ActivityPub, the Fediverse and Decentralized IDs

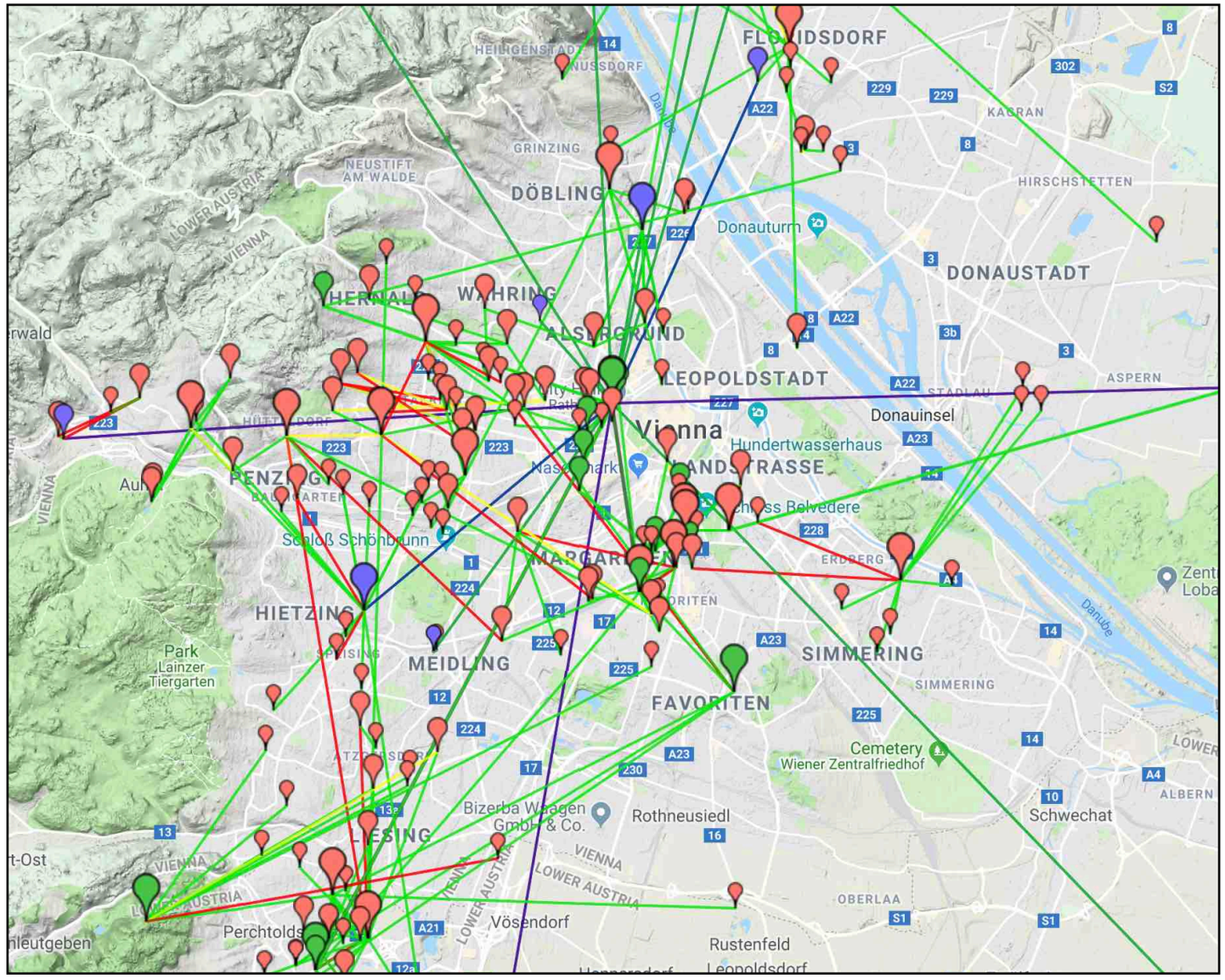
Paul Fuxjaeger
@cypherhippie@chaos.social
Wireless Battlemesh v12 2019 Paris

