Matrix: Status update

@kitsune:matrix.org (https://matrix.to/#/@kitsune:matrix.org)
Twitter: @matrixdotorg, @aerusakov
https://matrix.org

[matrix]

Matrix is an open network for secure, decentralised real-time communication.

Interoperable chat

Interoperable VoIP

Open comms for VR/AR

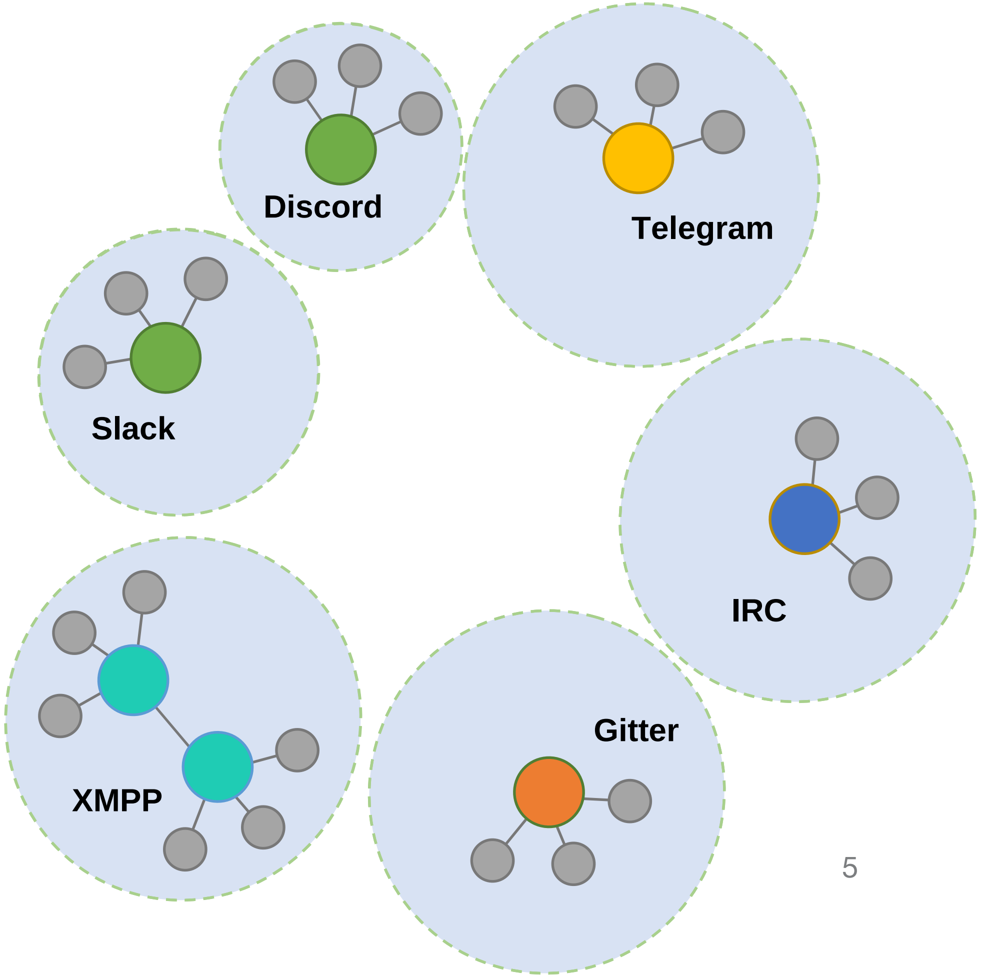
Real-time IoT data fabric

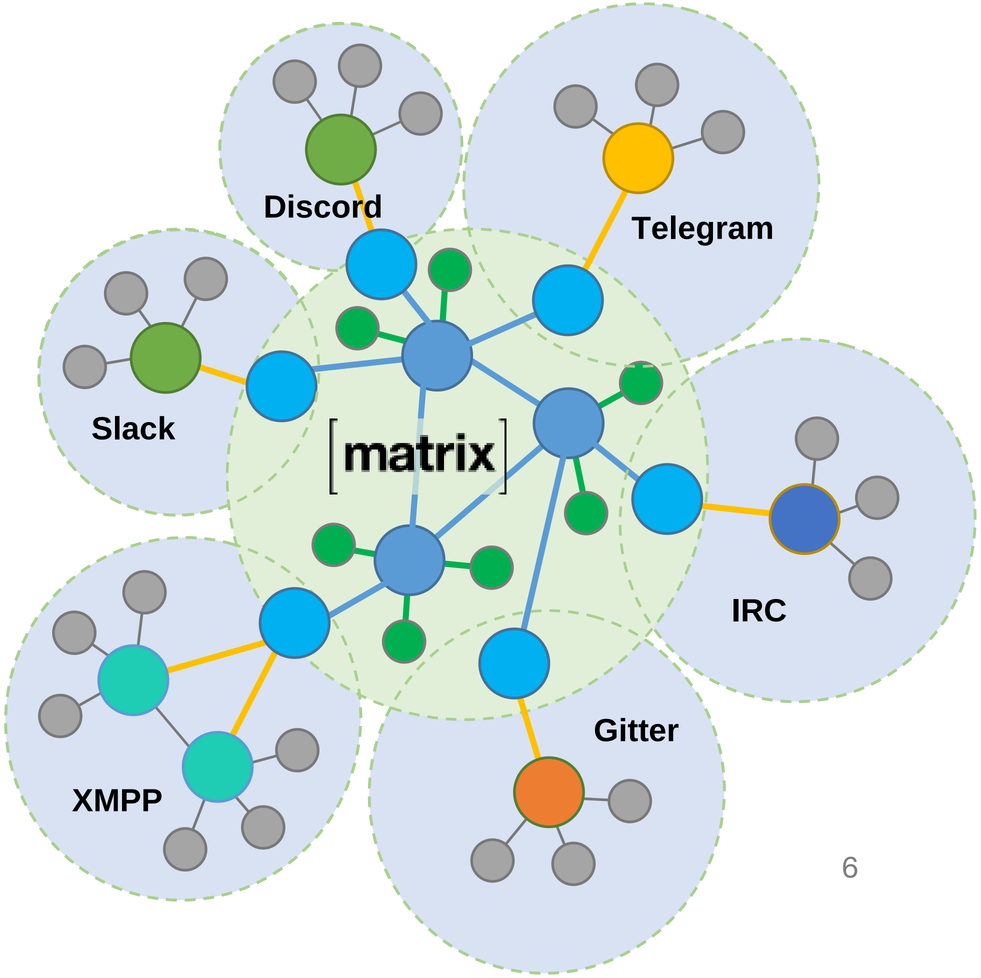
[matrix]

