

# FAIR Package Manager

Securing WordPress at scale



## KARIM MARUCCHI

- Entrepreneur
- Digital Business Strategist
- Professional Service Teams Strategist
- Unconventional Growth & Strategic M&A

### Selected Board Seats:



Beech Hollow  
wildflower farm

Post Status

SCALE  
CONSORTIUM

### 30 Years of Building Enterprise Digital Solutions:

Disney

Microsoft

NVIDIA

AT&T

LEXUS

THE NATIONAL  
ACADEMY OF  
TELEVISION  
ARTS & SCIENCES

NATIONAL  
GEOGRAPHIC

Campbell's

THOMSON REUTERS

Janus Henderson  
INVESTORS

STARZ

mailchimp

Providence

Rabobank

Meta



Ogilvy

mozilla  
FOUNDATION

TE

NBC  
Sports

H-E-B



abc studios

NIH  
National Institutes  
of Health

intel

SONY

NGINX

United States  
Olympic  
& Paralympic  
Museum





## JOOST DE VALK

- Entrepreneur
- Investor
- Developer
- Marketer

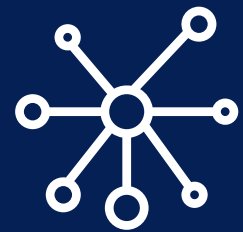


Board of & investor in:



Investor in:





**F**

Federated



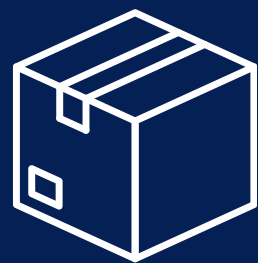
**A**

And



**I**

Independent




**R**

Repositories







A wooden desk with a notebook, pen, glasses, and a cup of coffee. The notebook is open, showing a grid pattern. The pen is black and lies diagonally across the desk. The glasses are black and lie horizontally across the desk. The cup is white and filled with coffee. The background is a wooden surface.

EMBRACE

CHANGE



A man with short dark hair, wearing a white t-shirt, is shown from the chest up. He has a shrugging expression on his face and his hands are held out to the sides, palms up, in a gesture of uncertainty or questioning. The entire image is overlaid with a semi-transparent blue filter. Centered over the man's torso is the text "For who is FAIR?" in a white, sans-serif font.

For who is FAIR?



# Developers

For developers, FAIR provides one consistent update mechanism and real choices in distribution.



The background is a dark blue gradient. It features a stylized illustration of server racks on the left and right sides, with horizontal lines representing data or circuitry. In the center, there is a light blue cloud shape. Overlaid on the cloud and the background is a network diagram consisting of several circular nodes of varying sizes, some with concentric rings, connected by thin white lines. The overall aesthetic is technological and digital.

# Hosts

For hosts, FAIR offers a CRA-compliant update pipeline and the option to run curated or private repositories.





# Enterprise & government

For enterprises and governments, FAIR provides internal distribution options, restricted plugin catalogs, and zero outbound data flow.

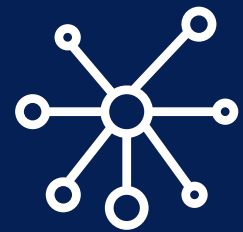


A group of four people (three men and one woman) are gathered around a smartphone, looking at the screen with interest. The man in the foreground is wearing sunglasses and a plaid shirt. The woman next to him is smiling. The background is a textured wall. The entire image is overlaid with a semi-transparent blue filter.

# Users

Users hardly see change. The experience stays the same.  
The system underneath becomes safer & truly open source.





**F**

Federated



**A**

And



**I**

Independent



**R**

Repositories

A decentralized and verifiable  
package network for WordPress and  
any other open source project.





FAIR is bigger than  
WordPress





A man with short dark hair, wearing a white t-shirt, is shown from the chest up. He has a shrugging expression on his face and his hands are held out to the sides, palms up, in a gesture of uncertainty or questioning. The entire image is overlaid with a semi-transparent blue filter. The text "What is at stake?" is centered over the man's chest in a white, sans-serif font.

What is at stake?



Every WordPress site depends on  
WordPress.org for installs and updates.





# One point of failure

One domain.

One operator.

