
Independent
Repositories

Disruptive Potential

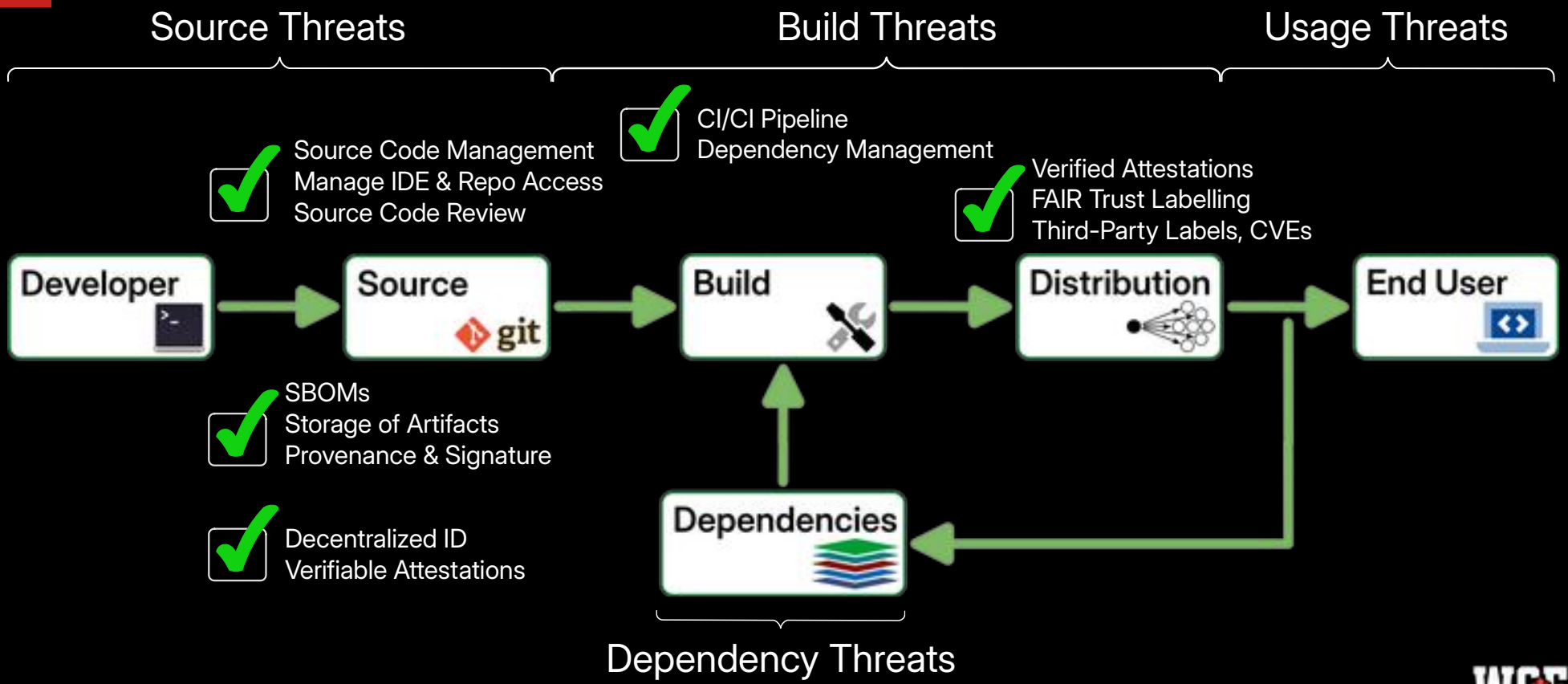
What's a FAIR Response?

- FAIR Protocol & Architecture
  - Leverages existing standards & protocols (W3C, Bluesky)
- General protocol with WordPress-specific extensions

