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
## Projects

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

**Lemmy - reddit clone for the fediverse**

[https://github.com/dessalines/lemmy](https://github.com/dessalines/lemmy)
https://the-federation.info

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Nodes</th>
<th>Users</th>
</tr>
</thead>
<tbody>
<tr>
<td>activitypub</td>
<td>3,840</td>
<td>2,197,189</td>
</tr>
<tr>
<td>ostatus</td>
<td>3,373</td>
<td>2,169,763</td>
</tr>
<tr>
<td>diaspora</td>
<td>464</td>
<td>718,452</td>
</tr>
<tr>
<td>matrix</td>
<td>235</td>
<td></td>
</tr>
<tr>
<td>zot</td>
<td>117</td>
<td>6,133</td>
</tr>
<tr>
<td>dfrn</td>
<td>109</td>
<td>14,256</td>
</tr>
<tr>
<td>webmention</td>
<td>15</td>
<td>76</td>
</tr>
<tr>
<td>microformats</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>smtp</td>
<td>1</td>
<td>17,978</td>
</tr>
<tr>
<td>xmpp</td>
<td>1</td>
<td>17,978</td>
</tr>
<tr>
<td>micropub</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>vouch</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>
Mastodon Rocks!
“User Growth”

https://mnm.social
Mastodon

Why ActivityPub is the future

https://blog.joinmastodon.org

Eugen Rochko
@gargon@mastodon.social
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",    
    "moveTo": {    
      "@id": "as:moveTo",    
      "@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:object109:objectType=Conversation",
    "content": "&lt;p&gt;Hello Easterhegg 2019&lt;/p&gt;",
    "contentMap": {
      "en": "&lt;p&gt;Hello Easterhegg 2019&lt;/p&gt;"
    },    
    "attachment": [],    
    "tag": []
  }
},
"signature": {
  "type": "RsaSignature2017",
  "creator": "http://node1/users/paul1#main-key",
  "created": "2019-03-27T17:32:50Z",
  "signatureValue": "Tnd3fB1p43hlKvG1b1hLtOARymeD+CpVejdNFMg5X0LaCYK9BTs4A2z"}"
```
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

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

[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 keys server 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 keys server 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 keys server network.

https://gist.github.com/rjhansen
DID
Decentralized Identifier
Decentralized Identifiers

Issuer
(Website)
Government, Employer, etc.

Holder
(Digital Wallet / Personal Data Store)
Citizen, Employee, etc.

Verifier
(Website)
Company, Bank, etc.

Decentralized Identifiers
(Identifiers are owned by individuals)

Blockchains / DHTs
(Decentralized Ledger)
Veres One, Sovrin, Bitcoin, Ethereum, etc.

https://creativecommons.org/licenses/by-sa/4.0/
<table>
<thead>
<tr>
<th>Method</th>
<th>DID Prefix</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sovrin</td>
<td>did:sov:</td>
</tr>
<tr>
<td>Veres One</td>
<td>did:v1:</td>
</tr>
<tr>
<td>uPort</td>
<td>did:uport:</td>
</tr>
<tr>
<td>Bitcoin</td>
<td>did:btcr:</td>
</tr>
<tr>
<td>Blockstack</td>
<td>did:stack:</td>
</tr>
<tr>
<td>ERC725</td>
<td>did:erc725:</td>
</tr>
<tr>
<td>IPFS</td>
<td>did:ipid:</td>
</tr>
</tbody>
</table>

DIDs are Agnostic to Ledger/Database
Permissionless Proof-of-Work

DID:BTCR:asdf1234

cypherhippie@chaos.social

Permissionless IPFS

DID:IPID:12afe32k

DID:SOV:10fjs200

Permissioned Proof-of-Authority
Verifiable Claims

Issuer

Person

Claim

Verifier

Issue Claim

Present Claim > < Verify Ownership

Register Proof of Claim Integrity & Provenance

Validate Claim Integrity & Provenance

Blockchain Registry

10
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

...
Our World Needs More

Activity Pub Enthusiast