If it goes down, plugin, theme & update delivery stops.



# Lack of governance

WordPress.org is  
not controlled by  
the foundation.

It is privately  
controlled.





# The CRA changes everything

The EU Cyber  
Resilience Act forces  
stronger control over  
software supply chains.





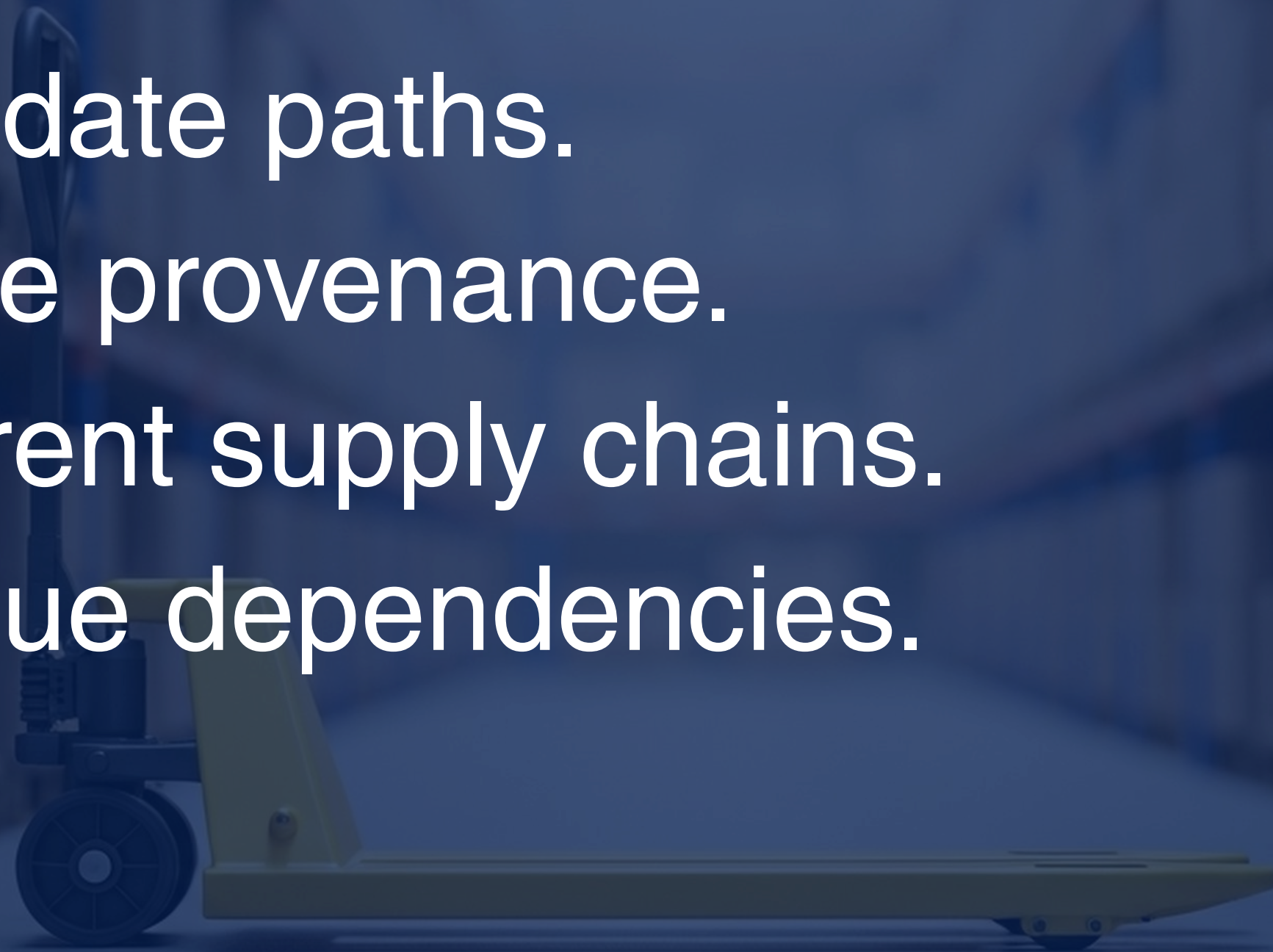
# CRA requires...