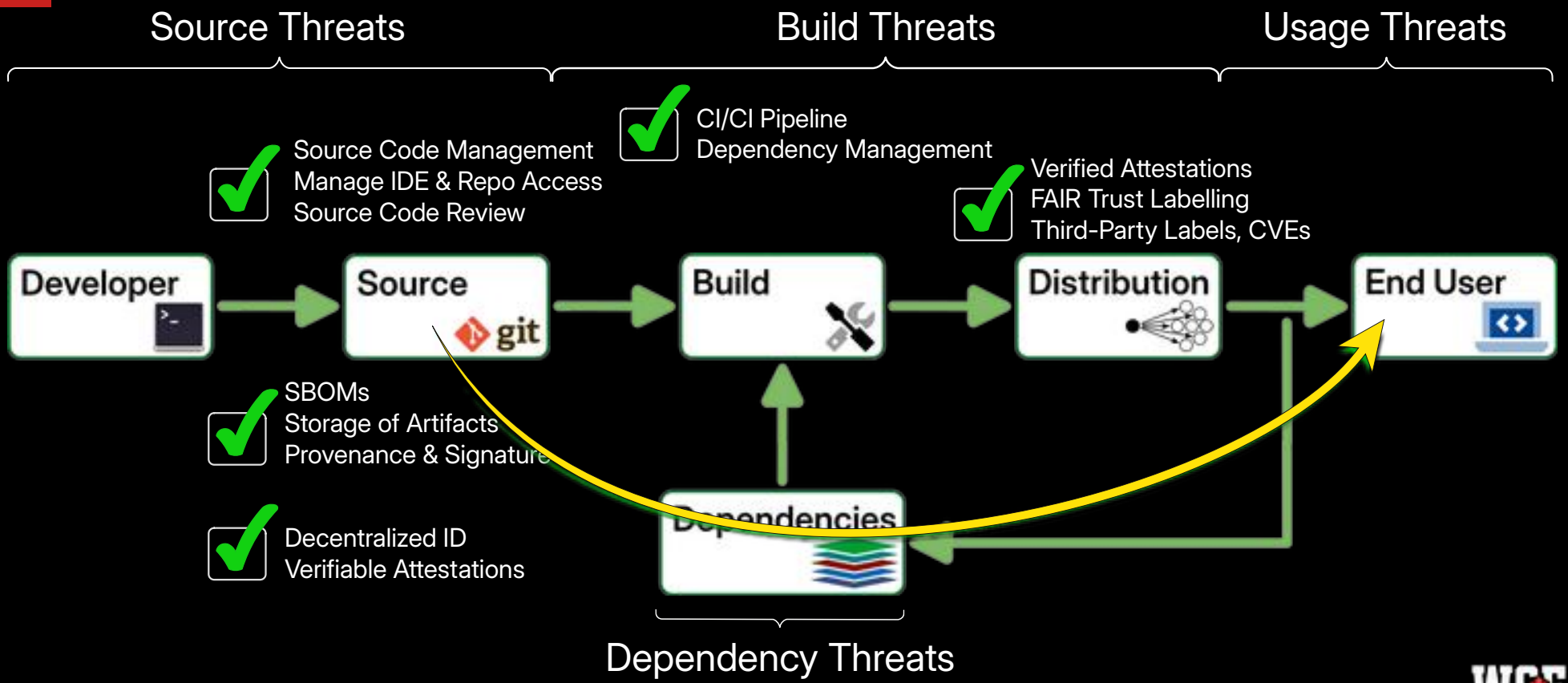
A Secure WordPress Supply Chain



A Secure WordPress Supply Chain



A Secure WordPress Supply Chain

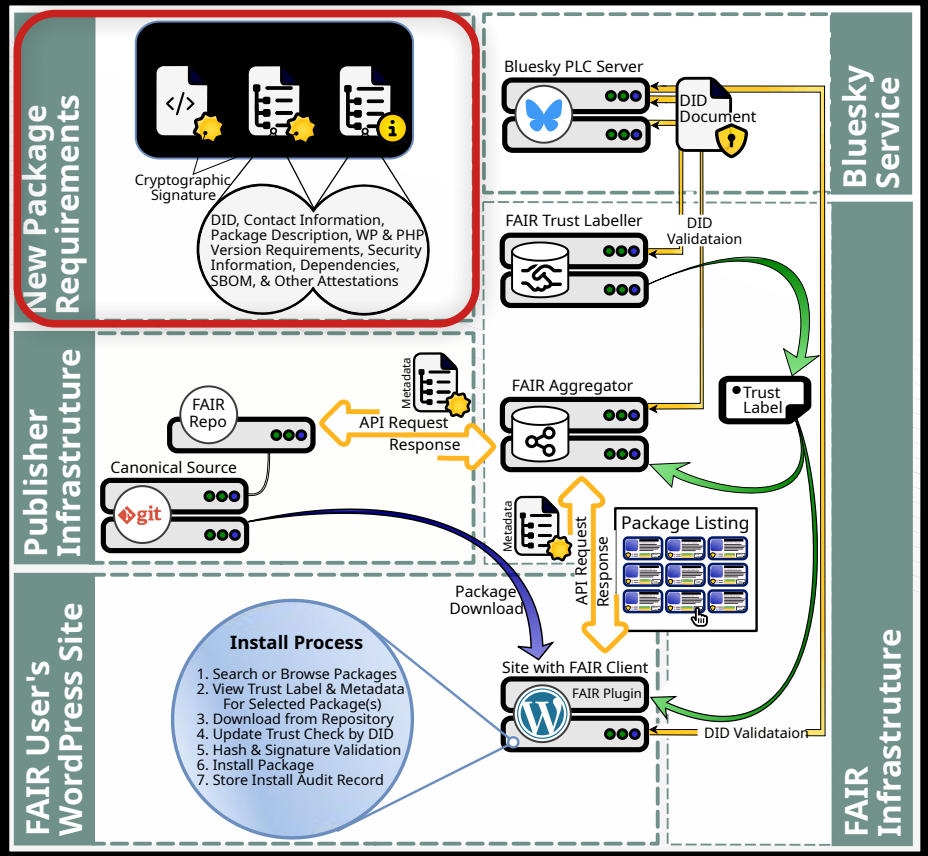


Burning Question:

So How Does it Work?