Mission: to create a global decentralised encrypted comms network that provides an open platform for real-time communication.

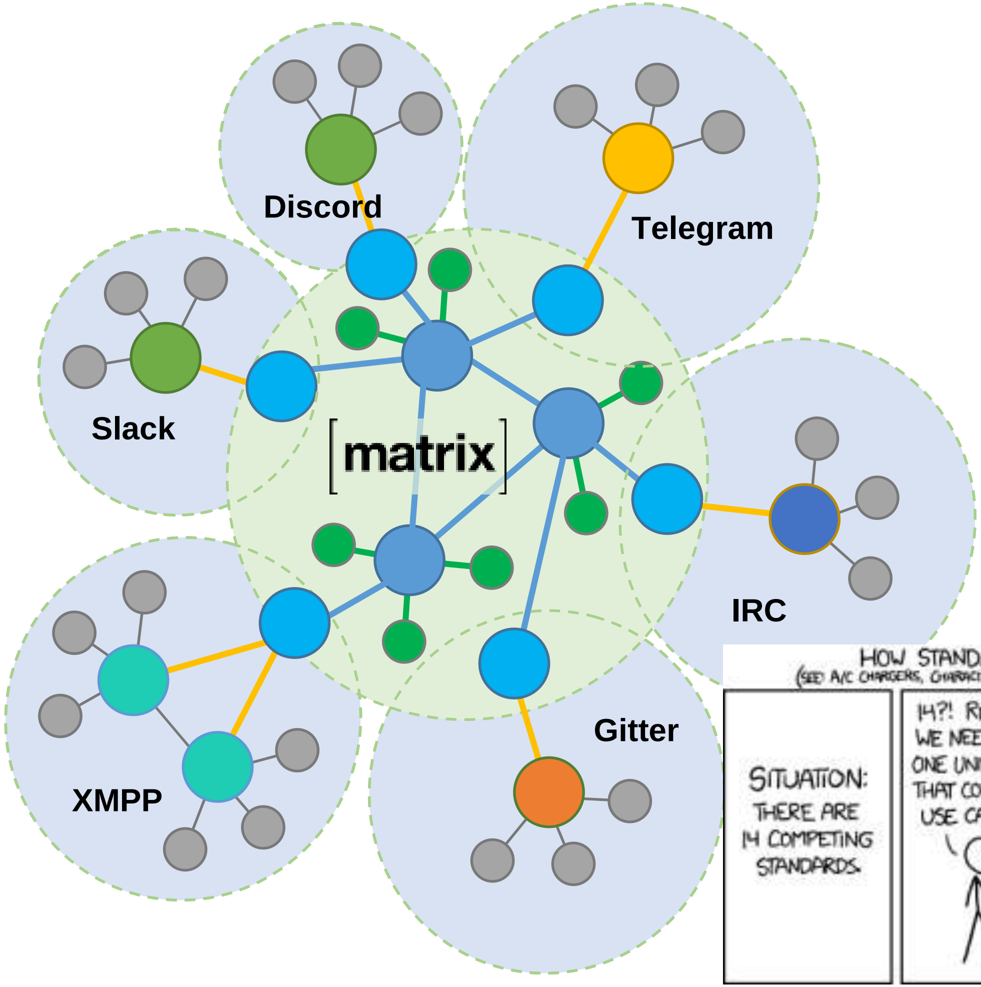
The Matrix Manifesto. We believe…

- People should have **full control** over their own communication.
- People should **not be locked into centralised silos**, but instead be free to pick who they choose to host their communication without limiting who they can reach.
- The ability to **converse securely and privately** is a basic human right.
- Communication should be available to everyone as a **free and open, unencumbered, standard** and global network.