Clear update paths.

Traceable provenance.

Transparent supply chains.

No opaque dependencies.







Sites → WordPress.org → Plugins

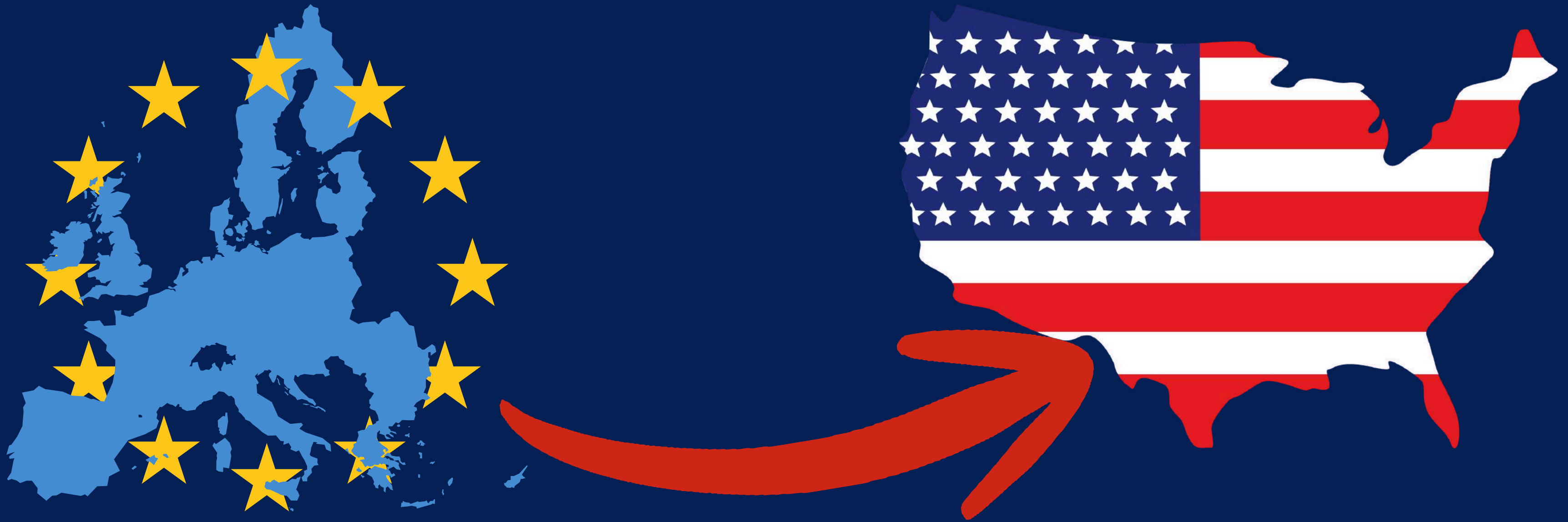
You cannot comply when your updates come from an *external system with opaque control* and that cannot be *audited*.



A photograph of a server room with rows of server racks. The racks are filled with electronic equipment, and many small, colorful indicator lights are visible. A person is standing in the distance, providing a sense of scale. The image is overlaid with a semi-transparent blue filter.

European hosts and organisations cannot  
prove supply-chain control under the  
current model.





WordPress update checks send data to WordPress.org and (US based) Automattic. Blocking this breaks updates.



The current plugin distribution model  
has **at least five** major flaws.



1

You can only **easily** install new plugins from WordPress.org.

*INSTALL*







2

Every non w.org plugin uses its own update system.



3

There are no consistent safety checks outside WordPress.org.





4

(Update) data is sent upstream  
without clear consent or control.



Three **new** challenges come with  
decentralization.



5

Analytics without central surveillance.



The background of the slide is composed of numerous overlapping squares in various shades of blue and purple. The squares are arranged in a way that creates a sense of depth and movement, with some squares appearing to be on top of others. The colors range from deep indigo to a lighter, dusty blue.