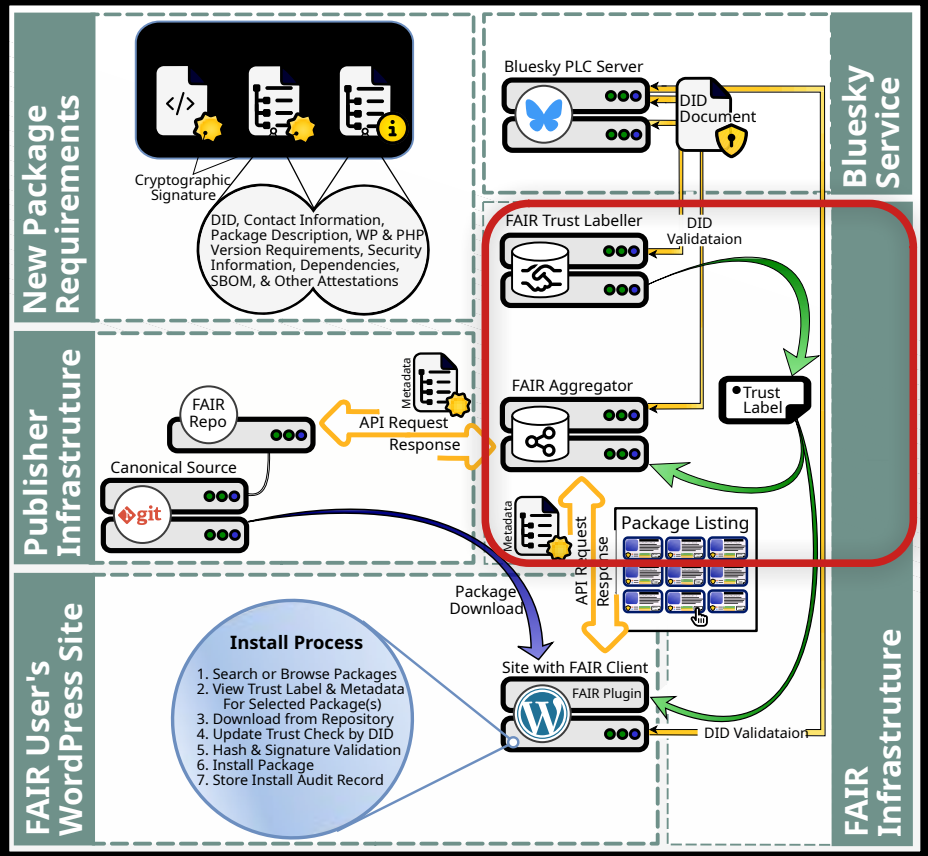
Source: Pexels; Photo by Pixabay

Decentralized Architecture



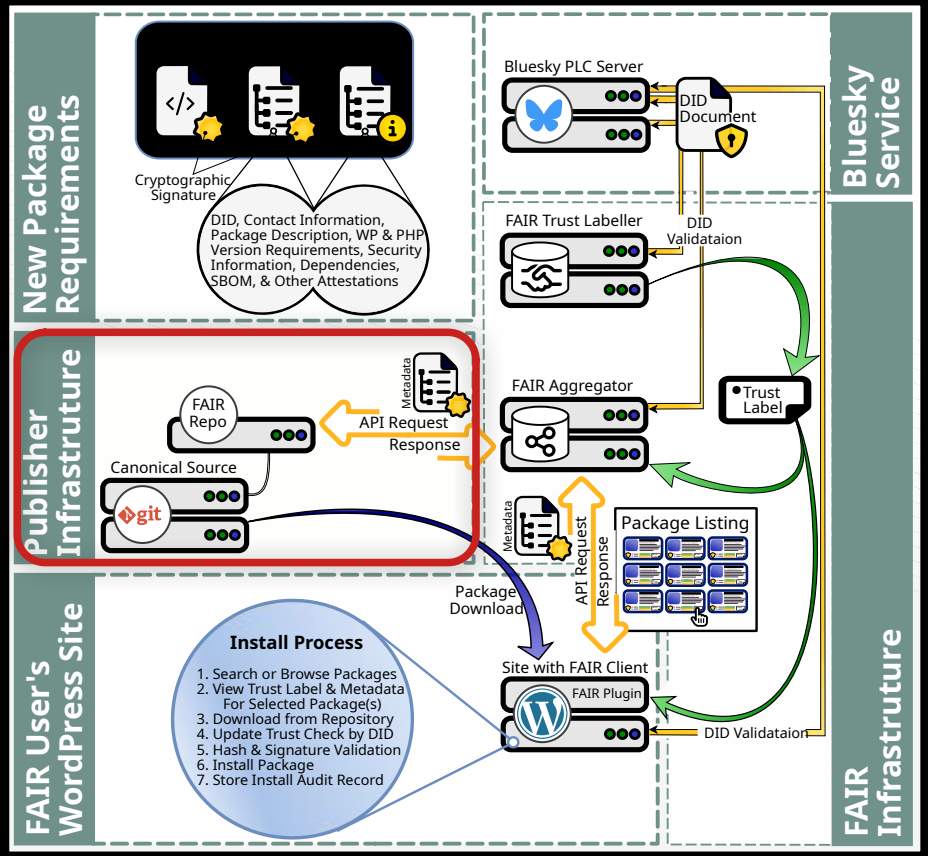
- Signed Package & Metadata (ED25519)
  - Decentralized ID (DID)
  - Provenance Document
  - Software Bill Of Materials (SBOM)

Decentralized Architecture



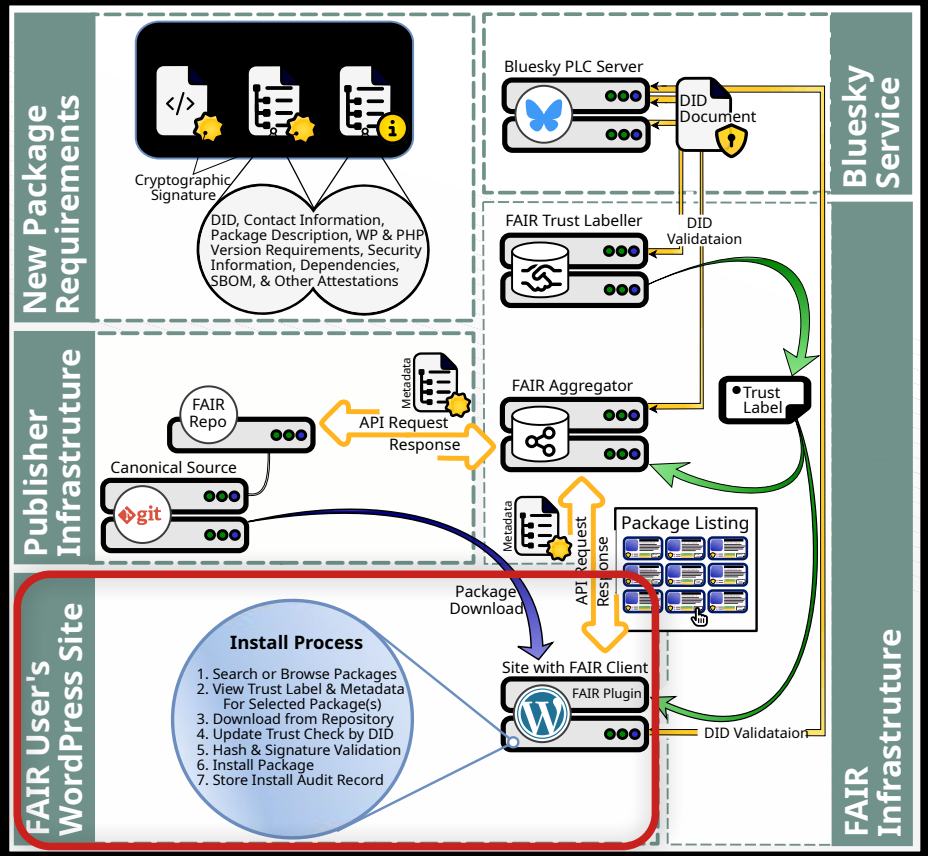
- Verify & Validate
  - Provenance & Attestations
  - Code Scanning
  - Trust Labels