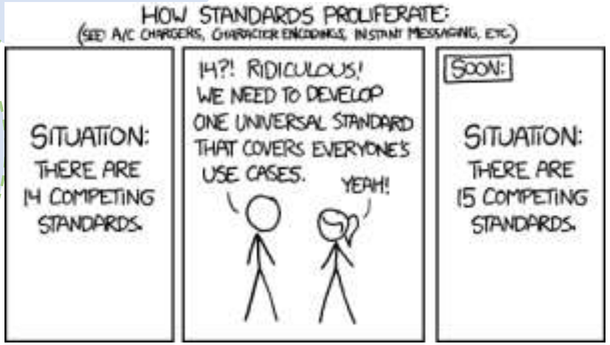

Discord
Telegram
Slack
IRC
XMPP
Gitter


Discord
Telegram
Slack
[matrix]
IRC
XMPP
Gitter

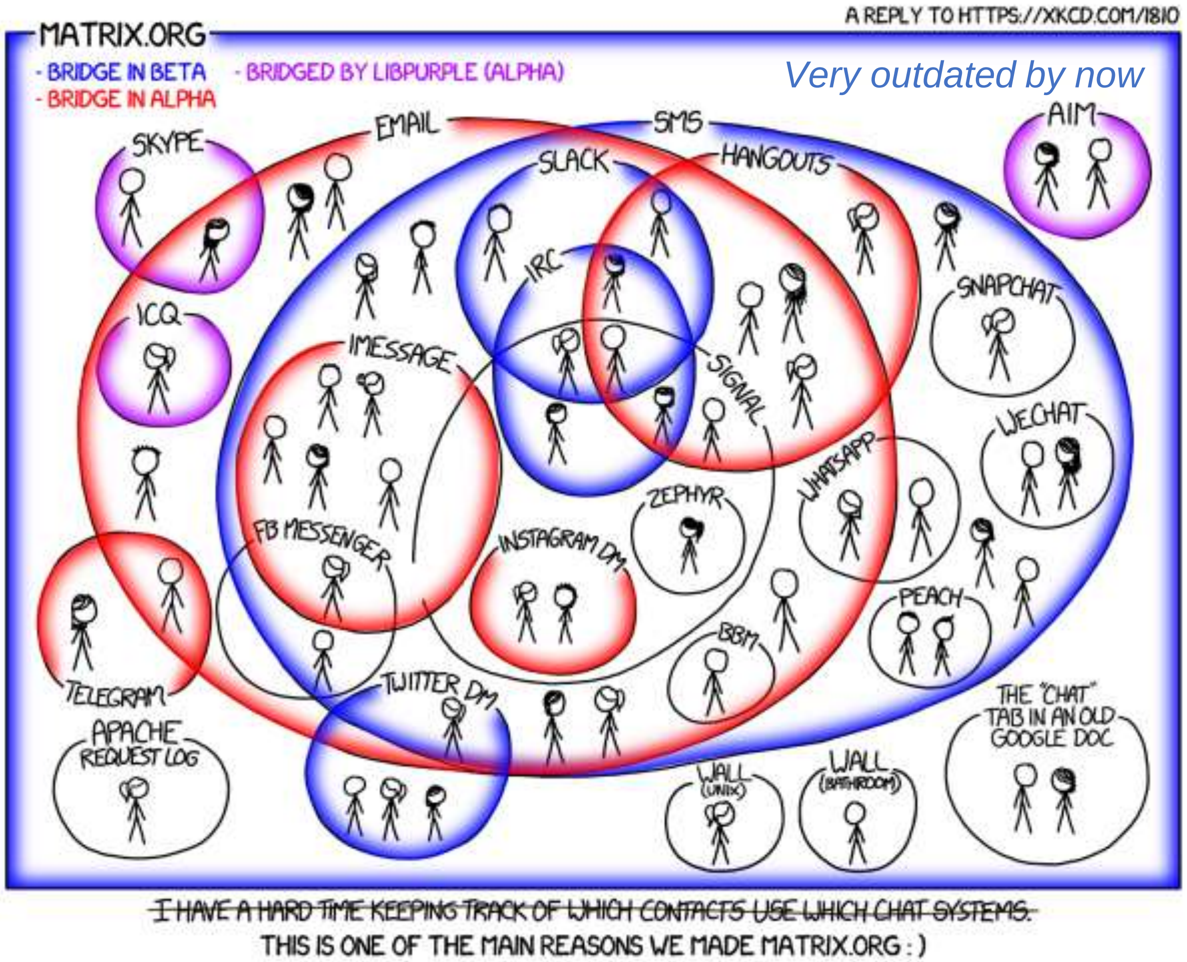
[matrix]



Discord
Telegram
Slack
[matrix]
IRC
XMPP
Gitter



HOW STANDARDS PROLIFERATE:
(SEE A/C CHARGERS, CHARACTER ENCODINGS, INSTANT MESSAGING, ETC.)
SITUATION: THERE ARE 14 COMPETING STANDARDS.
14?! RIDICULOUS! WE NEED TO DEVELOP ONE UNIVERSAL STANDARD THAT COVERS EVERYONE'S USE CASES.
YEAH!
SOON:
SITUATION: THERE ARE 15 COMPETING STANDARDS.


A REPLY TO HTTPS://XKCD.COM/1810
MATRIX.ORG
- BRIDGE IN BETA
- BRIDGE IN ALPHA
- BRIDGED BY LIBPURPLE (ALPHA)
EMAIL
SMS
SKYPE
SLACK
HANGOUTS
AIM
IRC
ICQ
SNAPCHAT
IMESSAGE
SIGNAL
WECHAT
WHATSAPP
ZEPHYR
FB MESSENGER
INSTAGRAM DM
PEACH
BBM
TELEGRAM
TWITTER DM
THE "CHAT" TAB IN AN OLD GOOGLE DOC
APACHE REQUEST LOG
WALL (UNIX)
WALL (BATHROOM)
~~I HAVE A HARD TIME KEEPING TRACK OF WHICH CONTACTS USE WHICH CHAT SYSTEMS.~~
THIS IS ONE OF THE MAIN REASONS WE MADE MATRIX.ORG :)

Very outdated by now

[matrix]

[matrix]