OPEN SOCIETY

NEEDS

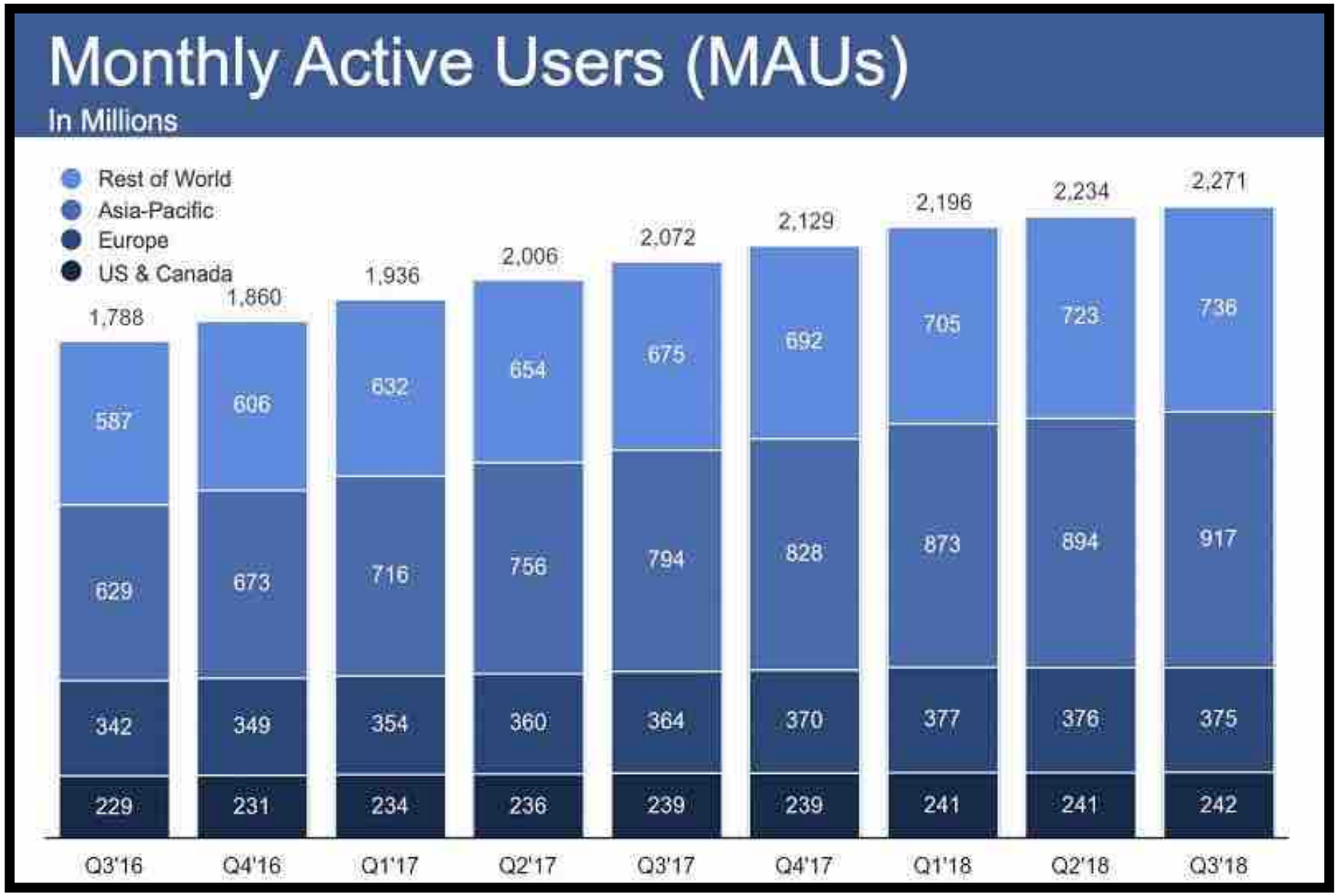
OPEN COMMUNICATION

Funkfeuer.at



A OLSR-based mesh over Vienna with ~200 nodes

PLATFORM ZOMBIE APOCALYPSE



0 days since last facebook scandal

https://the-federation.info

Projects

Project	Nodes	Users	Website	Code
Mastodon	2,711	2,126,748	joinmastodon.org	AGPLv3
Pleroma	482	28,134	pleroma.social	AGPLv3
PeerTube	322	11,291	joinpeertube.org	AGPLv3
diaspora*	247	701,749	diasporafoundation.org	AGPLv3
Matrix (Synapse)	239		matrix.org	Apache 2.0
Write Freely	134	2,930	writefreely.org	AGPLv3
Friendica	110	14,288	friendi.ca	AGPLv3
Hubzilla	105	6,023	hubzilla.org	MIT
PixelFed	61	8,785	pixelfed.org	AGPLv3
Misskey	54	18	misskey.xyz	AGPLv3
WordPress	29	130	wordpress.org	GPLv2
ActivityRelay	27	19	git.pleroma.social/pleroma/relay	AGPLv3
Funkwhale	21	1,588	funkwhale.audio	AGPLv3
Plume	18	797	joinplu.me	AGPLv3
Osada	7	81	zotlabs.com/osada	MIT
Socialhome	7	1,032	socialhome.network	AGPLv3
Prismo	5	173	gitlab.com/mbajur/prismo	AGPLv3
GNU social	4	35	gnu.io/social	AGPLv3

BRAND NEW!