Decentralized Architecture



- Distributed Repositories
  - Installs directly from Canonical Sources

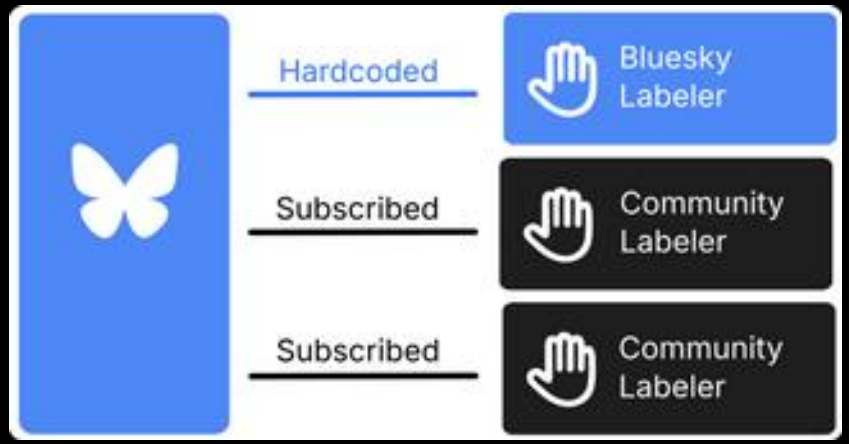
Decentralized Architecture



- Cryptographic Signature Validation

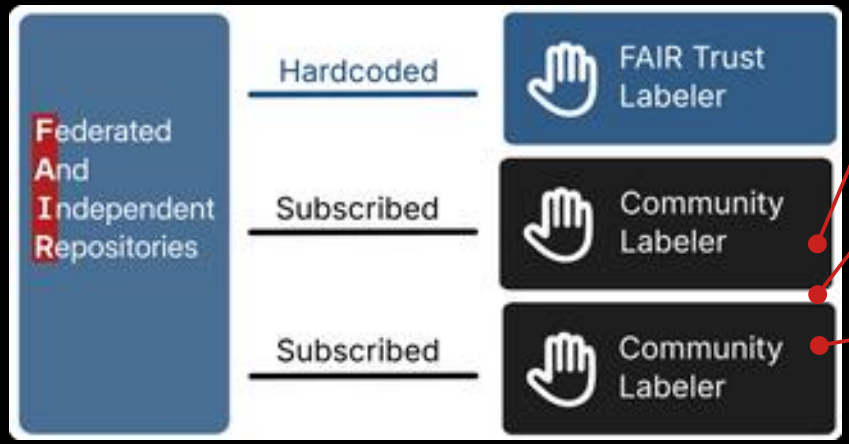
Package Labelling

- Bluesky Labelling Spec
- Decentralized Labelling
- Required & Optional Labels



Package Labelling

- Bluesky Labelling Spec
- Decentralized Labelling
- Required & Optional Labels
- Trust Model for FAIR



CVE (Common Vulnerabilities & Exposures)

No Unpatched Vulnerabilities

WPVulnerability.com

patchstack

Wordfence

SUCURI

Third-Party Tagging, Categorization, or Validation

It's FLOSS!

Meets WCAG 2.2 AA

GDPR Compliant

List Curation

Digital Trust is Kind of a Big Deal.

A Trust Model, You Say?

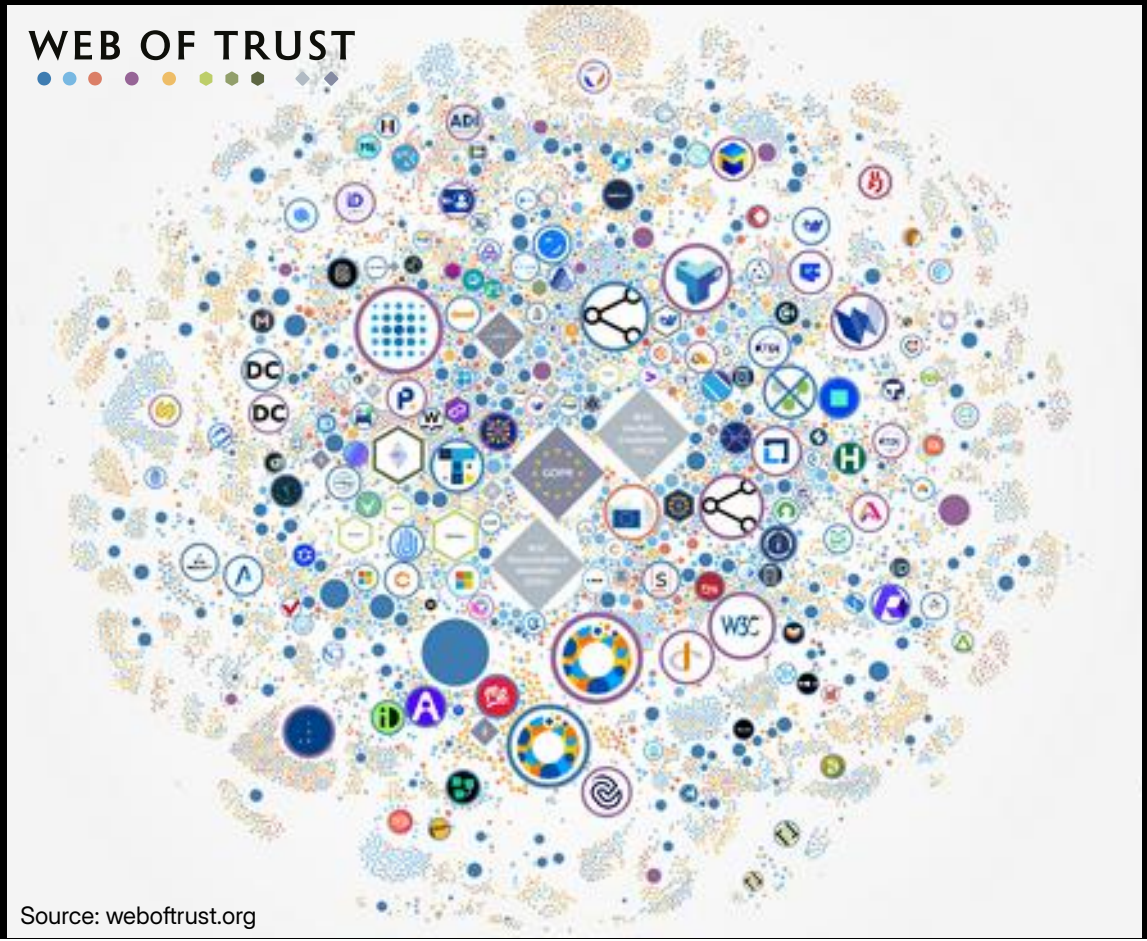
Digital Trust is getting a
lot of attention right now.