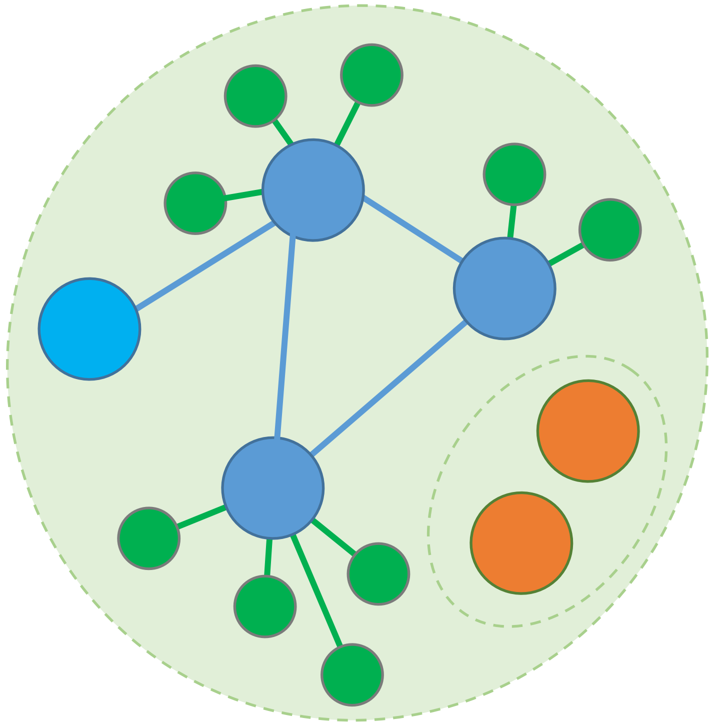
Matrix Architecture

● Clients

● Home Servers

● Application Servers

● Identity Servers



No single party owns your conversations.

Conversations are shared over all participants.

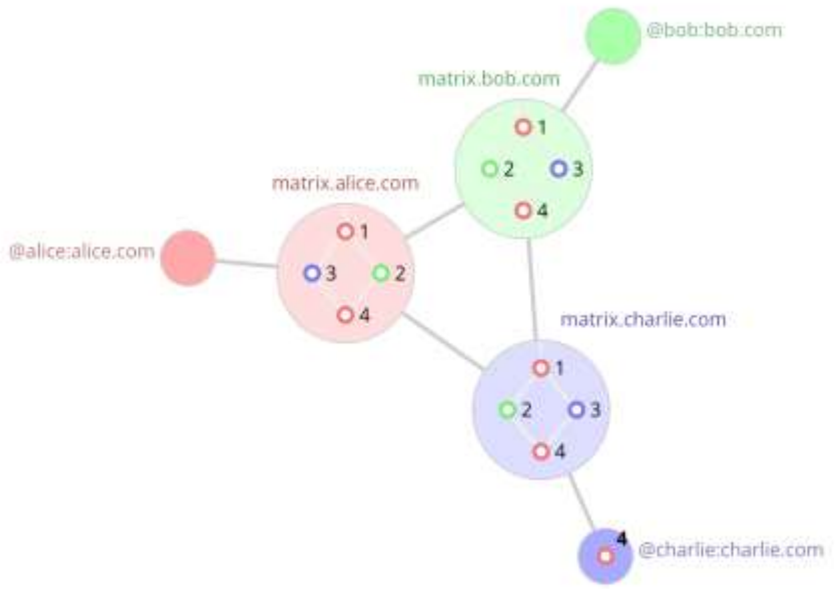
It’s like an permissionless blockchain… but for real-time comms

- Messages (‘events’) are stored in rooms
- Rooms are decentralised and replicated over all participating nodes, similar to a distributed ledger
- There are no PoW/PoS or doublespend protection however, as low latency is more important than consistency in real-time communications
- Transactions can be layered on top when needed
- Proofs are used for semantically important events (e.g. kicks, bans, ops)
- Consistency is gradual and eventual
- Optimises for the AP of CAP theorem

How does it work?