Lemmy - reddit clone for the fediverse

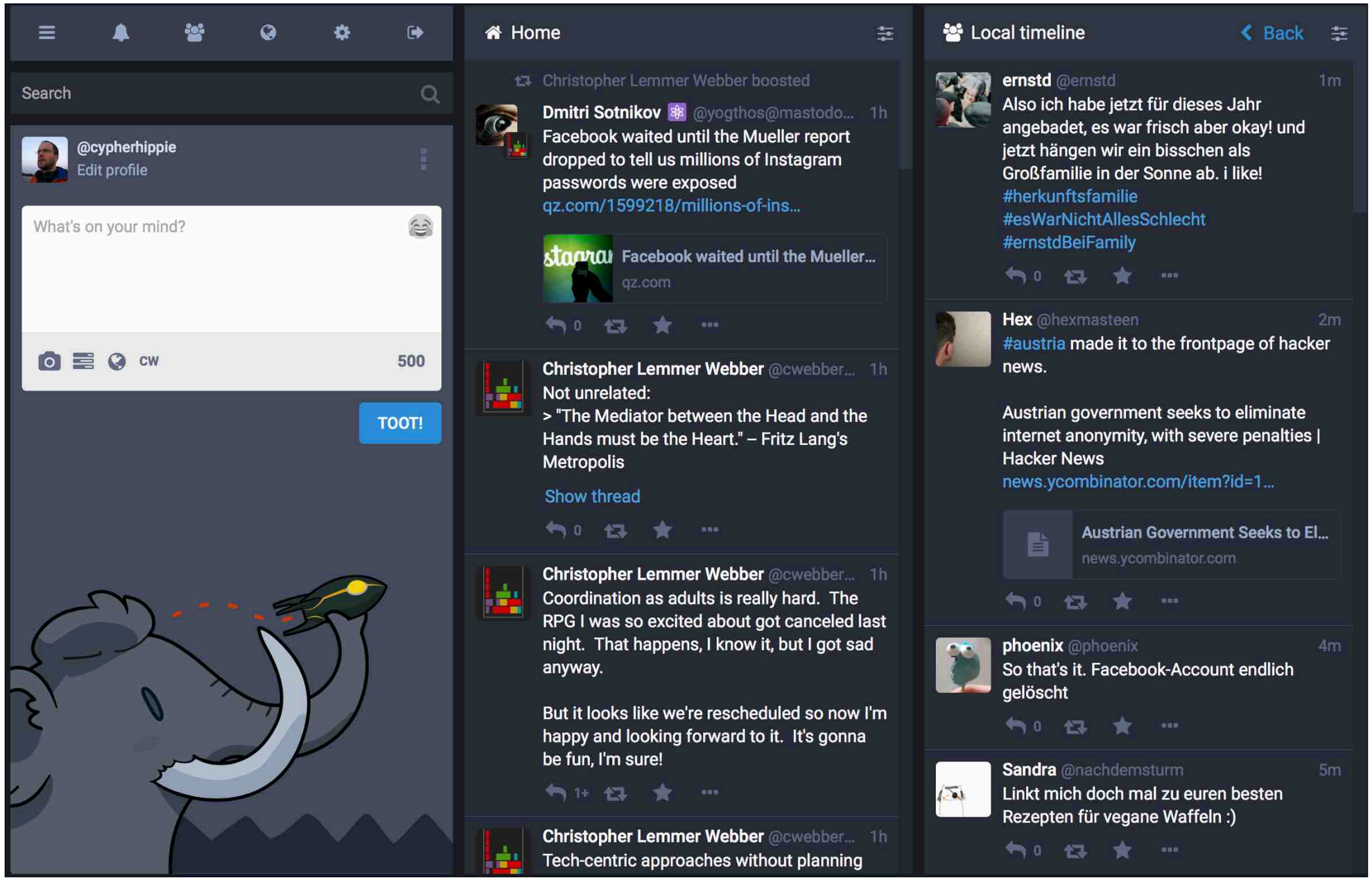
https://github.com/dessalines/lemmy

https://the-federation.info

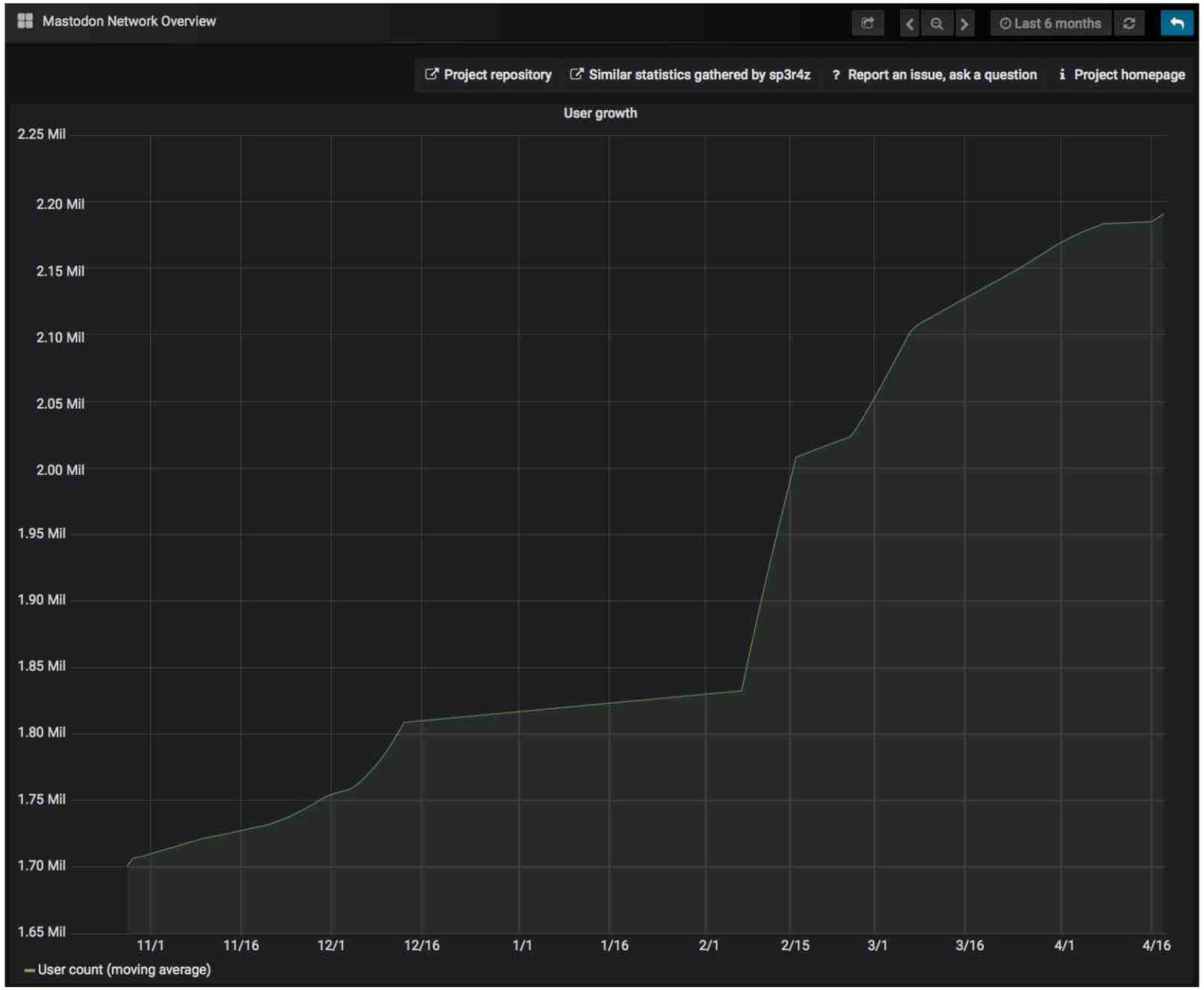
Protocols

Protocol	Nodes	Users
activitypub	3,840	2,197,189
ostatus	3,373	2,169,763
diaspora	464	718,452
matrix	235	
zot	117	6,133
dfrn	109	14,256
webmention	15	76
microformats	1	1
smtp	1	17,978
xmpp	1	17,978
micropub	1	1
vouch	1	1

Mastodon Rocks!