Photo by Fabian Gieske on Unsplash

LF DECENTRALIZED TRUST DIACC CCIAN

TRUST Over IP OpenID Interac DIF WEB OF TRUST

Mapping Decentralized Digital Trust

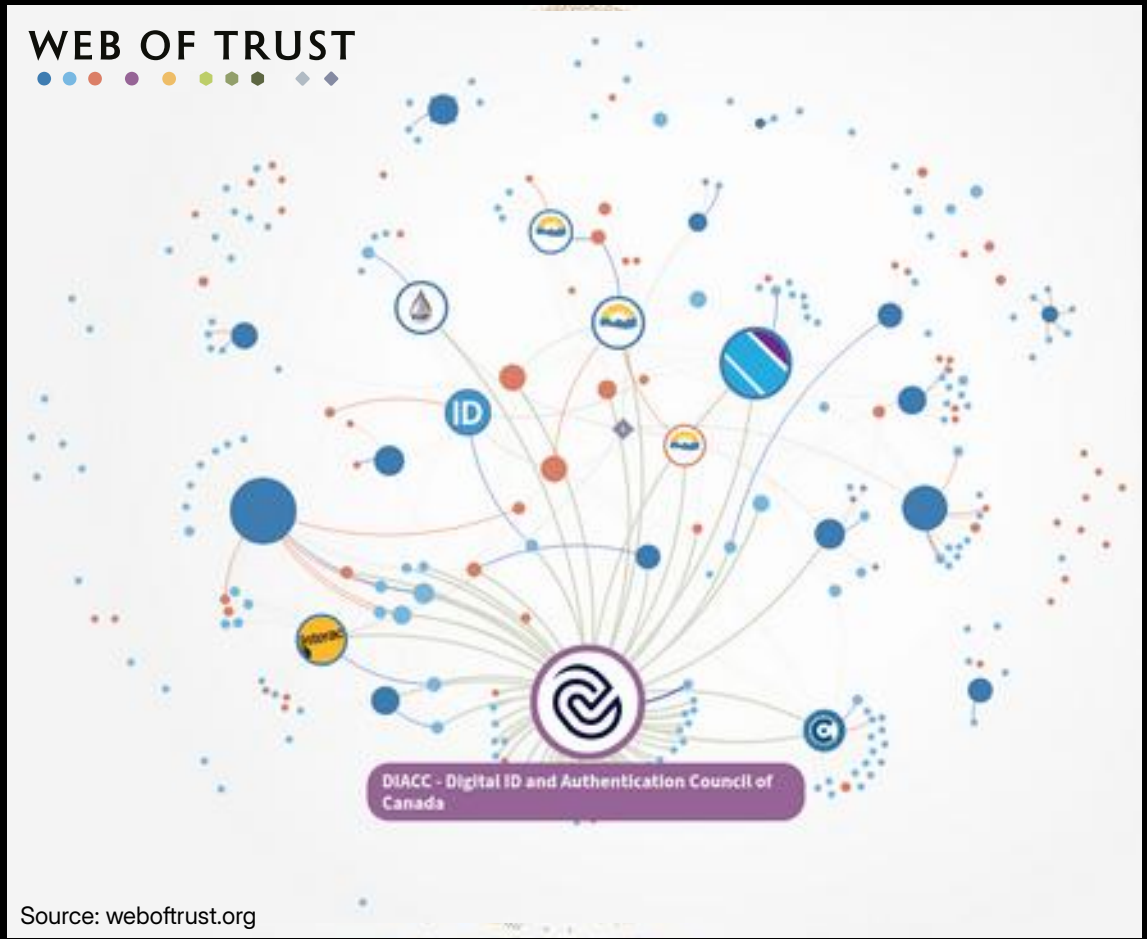


Source: weboftrust.org

Globally

- 267 ID Projects
- 43 Consortia
- 1,205 Public Entities
- 42 Regulations
- 83 Standards/Protocols
- 134 DID Methods