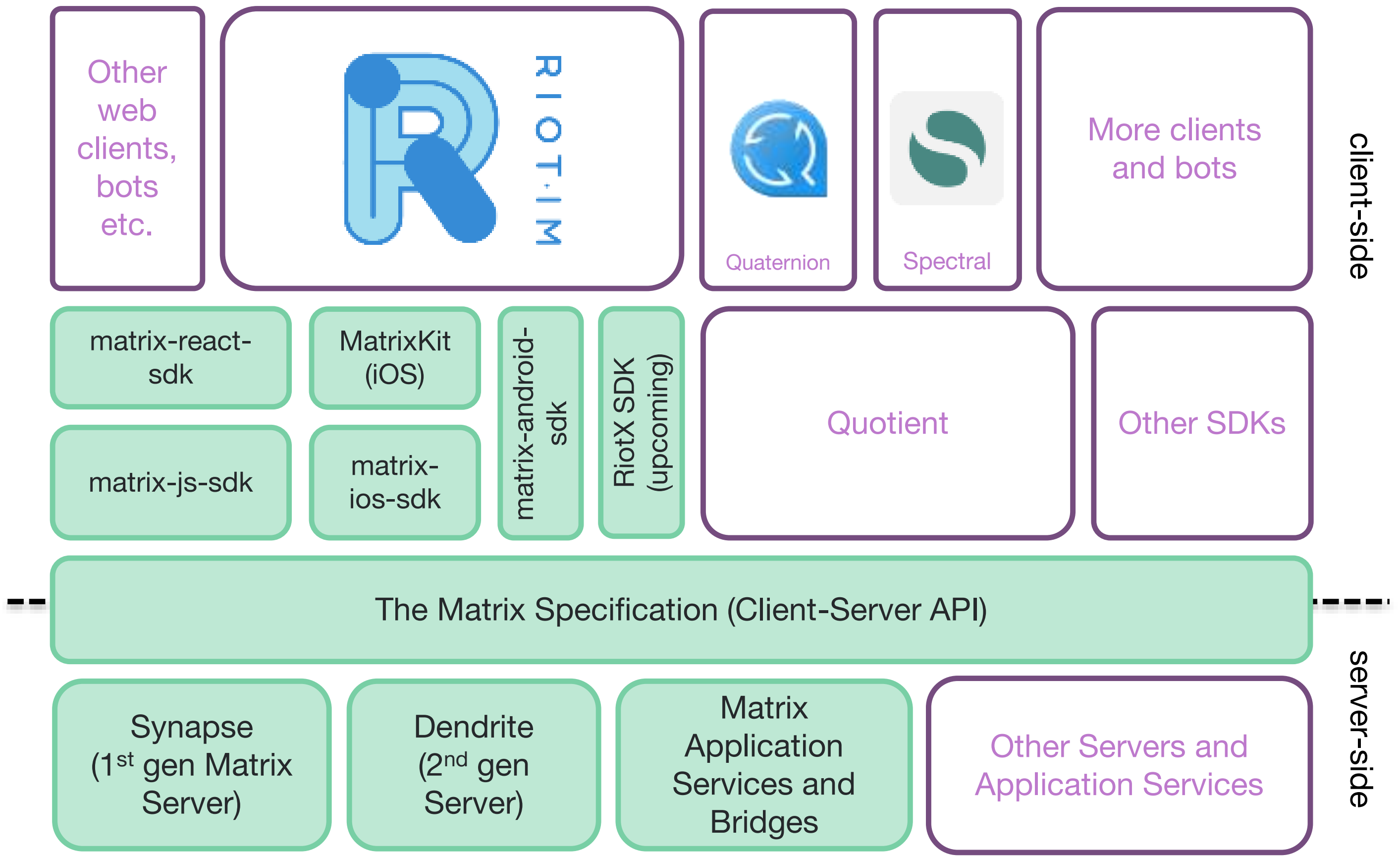
https://matrix.org/#about

- Messages are stored in a Merkle Directed Acyclic Graph (DAG)
- Messages are signed for integrity, including their position in the DAG.
- The DAG is replicated between servers, with eventual consistency semantics
- “Blockchain for real-time communication”



Matrix Open Source Ecosystem

[matrix]


Other web clients, bots etc.
RIOT·IM
Quaternion
Spectral
More clients and bots
client-side
matrix-react-sdk
MatrixKit (iOS)
matrix-android-sdk
RiotX SDK (upcoming)
Quotient
Other SDKs
matrix-js-sdk
matrix-ios-sdk
The Matrix Specification (Client-Server API)
Synapse (1st gen Matrix Server)
Dendrite (2nd gen Server)
Matrix Application Services and Bridges
Other Servers and Application Services
server-side

What do you get in the spec?

- Decentralised **conversation history**
- **Group** Messaging (and 1:1)
- **End-to-end Encryption**
- **VoIP** signalling for WebRTC
- Server-side **push notification** rules
- Server-side **search**
- Read receipts, Typing Notifs, Presence
- Synchronised read state and **unread counts**
- Decentralised **content repository**
- “**Account data**” for users per room

Clients

- >50 matrix clients (that we know about)
  - Ranging from text UIs (Weechat, Emacs, gomuks)
  - …to desktop apps (Qt: Quaternion, Spectral, Nheko; GNOME: Fractal)
  - …to glossy web and mobile clients (Riot)
  - …to protocol proxies (matrix-ircd, Pantalaimon)
- Over 15 client-side SDKs:
  - Official: JS, React, iOS, Android
  - Semi-official: Python, Perl5, Go
  - Community: C++, Erlang, Ruby, Lisp, Elixir, Haskell, Rust…

The Client-Server API

To send a message:

```
curl -XPOST -d '{"msgtype":"m.text", "body":"hello"}'
"https://alice.com:8448/_matrix/client/api/v1/rooms/ROOM_ID/send/m.room.m
essage?access_token=ACCESS_TOKEN"
```

```
{
    "event_id": "YUwRidLecu"
}
```

The Server-Server API

matrix

```
curl -XPOST -H ‘Authorization: X-Matrix origin=matrix.org,key=”898be4…”,sig=“j7JXfIcPFDWl1pdJz…”’ -d ‘{
    "ts": 1413414391521,
    "origin": "matrix.org",
    "destination": "alice.com",
    "prev_ids": ["e1da392e61898be4d2009b9fecce5325"],
    "pdus": [{
        "age": 314,
        "content": {
            "body": "hello world",
            "msgtype": "m.text"
        },
        "context": "!fkILCTRBTHhftNYgkP:matrix.org",
        "depth": 26,
        "hashes": {
            "sha256": "MqVORjmjauxBDBzSyN2+Yu+KJxw0oxrrJyuPW8NpELs"
        },
        "is_state": false,
        "origin": "matrix.org",
        "pdu_id": "rKQFuZQawa",
        "pdu_type": "m.room.message",
        "prev_pdus": [
            ["PaBNREEuZj", "matrix.org"]
        ],
        "signatures": {
            "matrix.org": {
                "ed25519:auto":
"jZXTwAH/7EZbjHFhIFg8Xj6HGoSI+j7JXfIcPFDWl1pdJz+JJPMHTDIZRha75oJ7lg7UM+CnhNAayHWZsUY3Ag"
            }
        },
        "origin_server_ts": 1413414391521,
        "user_id": "@matthew:matrix.org"
    }]
}’ https://alice.com:8448/_matrix/federation/v1/send/916d630ea616342b42e98a3be0b74113
```

The Application Service API

- Extensible custom application logic
- They have privileged access to the server (granted by the admin).
- They can subscribe to wide ranges of server traffic (e.g. events which match a range of rooms, or a range of users)
- They can masquerade as 'virtual users'.
- They can lazy-create 'virtual rooms'
- They can receive traffic by push.