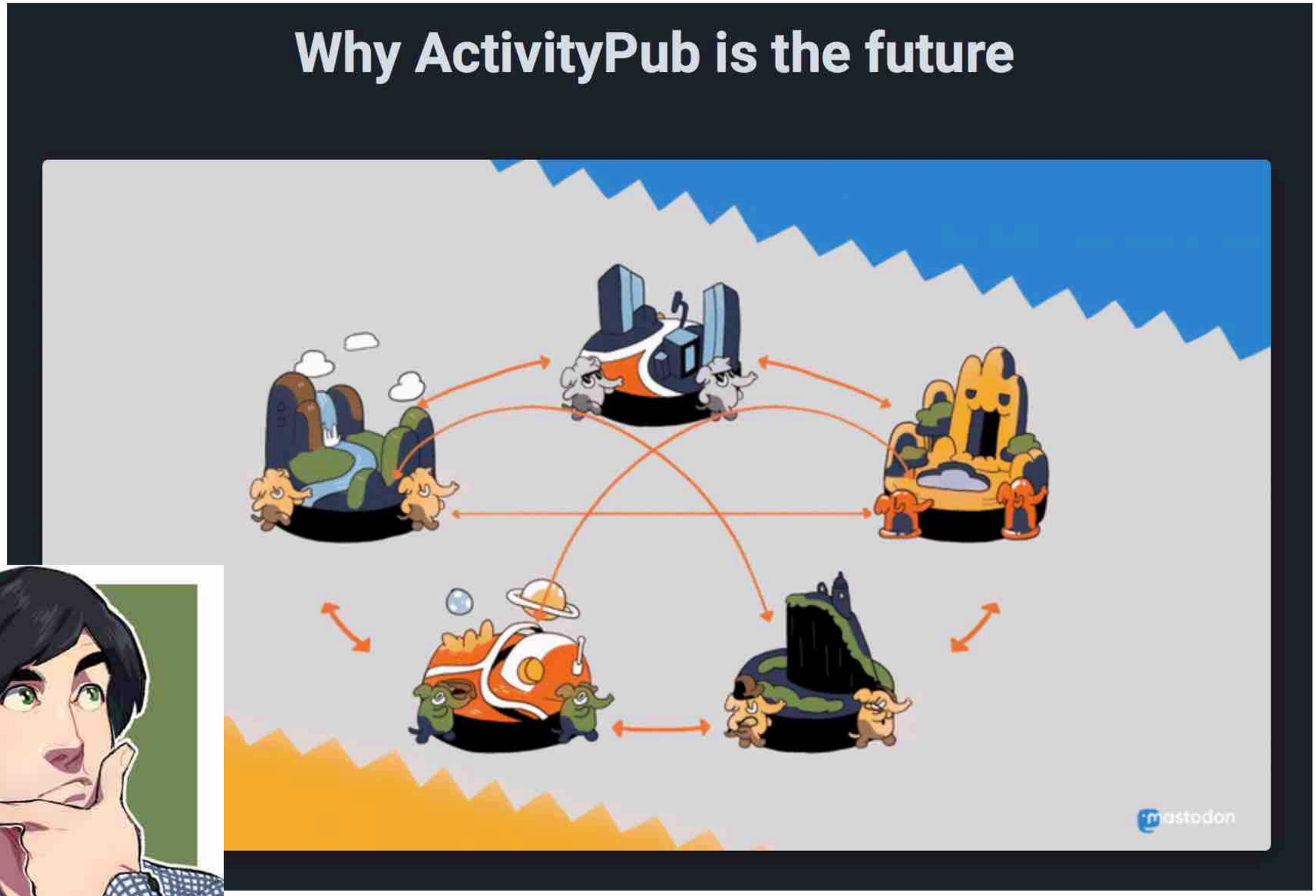


“User Growth”



https://mnm.social

Mastodon



https://blog.joinmastodon.org

Eugen Rochko
@gargron@mastodon.social

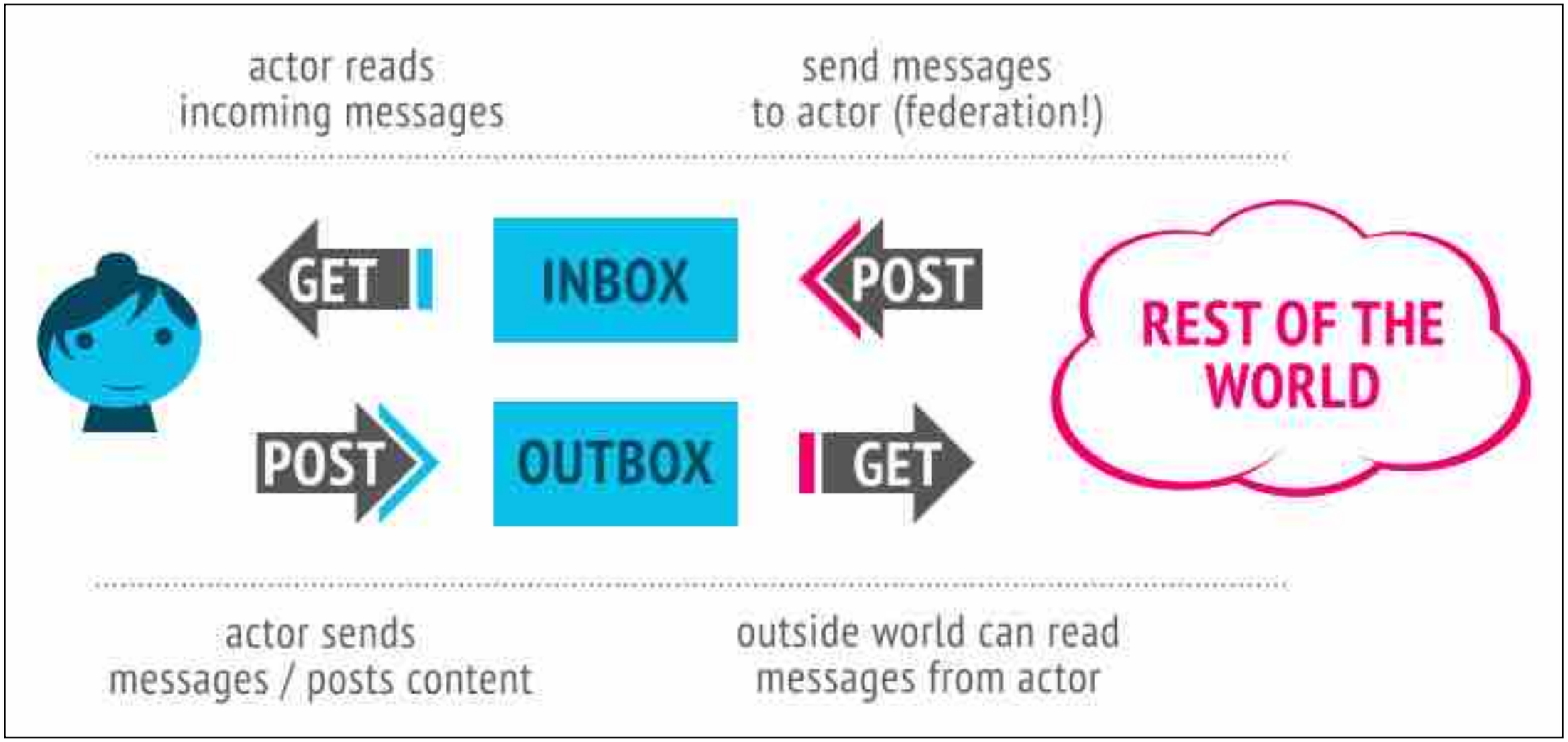
ActivityPub

ActivityPub reaches W3C Recommendation status! Everybody party!

Christopher Allan Webber -- Tue 20 March 2018

https://activitypub.rocks

What is ActivityPub?



Decentralized & Extensible
Social Networking Protocol

“Inbox”

https://<hostname>/users/<username>/inbox

Read access is owner-only
Write access is public*

“Outbox”

https://<hostname>/users/<username>/outbox

Read access is public*
Write access owner-only

+ Basic vocabulary for activities, done by actors, on objects

Why JSON-LD?