Mapping Decentralized Digital Trust

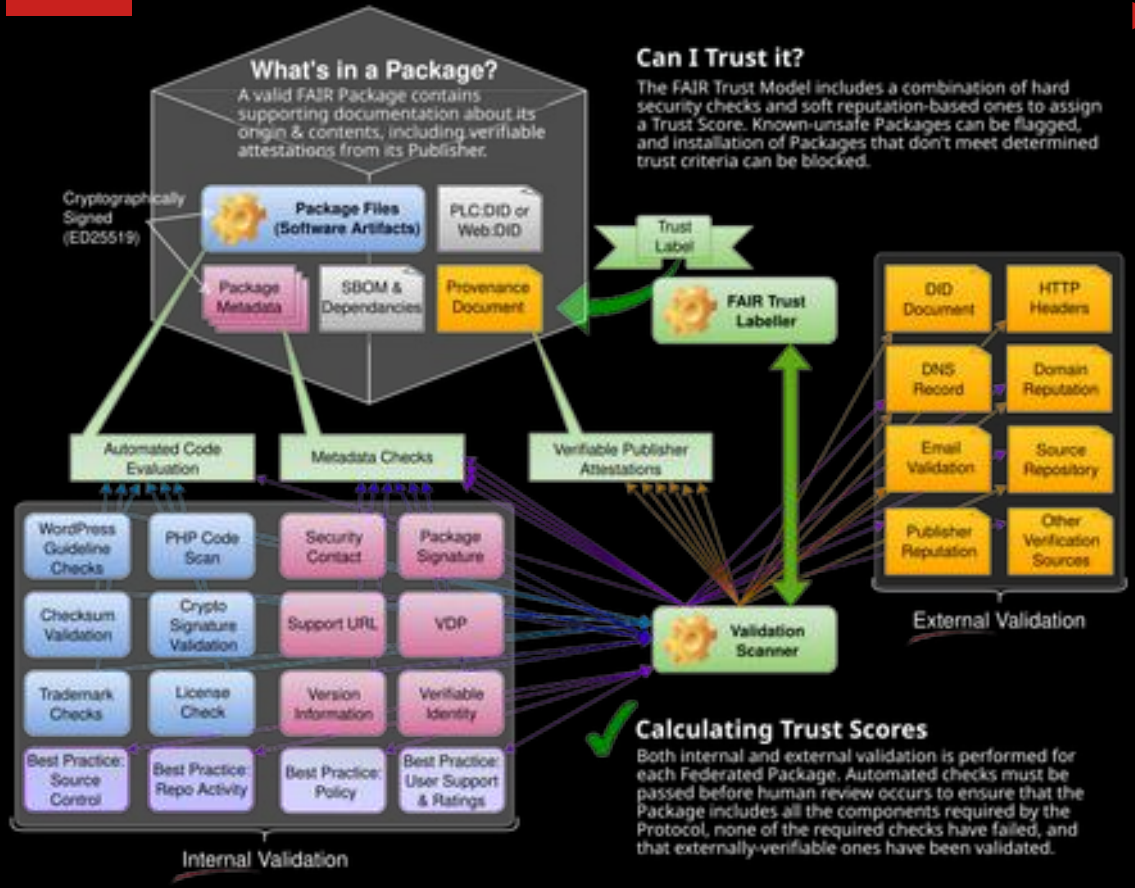


Source: weboftrust.org

Canada

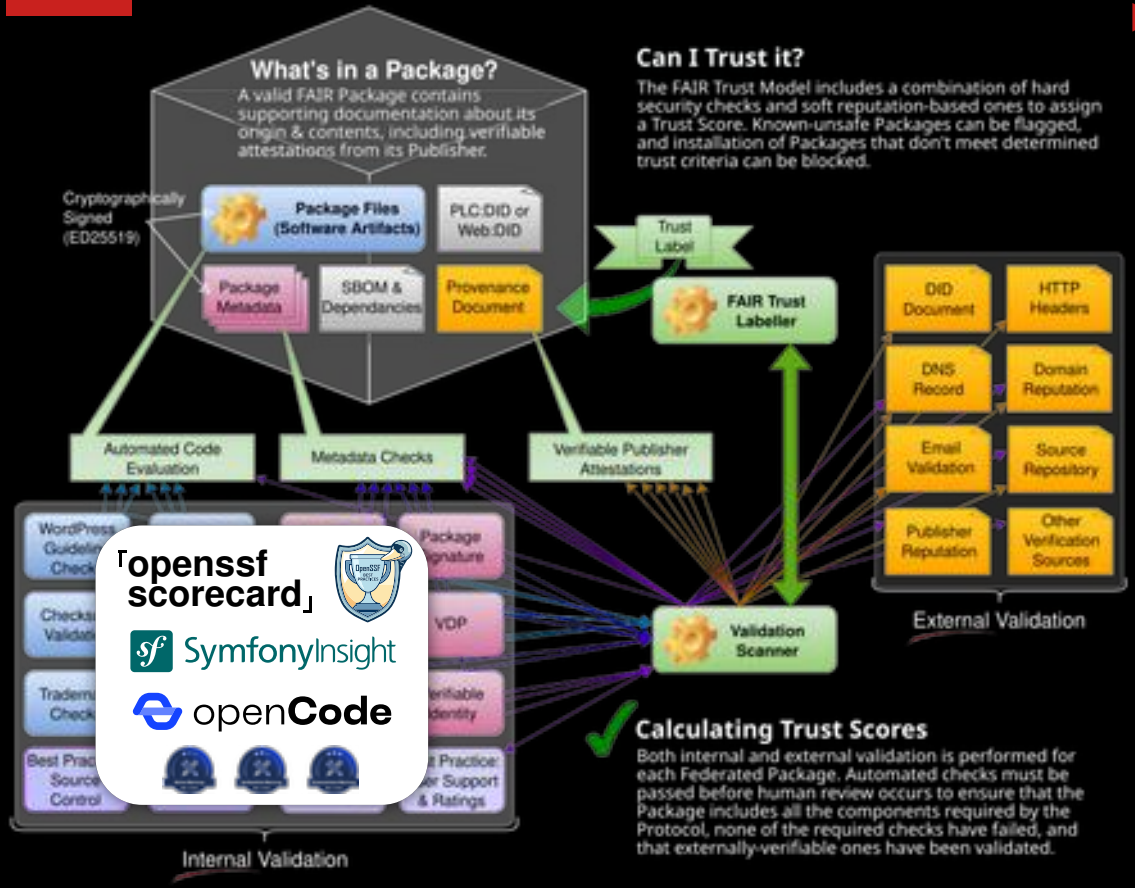
- 21 ID Projects
- 1 Consortium
- 73 Public Entities
- 5 Regulations