A trivial application service

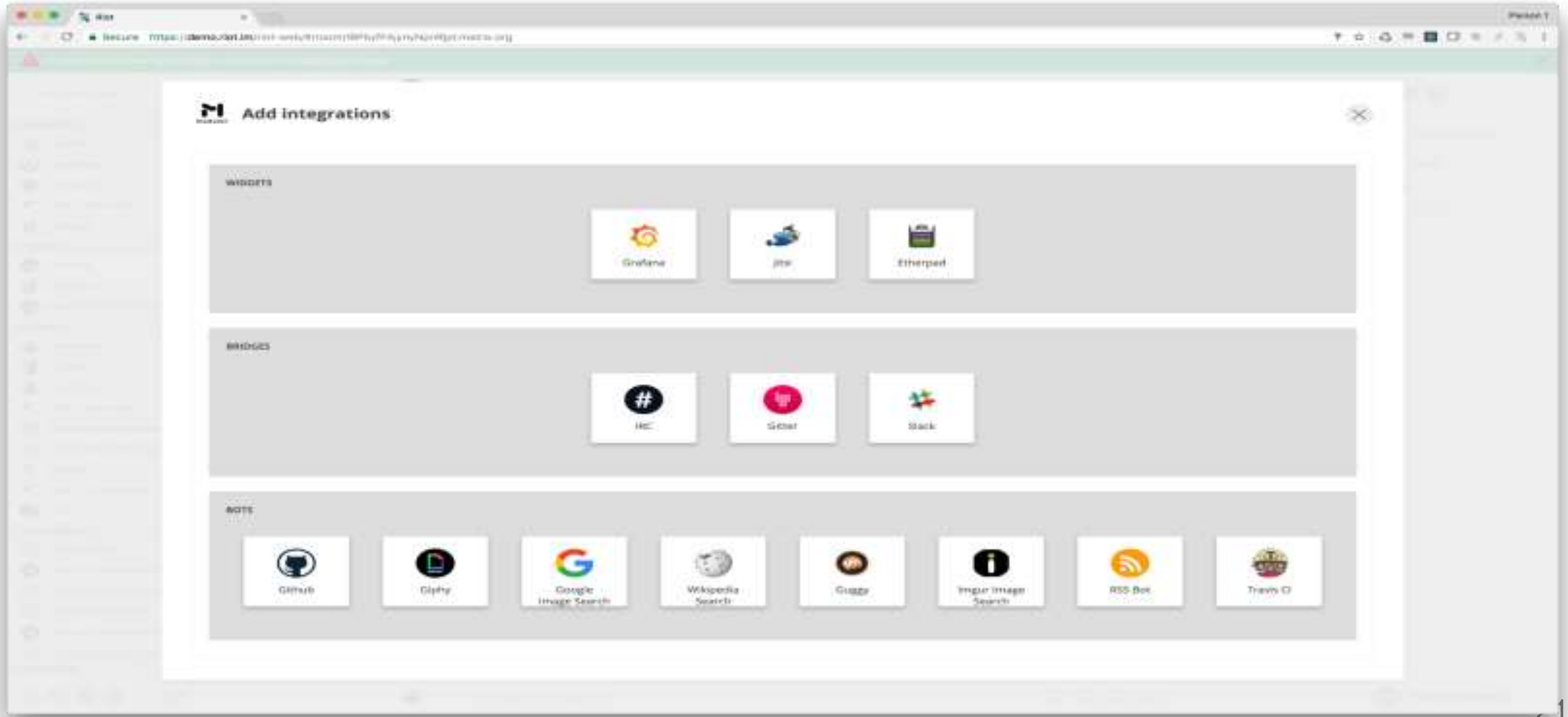
```python
import json, requests  # we will use this later
from flask import Flask, jsonify, request
app = Flask(__name__)

@app.route("/transactions/<transaction>", methods=["PUT"])
def on_receive_events(transaction):
    events = request.get_json()["events"]
    for event in events:
        print "User: %s Room: %s" % (event["user_id"], event["room_id"])
        print "Event Type: %s" % event["type"]
        print "Content: %s" % event["content"]
    return jsonify({})

if __name__ == "__main__":
    app.run()
```