This is a toot posted to inbox on server of a “following” actor:


```
"@context": [
    "https://www.w3.org/ns/activitystreams",
    "https://w3id.org/security/v1",
    {
        "manuallyApprovesFollowers": "as:manuallyApprovesFollowers",
        "sensitive": "as:sensitive",
        "movedTo": {
            "@id": "as:movedTo",
            "@type": "@id"
        },
        "alsoKnownAs": {
            "@id": "as:alsoKnownAs",
            "@type": "@id"
        },
        "Hashtag": "as:Hashtag",
        "ostatus": "http://ostatus.org#",
        "atomUri": "ostatus:atomUri",
        "inReplyToAtomUri": "ostatus:inReplyToAtomUri",
        "conversation": "ostatus:conversation",
        "toot": "http://joinmastodon.org/ns#",
        "Emoji": "toot:Emoji",
        "focalPoint": {
            "@container": "@list",
            "@id": "toot:focalPoint"
        },
        "featured": {
            "@id": "toot:featured",
            "@type": "@id"
        },
        "schema": "http://schema.org#",
        "PropertyValue": "schema:PropertyValue",
        "value": "schema:value"
    }
],
```



```
"id": "http://node1/users/paul1/statuses/101823805578573700/activity",
"type": "Create",
"actor": "http://node1/users/paul1",
"published": "2019-03-27T17:32:50Z",
"to": [
    "https://www.w3.org/ns/activitystreams#Public"
],
"cc": [
    "http://node1/users/paul1/followers"
],
"object": {
    "id": "http://node1/users/paul1/statuses/101823805578573700",
    "type": "Note",
    "summary": null,
    "inReplyTo": null,
    "published": "2019-03-27T17:32:50Z",
    "url": "http://node1/@paul1/101823805578573700",
    "attributedTo": "http://node1/users/paul1",
    "to": [
        "https://www.w3.org/ns/activitystreams#Public"
    ],
    "cc": [
        "http://node1/users/paul1/followers"
    ],
    "sensitive": false,
    "atomUri": "http://node1/users/paul1/statuses/101823805578573700",
    "inReplyToAtomUri": null,
    "conversation": "tag:node1,2019-03-27:objectId=9:objectType=Conversation",
    "content": "<p>Hello Easterhegg 2019</p>",
    "contentMap": {
        "en": "<p>Hello Easterhegg 2019</p>"
    },
    "attachment": [],
    "tag": []
},
"signature": {
    "type": "RsaSignature2017",
    "creator": "http://node1/users/paul1#main-key",
    "created": "2019-03-27T17:32:50Z",
    "signatureValue": "Tnd3f8ip+4hHiKvG1IbihLtOARymeD+CpbVejdNFMgSX0LaCYk9BTs4A2s
}
```

Christopher Lemmer Webber
@cwebber@octodon.social

Check out this Podcast!

https://librelounge.org

Welcome to the Mastodon Monitoring Project

We're here to monitor the Mastodon Network and offer publicly available and easily browsable metrics about Mastodon.

Check-out our pretty dashboards to start diving into the data.

If you want to get involved, report an issue or request a feature, please visit our repository.

Biggest instances of the Mastodon network

Instance	Users	Statuses	Country	Last fetched on	Detailed dashboard
pawoo.net	535379	28244282	Japan	2 minutes ago	Go to dashboard
mastodon.social	312297	13430945	Germany	2 minutes ago	Go to dashboard
mstdn.jp	190728	48384719	Japan	2 minutes ago	Go to dashboard
switter.at	118232	2306642	Austria	2 minutes ago	Go to dashboard
humblr.social	97886	2793302		2 minutes ago	Go to dashboard
mastodon.cloud	54222	2762673	Germany	2 minutes ago	Go to dashboard
friends.nico	48239	24021846	Japan	2 minutes ago	Go to dashboard
mastodon.xyz	20572	929470	France	2 minutes ago	Go to dashboard
social.cloudfrancois.fr	20042	819	France	1 year, 12 months ago	Go to dashboard
sinblr.com	18605	417933		2 minutes ago	Go to dashboard

Browse all 6653 instances

https://mnm.social

Reflections: The ecosystem is moving

moxie0 on 10 May 2016

At Open Whisper Systems, we've been developing open source "consumer-facing" software for the past four years. We want to share some of the things we've learned while doing it.

As a software developer, I envy writers, musicians, and filmmakers. Unlike software, when they create something, it is really done — forever. A recorded album can be just the same 20 years later, but software has to change.

Software exists as part of an ecosystem, and **the ecosystem is moving**. The platform changes out from under it, the networks evolve, security threats and countermeasures are in constant shift, and the collective UX language rarely sits still. As more money, time, and focus has gone into the ecosystem, the faster the whole thing has begun to travel.

https://signal.org/blog/the-ecosystem-is-moving/

Facebook is a classic example of Metcalfe's law

Every new user connecting to other peers in the network (peer-to-peer) non-linearly increases the number of connections