Creating A FAIR Trust Model



- Evaluate ED25519 Signed Metadata
  - Meta includes package information, provenance, verifiable attestations, SBOM
  - Internal Checks & External Verifications
  - Calculate Trust Score & Apply Label

Creating A FAIR Trust Model



- Evaluate ED25519 Signed Metadata
  - Meta includes package information, provenance, verifiable attestations, SBOM
  - Internal Checks & External Verifications
  - Calculate Trust Score & Apply Label
  - Criteria similar to .org *et al*: best practices, technical factors, security, & authenticity
  - Block Unsafe Installs

“The Times, They Have A-Changed.”

- We structure software projects differently.
- We organize development teams differently.
- We do version control differently.
- We even use software differently.
- **We should distribute software differently.**

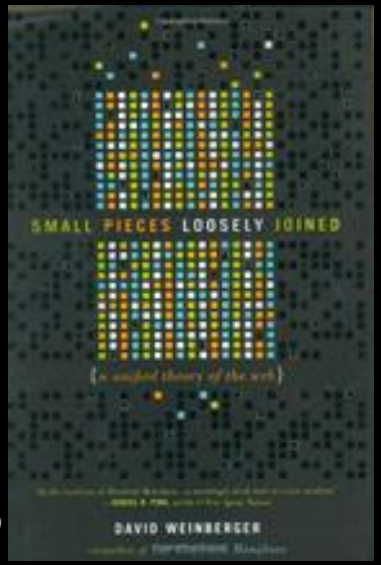
We can democratize the publishing of software.

Why the Future Will Be Federated

① **Distributed** is the natural, healthy state of the internet.

Why the Future Will Be Federated

In a perfect world, a central dispatcher (a piece of software) would know where every bit needs to go and would route each the most efficient way. But that router's every hiccough would have the effect on the rest of the system of a cardiac arrest. So the Internet was designed to have many decentralized routers, each making decisions about where to send packets next. If one of the routers goes offline... the packets are simply sent to another router. The internet routes around disruption.



The difference is between on the one hand, having your automobile club lay out a map that shows you a direct route from New York to San Francisco and, on the other hand, navigating by asking gas station attendants along the way who give replies such as, "Gosh, I don't know how to get you to San Francisco, but I think you'll be closer if you drive northwest to the next Sunoco station and ask again.

When it comes to packets in a highly dynamic highway system, the stop-and-ask technique turns out to be not only more robust, but more efficient. This only surprises us because we have long assumed that centralized power and efficiency go hand in hand.

- David Weinberger, *Small Pieces Loosely Joined: A Unified Theory of the Web* (2002)

Why the Future Will Be Federated

The spirit there was very decentralized. The individual was incredibly empowered. It was all based on there being no central authority that you had to go to to ask permission. **That feeling of individual control, that empowerment, is something we've lost.**

— Tim Berners-Lee

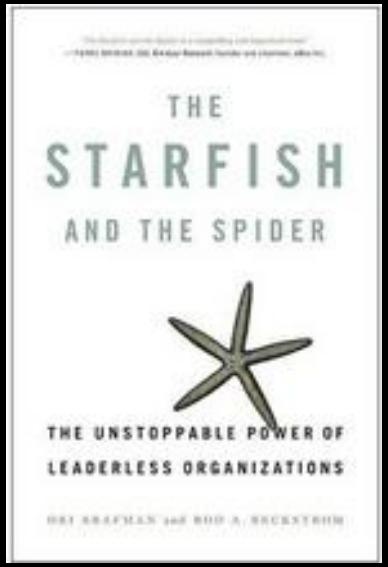
Why the Future Will Be Federated

Why the Future Will Be Federated

② The web has always been a **starfish**, not a **spider**.