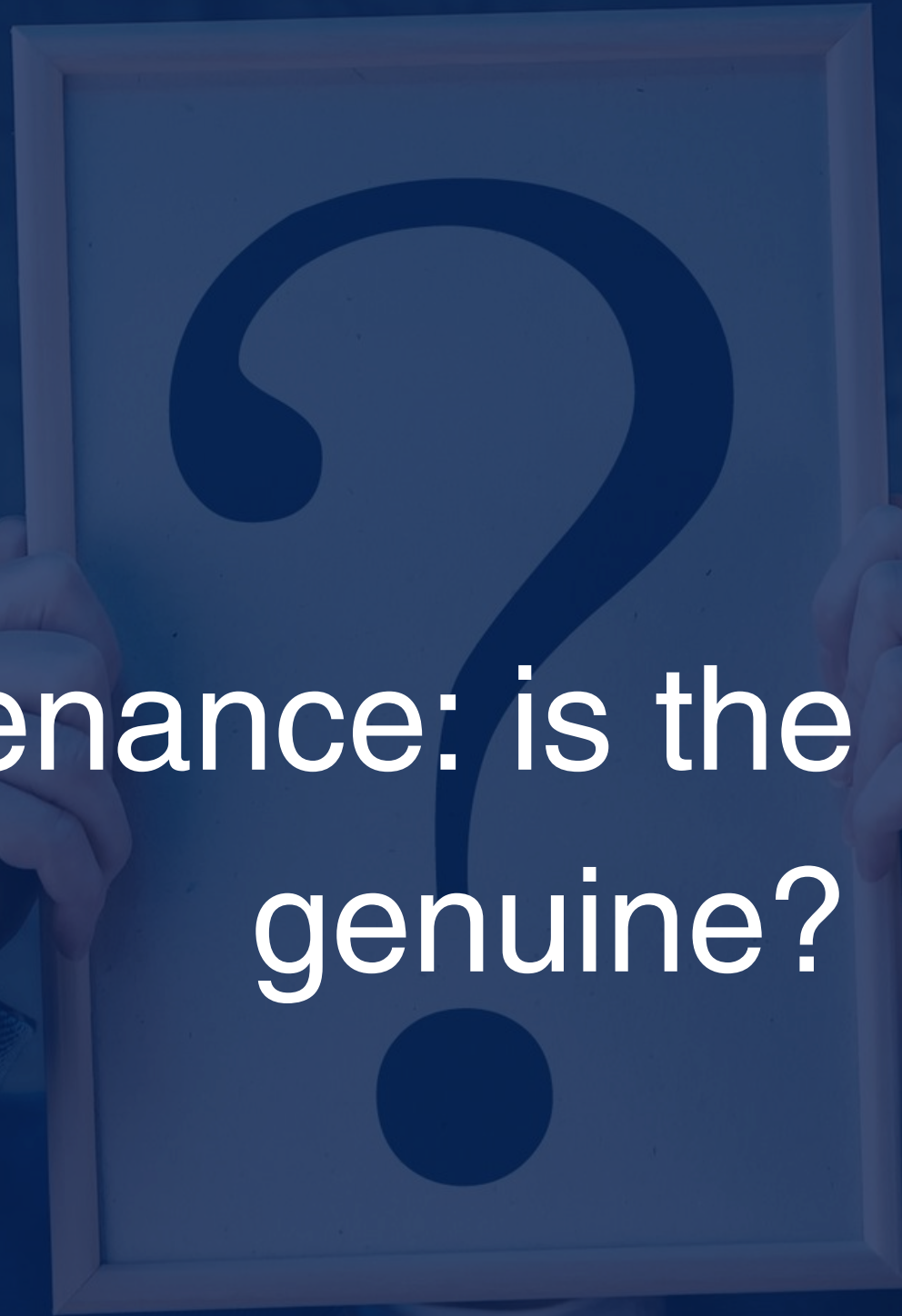
6

## Moderation without a single authority

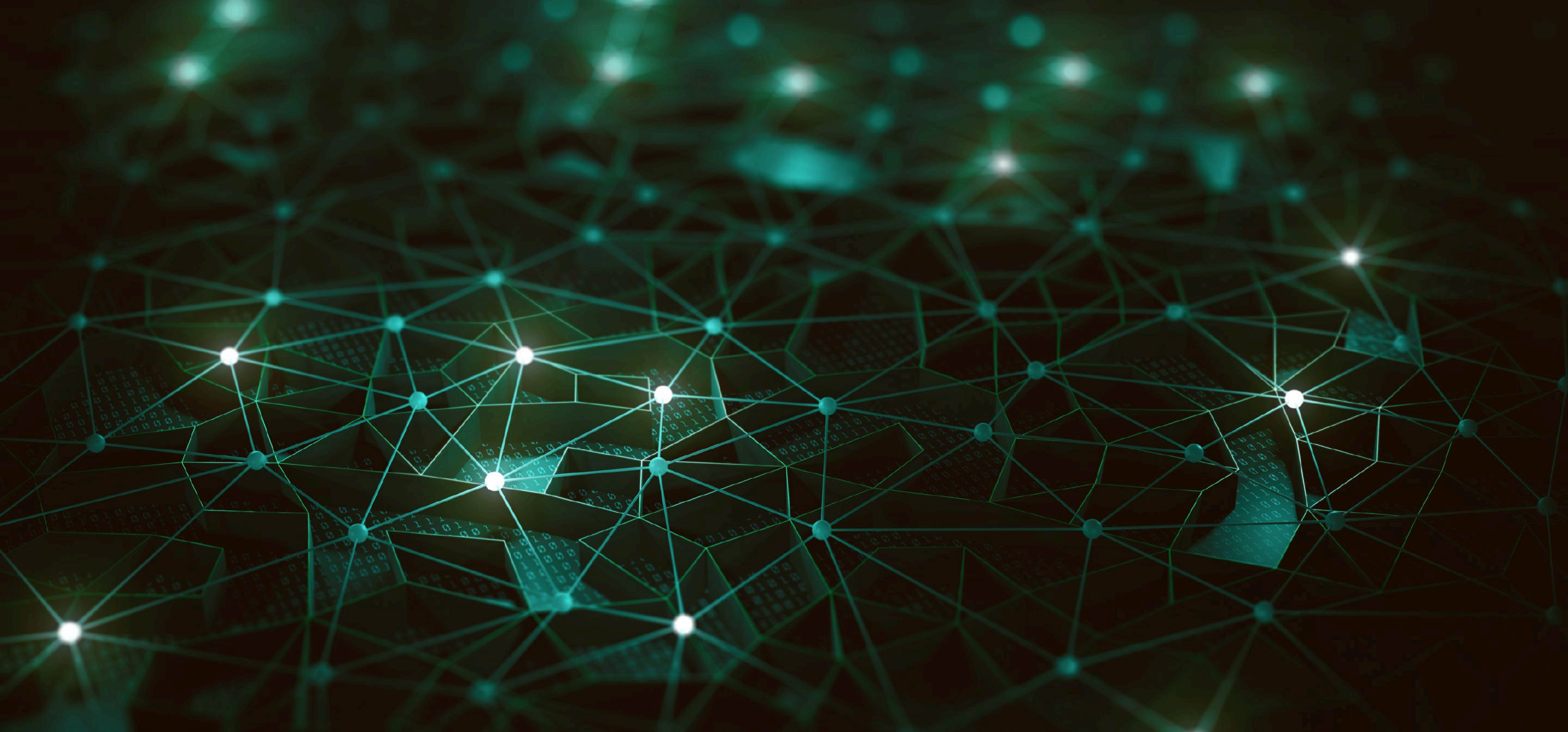


7

Provenance: is the package  
genuine?







**FAIR provides the solution.**





1

Updates and installs no longer depend on WordPress.org.






2

Many repositories, not one.  
You choose what you trust.





# Everything In

# Moderation

3 Baseline moderation. Optional  
external. Safe, cautious federation.





4

Domainname validation.  
Globally unique IDs.





# Data Privacy



5

Analytics without update-check  
telemetry or data harvesting.



# Components of FAIR



# FAIR Connect

Connect your site to FAIR.  
Independence tools built in.





# FAIR Beacon

Distribute your plugin or  
theme through FAIR.





# AspireCloud

A mirror of .org, evolving  
into FAIR's discovery layer.





# FAIR Explorer

A public directory of all  
FAIR-indexed packages.