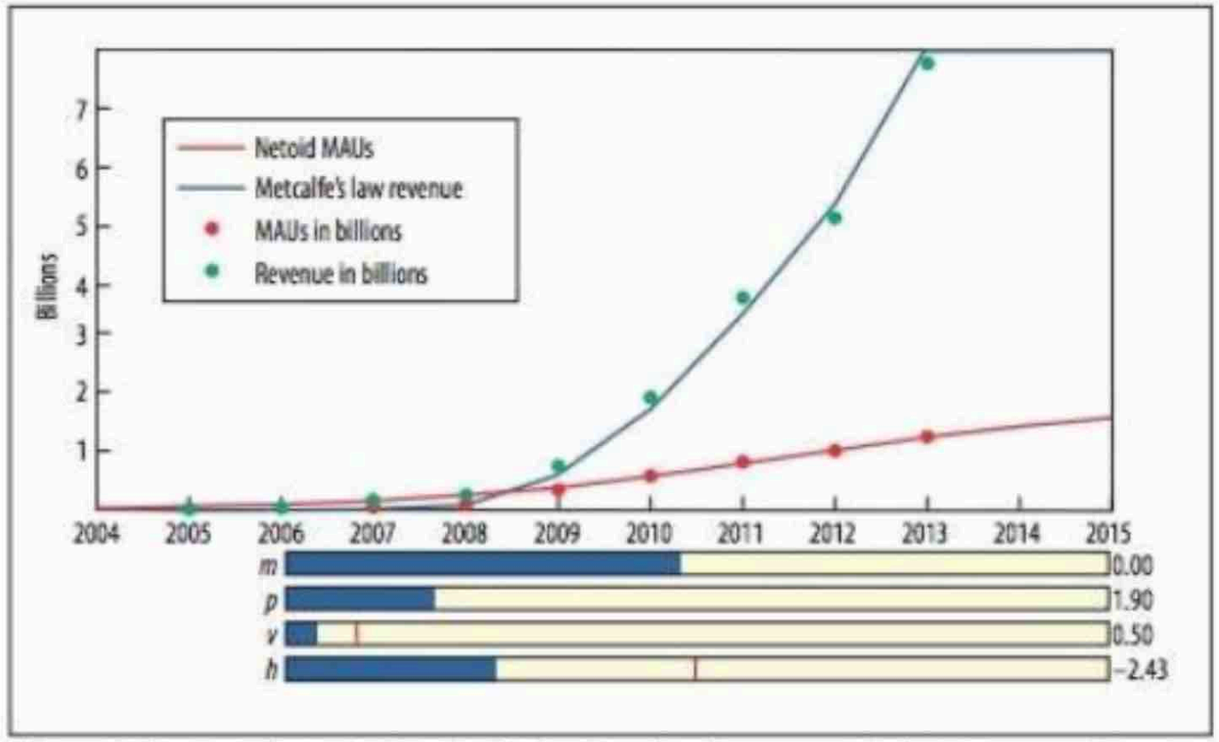


Figure 4. The netoid can be closely fitted to Facebook user growth data, measured in terms of monthly average users (MAUs), and Metcalfe's law can be closely fitted to Facebook's associated revenue data.

Source: Bob Metcalfe/ IEEE Computer 2013, via Bill Krause

Rebooting the Web-of-Trust

Current Web-of-Trust

Executive Summary

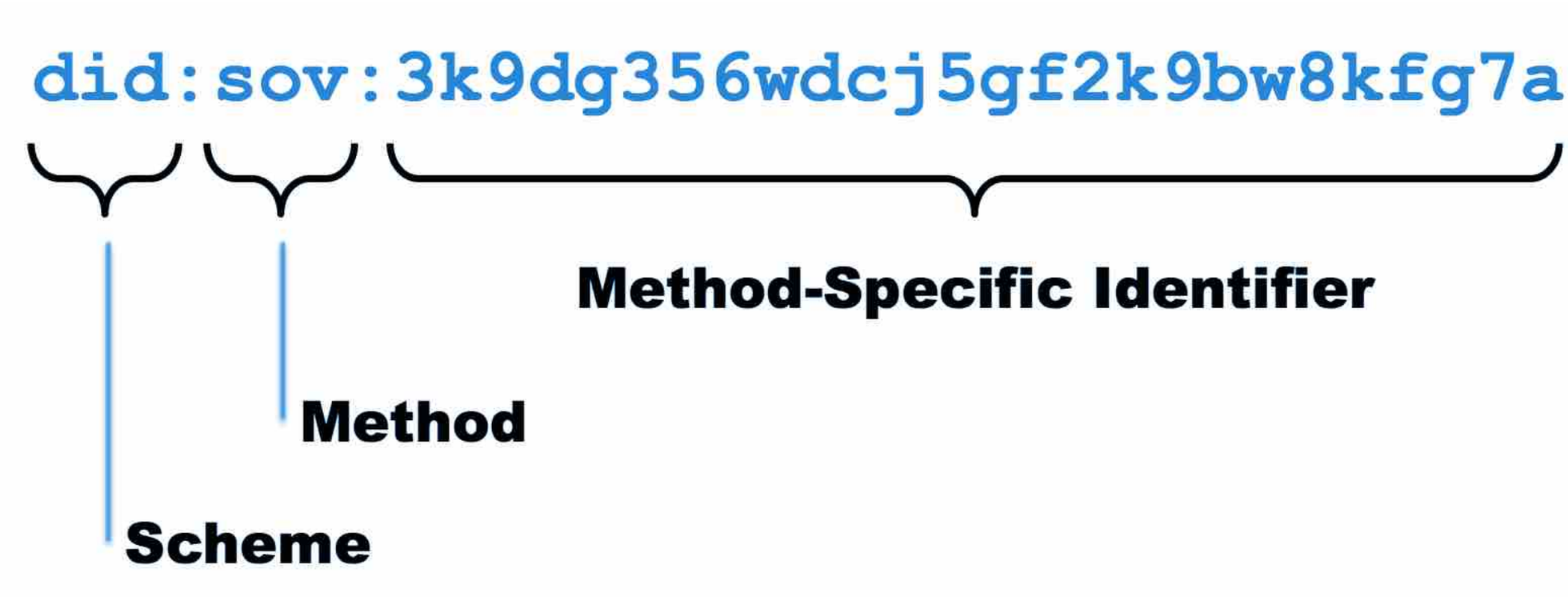
In the last week of June 2019 unknown actors deployed a certificate spamming attack against two high-profile contributors in the OpenPGP community (Robert J. Hansen and Daniel Kahn Gillmor, better known in the community as "rjh" and "dkg"). This attack exploited a defect in the OpenPGP protocol itself in order to "poison" rjh and dkg's OpenPGP certificates. Anyone who attempts to import a poisoned certificate into a vulnerable OpenPGP installation will very likely break their installation in hard-to-debug ways. Poisoned certificates are already on the SKS keyserver network. There is no reason to believe the attacker will stop at just poisoning two certificates. Further, given the ease of the attack and the highly publicized success of the attack, it is prudent to believe other certificates will soon be poisoned.

This attack cannot be mitigated by the SKS keyserver network in any reasonable time period. It is unlikely to be mitigated by the OpenPGP Working Group in any reasonable time period. Future releases of OpenPGP software will likely have some sort of mitigation, but there is no time frame. The best mitigation that can be applied at present is simple: stop retrieving data from the SKS keyserver network.