Why the Future Will Be Federated

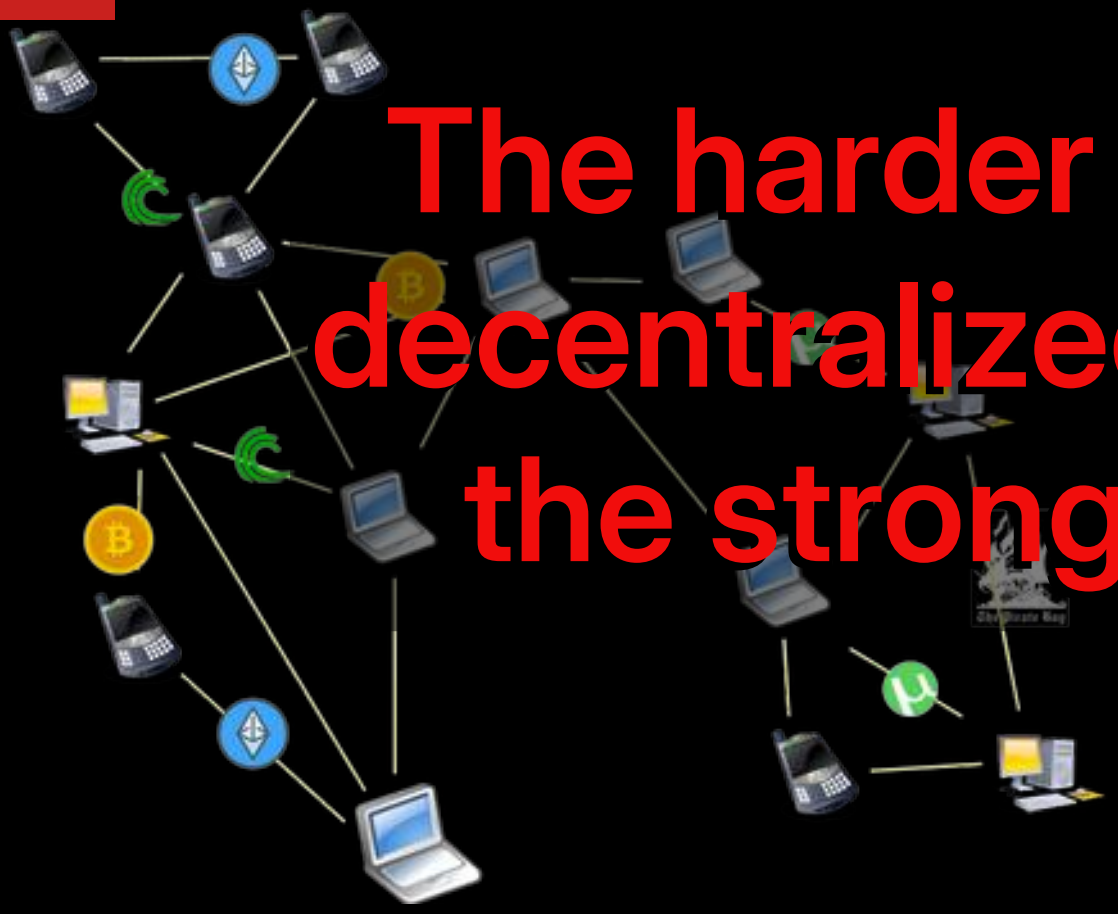
With a spider, what you see is pretty much what you get. A body's a body, a head's a head, and a leg's a leg. But starfish are very different. The starfish doesn't have a head. Its central body isn't even in charge. In fact, the major organs are replicated throughout each and every arm. If you cut the starfish in half, you'll be in for a surprise: the animal won't die, and pretty soon you'll have two starfish to deal with.



Starfish have an incredible quality to them: If you cut an arm off, most of these animals grow a new arm. And with some varieties... can replicate itself from just a single piece of an arm. ...They can achieve this magical regeneration because in reality, a starfish is a neural network—basically a network of cells. Instead of having a head, like a spider, the starfish functions as a decentralized network. Get this: for the starfish to move, one of the arms must convince the other arms that it's a good idea to do so. The arm starts moving, and then—in a process that no one fully understands—the other arms cooperate and move as well. The brain doesn't "yea" or "nay" the decision. In truth, there isn't even a brain to declare a "yea" or "nay." The starfish doesn't have a brain. There is no central command. Biologists are still scratching their heads over how this creature operates.

- Ori Brafman & Rod Beckstrom, *The Starfish and the Spider: The Unstoppable Power of Leaderless Organizations* (2006)

Why the Future Will Be Federated



The harder you fight a decentralized opponent, the stronger it gets.

— Ori Brafman

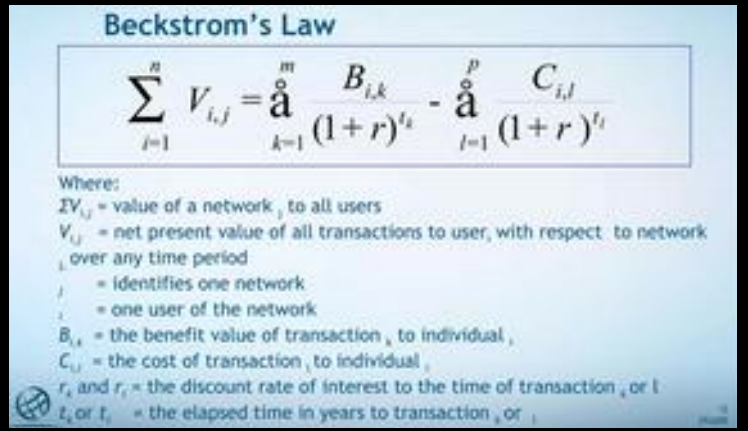
Why the Future Will Be Federated

③ Centralization brings *zero* **network value**.

Why the Future Will Be Federated

The value of a network equals the net value added to each user's transactions, summed for all users.

— Beckstrom's Law



Source: Beckstrom's Law & The Economics Of Networks – ICANN (Rod Beckstrom) on Slideshare

Individual Cost of Lost Network
x The Number of Users
= Network Value

Network Economics:
when everyone supplies a portion of the network, its users share in its costs.

Why the Future Will Be Federated

If you're not decentralized, you're not worth using.

— Linus Torvalds

Photo: Peter Adams, facesofopensource.com

Why the Future Will Be Federated

④ **It's time.**

The future starts *now*.

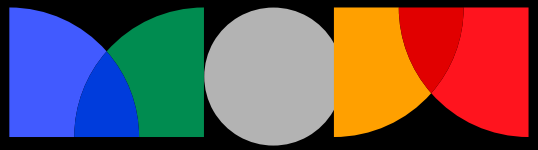
Why the Future Will Be Federated

Innovation tends to happen when the time is right.

— John Pierce

Why the Future Will Be Federated

The ethos of the Open Web is a decentralized web.



MOVEMENT
for an open web

Federated. Independent. Future.

The Future will not be Centralized.

End Notes

100PERCENT WEBHOST.CA

MODERN EARTH

Web

- W3C.org
- ATproto.com
- WebOfTrust.org
- SLSA.dev
- fair.pm
- LinuxFoundation.org
- OpenSSF.org

Books & Publications

- *Small Pieces Loosely Joined: A Unified Theory of the Web*, David Weinberger (2001)
- *The Starfish and the Spider: The Unstoppable Power of Leaderless Organizations*, Ori Brafman & Rod Beckstrom (2006)
- Beckstrom's Law & The Economics Of Networks (ICANN Presentation), Rod Beckstrom (2009)

FAIR

aspire PRESS

Get Involved

- chat.fair.pm
- GitHub.com/fairpm