Bridges

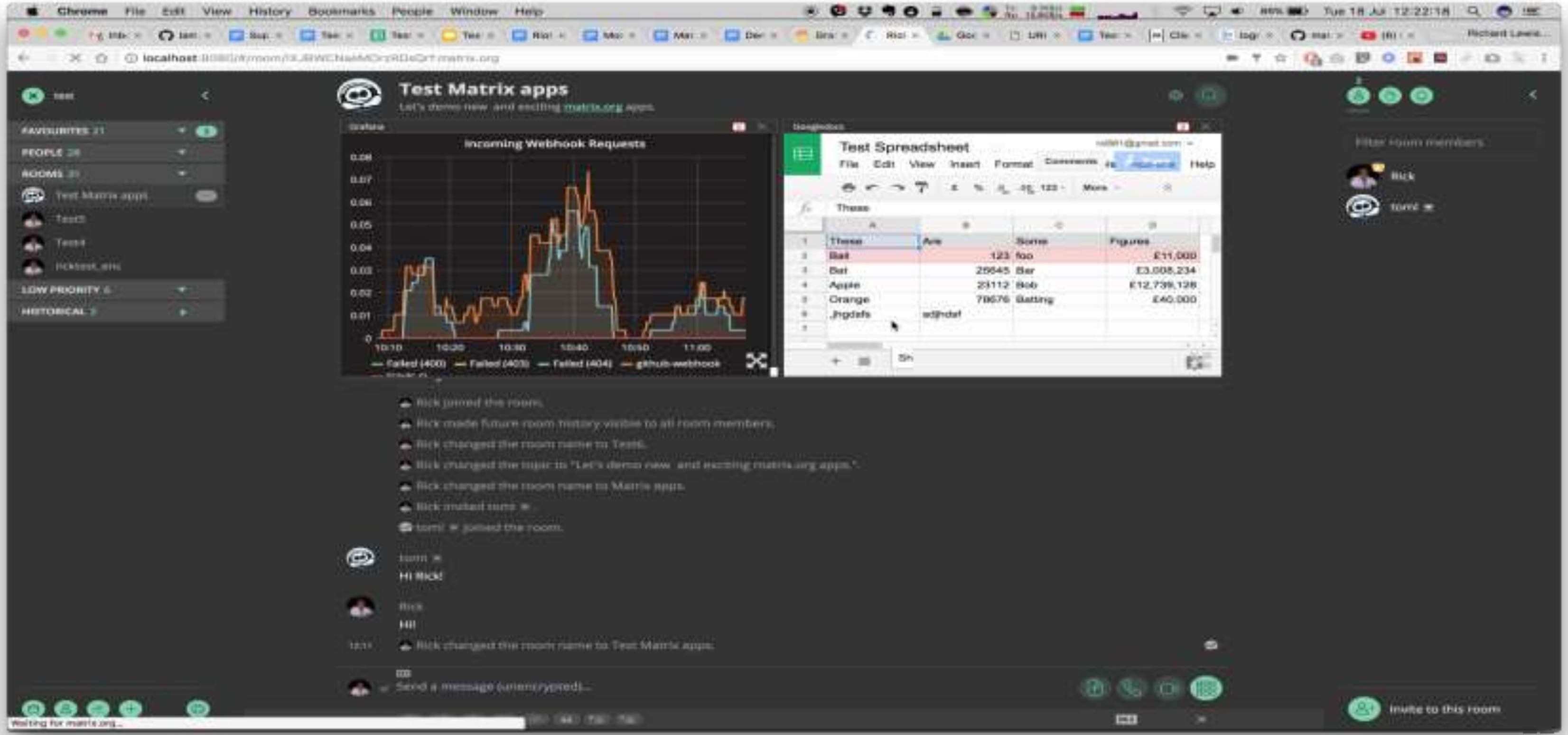
- Official ones:
  - IRC
  - Slack
  - Gitter
  - Telegram
  - Rocket.Chat
  - MatterMost
  - FreeSWITCH
  - Asterisk (Respoke)
  - Libpurple

- Community ones
  - Twitter
  - iMessage
  - Facebook Msgr
  - Signal
  - Hangouts
  - Slack
  - Gitter (‘sidecar’)
  - ~8 IRC ones…
  - ~4 XMPP ones...
  - ~3 Telegram ones…

Modular: an App Store for hosted Matrix Integrations



Modular Widgets: Embedding Real Apps into Matrix Rooms!



	A	B	C	D
1	These	Are	Some	Figures
2	Bat	123	foo	£11,000
3	Bat	25645	Bar	£3,008,234
4	Apple	23112	Bob	£12,739,128
5	Orange	78676	Batting	£40,000
6	Jhgdafs	adjhdaf		
7				

Rick joined the room.
Rick made future room history visible to all room members.
Rick changed the room name to Test6.
Rick changed the topic to "Let's demo new and exciting matrix.org apps.".
Rick changed the room name to Matrix apps.
Rick invited tomi.
tomi joined the room.

tomi
Hi Rick!

Rick
Hi!

12:11 Rick changed the room name to Test Matrix apps.

Send a message (unencrypted)...

End-to-end encryption (E2EE) overview

- Two mechanisms at work:
  - **Olm** – a Double Ratchet implementation
    - provides a secure channel between two devices
    - used mainly for syncing key data
  - **Megolm** - a new ratchet that encrypts sender’s messages for a **group** of receivers
    - Ratchet state is shared to receivers 1:1 over Olm
    - Ratchets can be replaced to seal history
    - Ratchets can be fast-forwarded to share selective history

Key management

- Uses EC25519 keys.
- Keypairs generated **per-device** at login.
- Private keys are stored ~~only~~ on the device (optionally backed up to a secure area on your homeserver).
- Public keys are published on your homeserver.
- Keys are verified by comparing ~~public fingerprints~~ short easy to read strings
- Attachments are AES-CTR encrypted (with integrity hash) using a new random key per file.