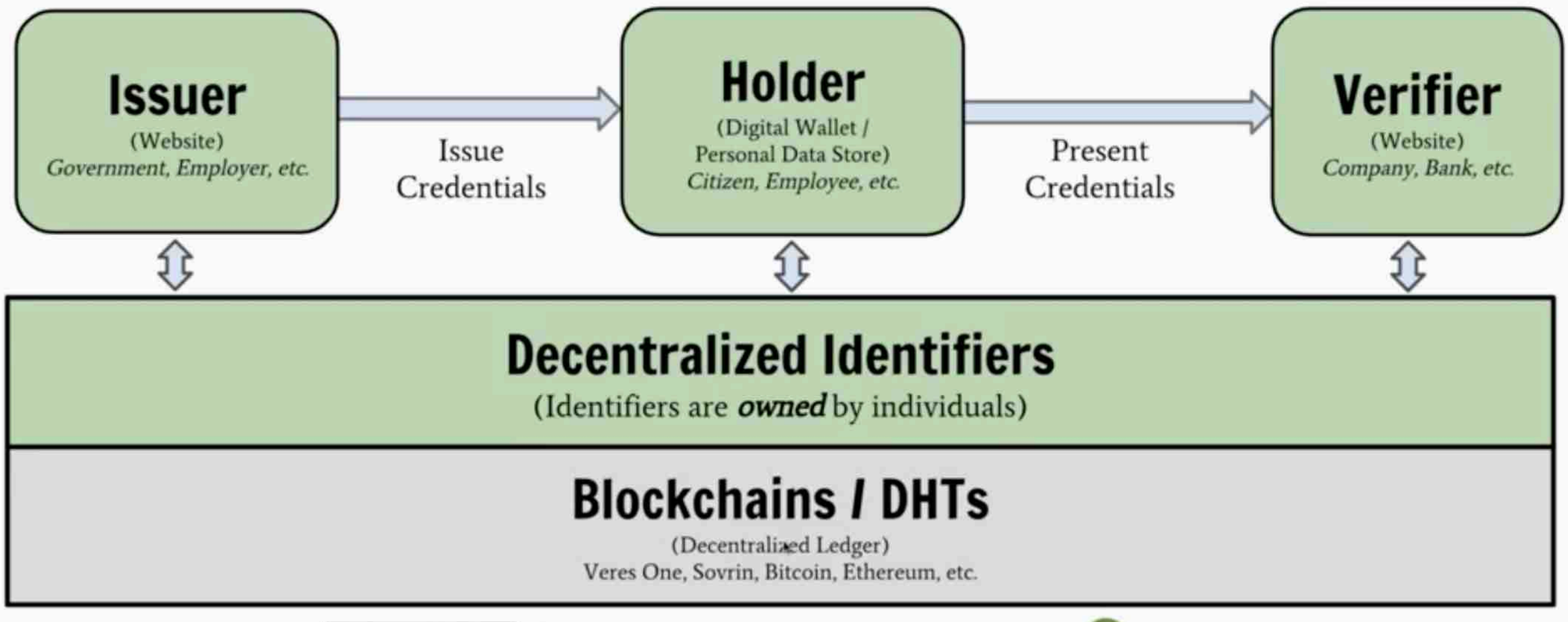
https://gist.github.com/rjhansen

DID

Decentralized Identifier



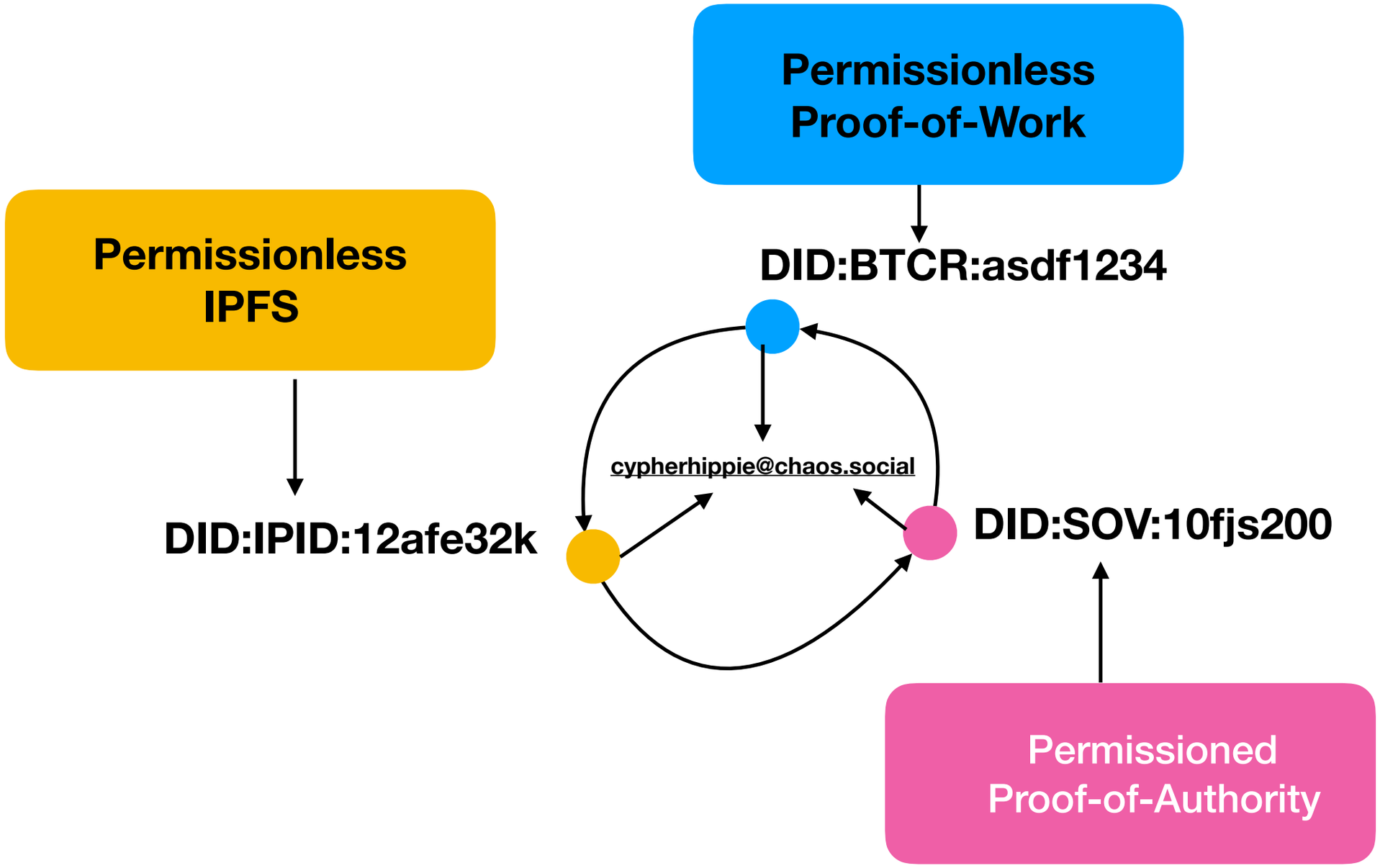
Decentralized Identifiers



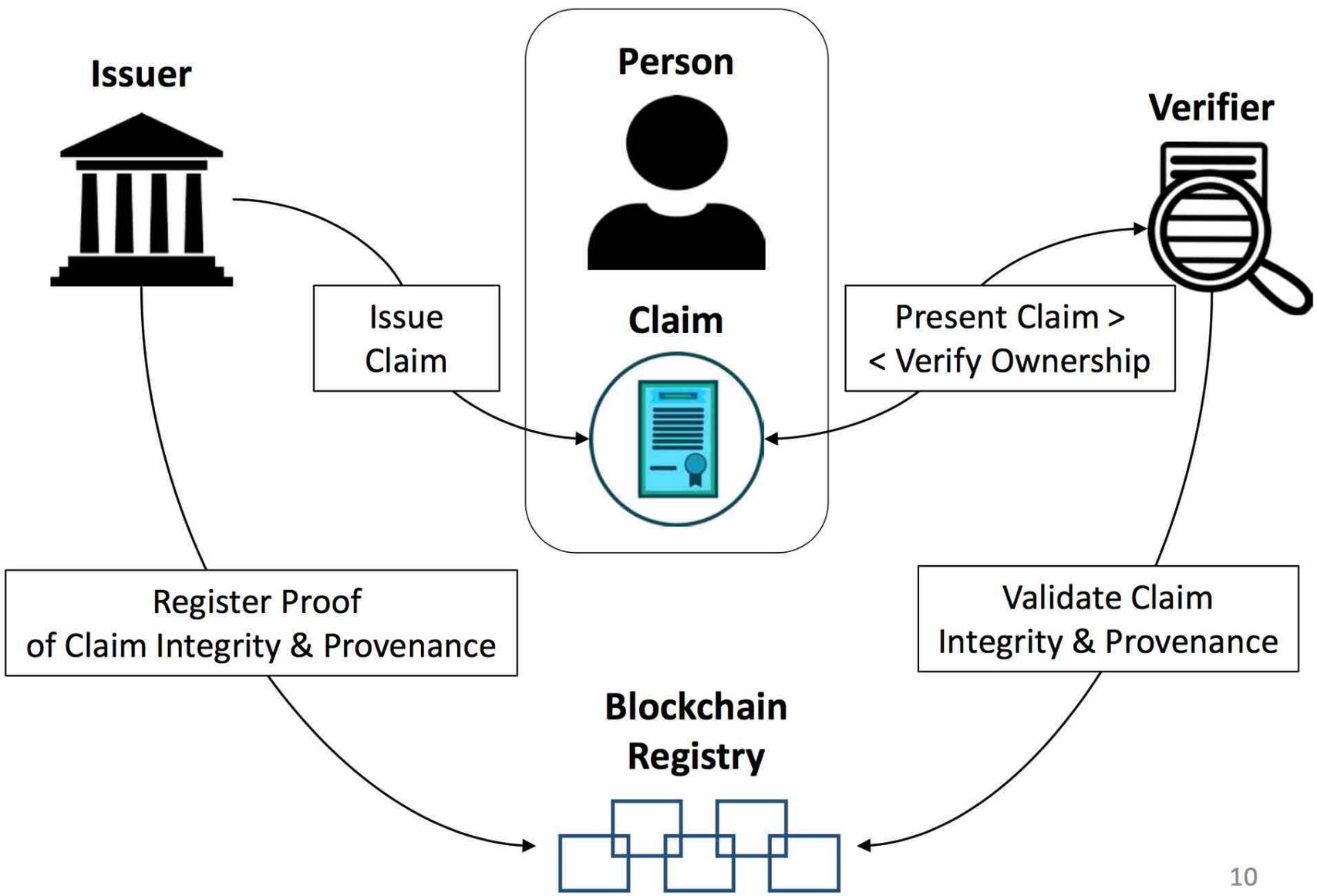
SSIMeetup.org

Method	DID Prefix
Sovrin	`did:sov:`
Veres One	`did:v1:`
uPort	`did:uport:`
Bitcoin	`did:btcr:`
Blockstack	`did:stack:`
ERC725	`did:erc725:`
IPFS	`did:ipid:`

DIDs are Agnostic to Ledger/Database


Permissionless
Proof-of-Work
DID:BTCR:asdf1234
Permissionless
IPFS
cypherhippie@chaos.social
DID:IPID:12afe32k