**WHAT'S  
NEXT?**




# Currently architecting:

- Analytics service
- Moderation services
- More documentation





A close-up photograph of a piece of brown, textured paper that has been torn. The tear is irregular and jagged, revealing a white surface underneath. The word "Governance" is printed in a black, serif font on the white surface. The brown paper has a fibrous texture and is slightly wrinkled. The lighting is even, highlighting the texture of the paper and the sharp edges of the tear.

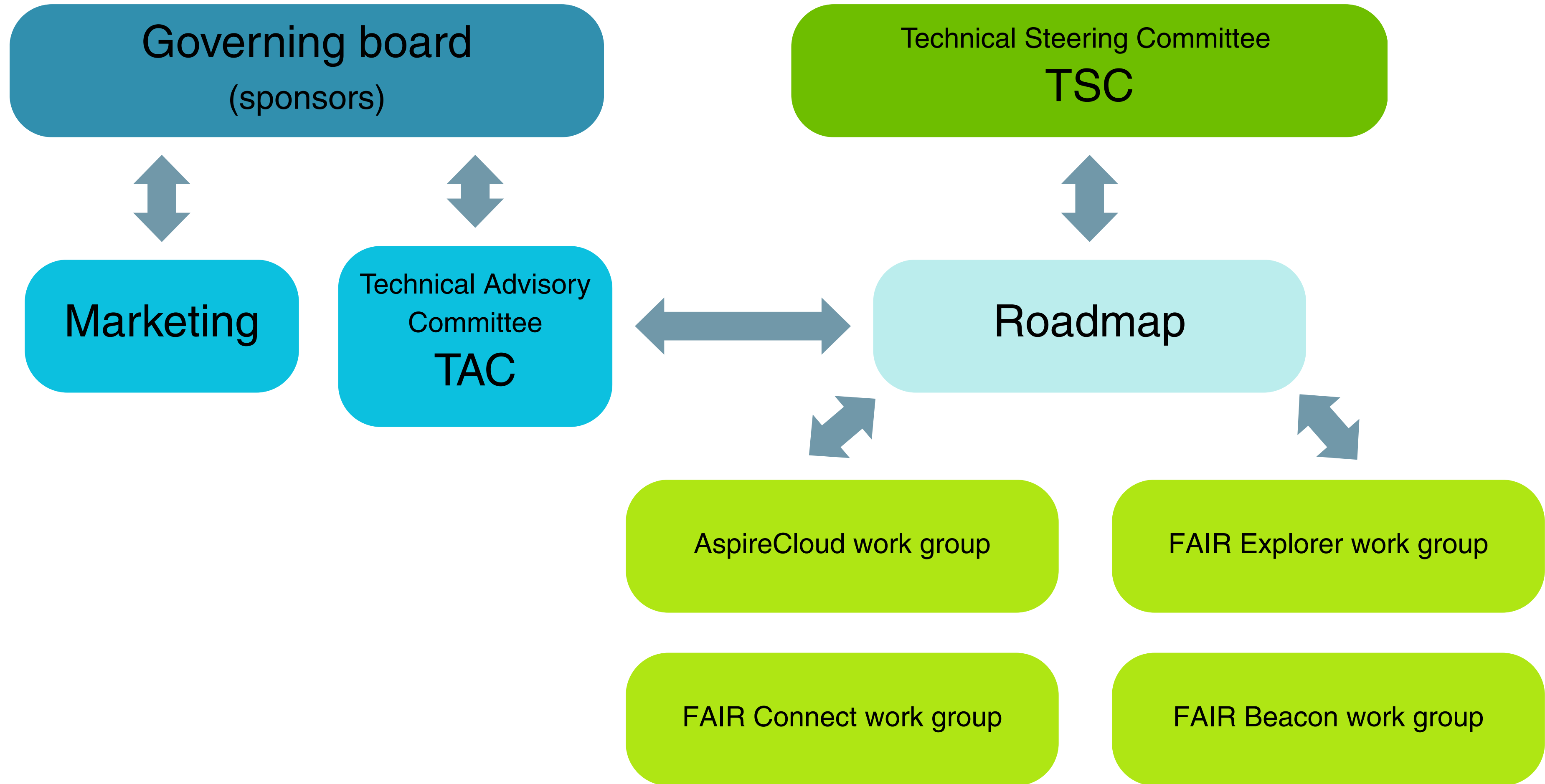
Governance



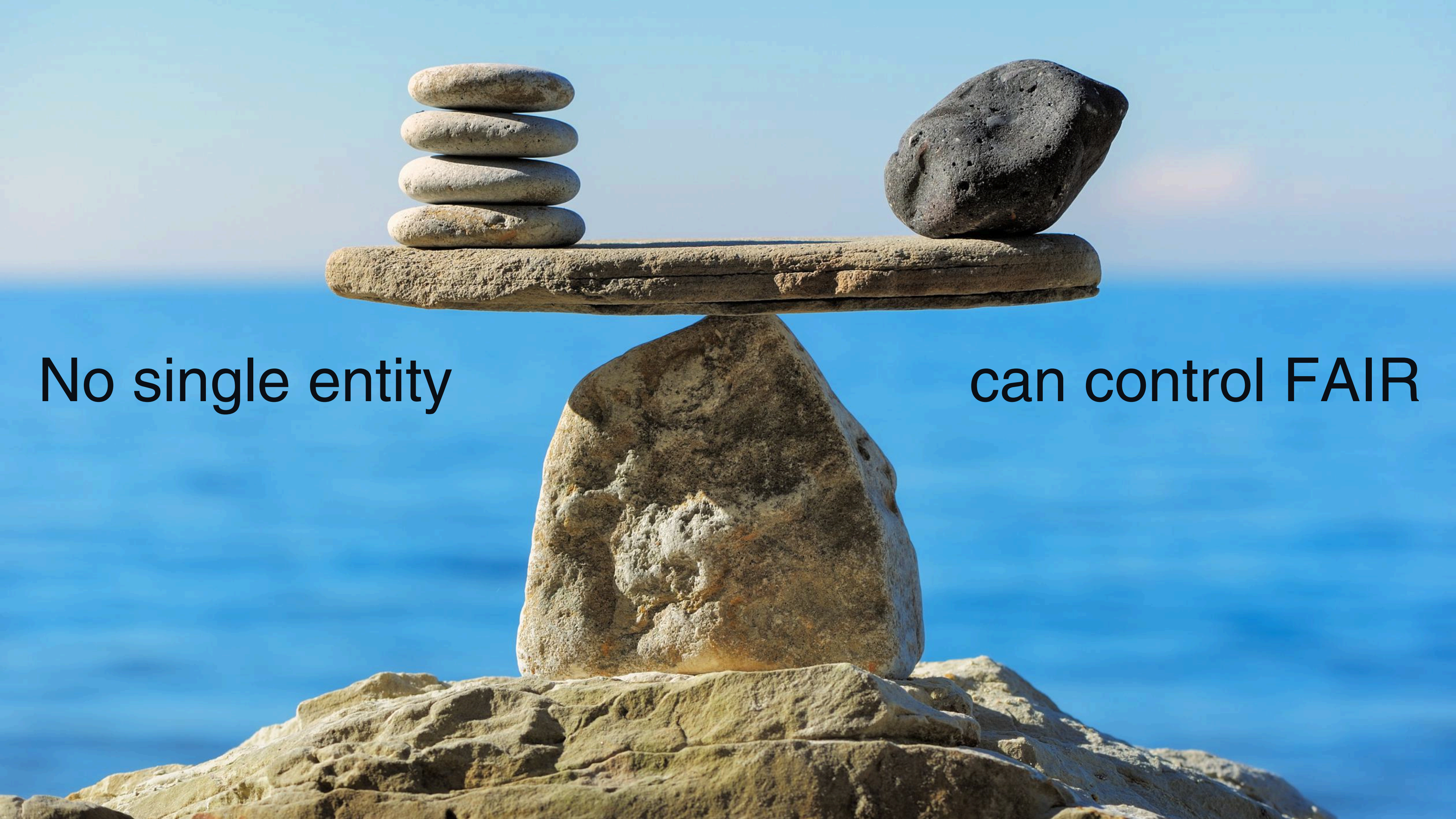


FAIR is governed openly under  
the Linux Foundation









No single entity

can control FAIR



# JOIN US

Web: [fair.pm](https://fair.pm)

Slack: [chat.fair.pm](https://chat.fair.pm)

GitHub: [github.com/fairpm](https://github.com/fairpm)