DID:SOV:10fjs200
Permissioned
Proof-of-Authority

Verifiable Claims



There was a time when…

… we didn’t have **Postal Addresses**

… we didn’t have **Telephone Numbers**

… we didn’t have **IP Addresses**

… we didn’t have **Domain Names**

… we didn’t have **Decentralized IDs**

…

Technological Development

Technological Development

Our World Needs More

ActivityPub Enthousiast

SovereignID

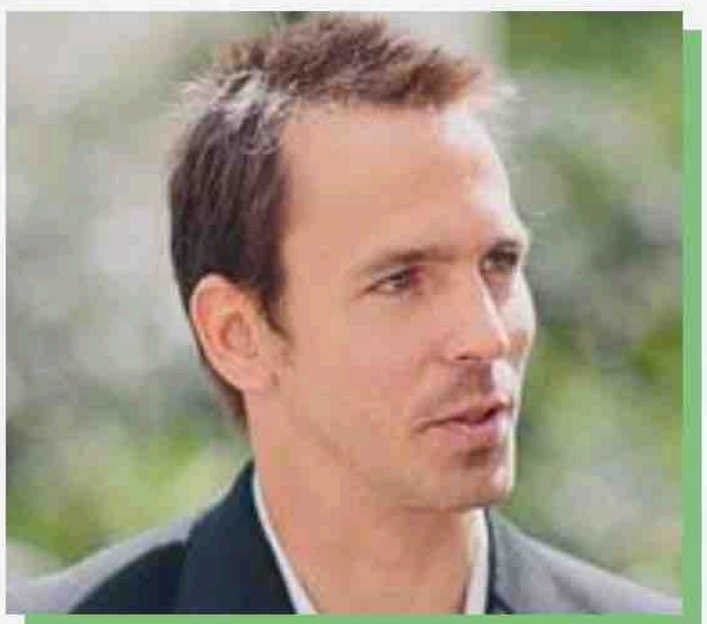
PERSONEN

Markus Sabadello

PERSONEN

Paul Fuxjäger

PERSONEN



Michael Pimmer

netidee
OPEN INNOVATIONS