Matrix in the Wild

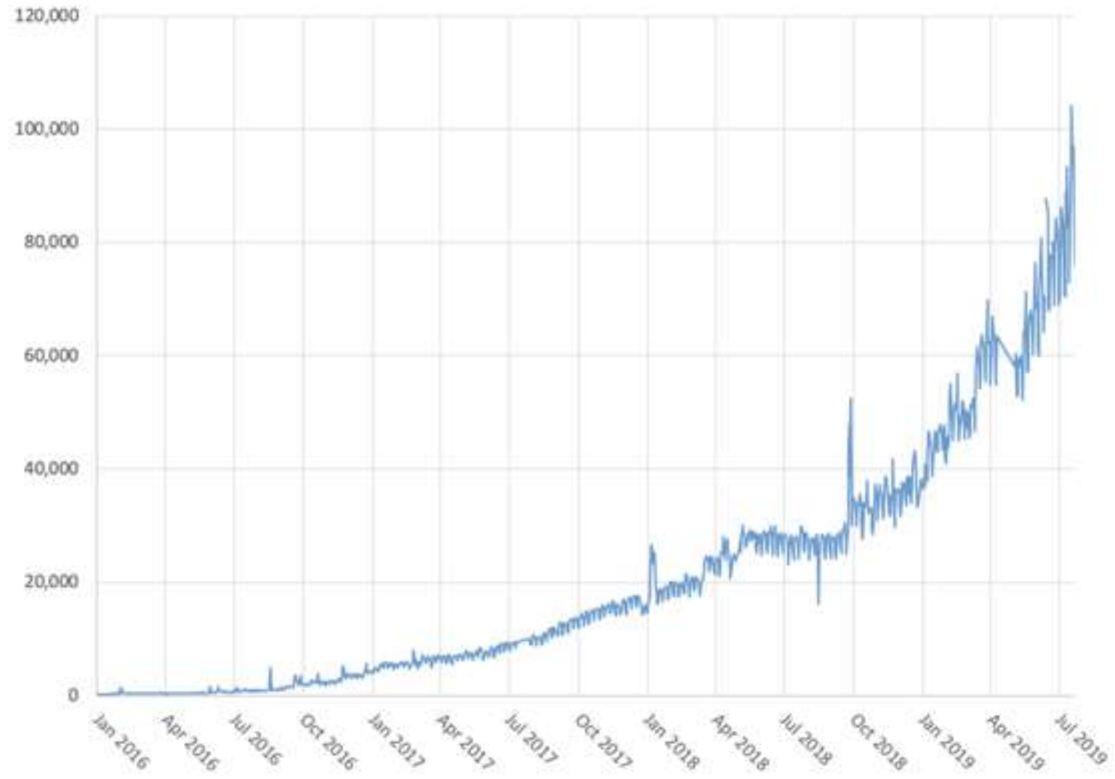
[matrix]

A brief history of Matrix

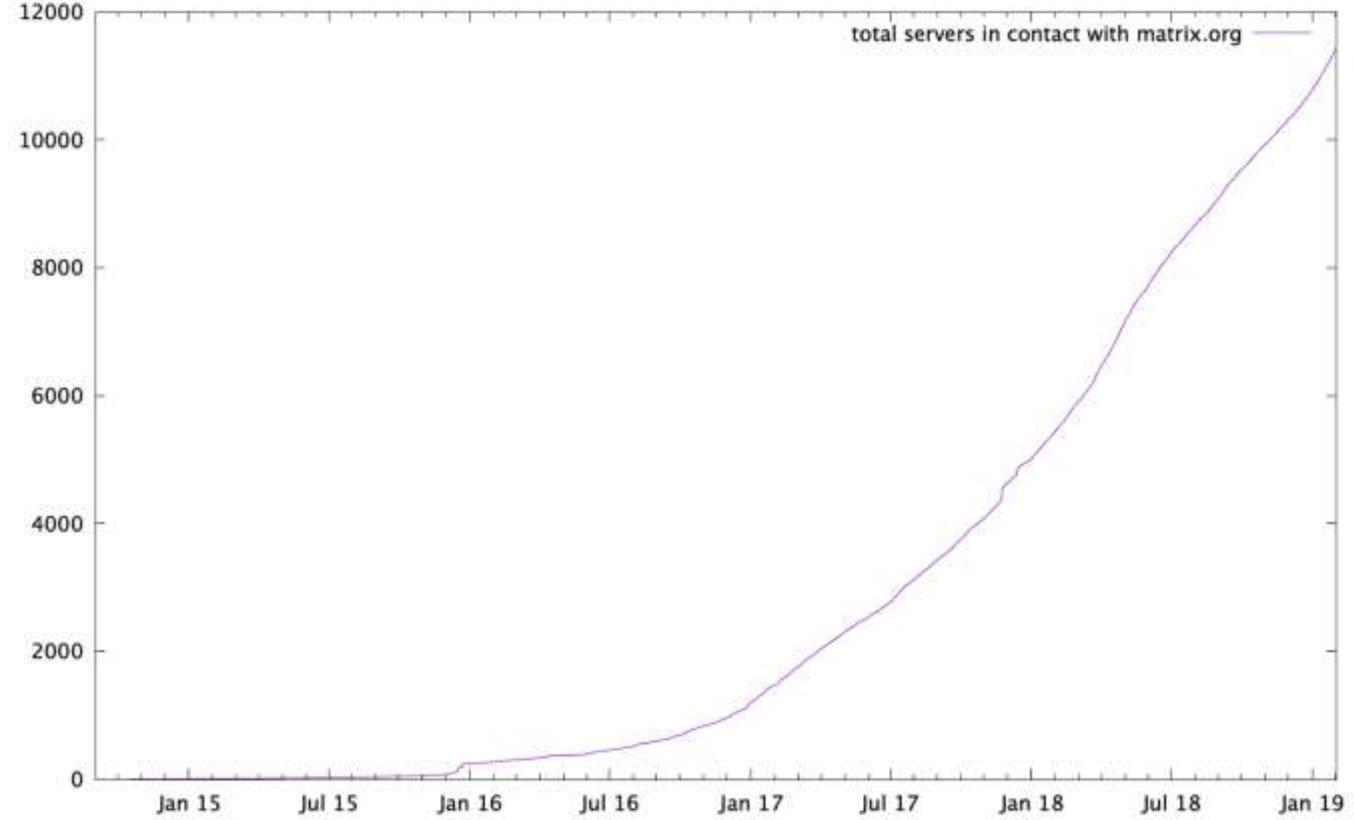
- 2014: First alpha!
- 2015: Federation becomes usable; add Postgres; add IRC
- 2015: First release of Vector as a flagship Matrix client; r0 CS API
- 2016: Scaling; First cut of E2E Encryption; Vector becomes Riot
- 2017: Widgets, Stickers, Jitsi, Communities, i18n, Dendrite
- 2018: Feature freeze. Road to 1.0: security, stability, governance.
- 2019: **Matrix 1.0** and beyond!

Daily active users on the public federation

[matrix]



Publicly visible servers



[matrix]

Community Status

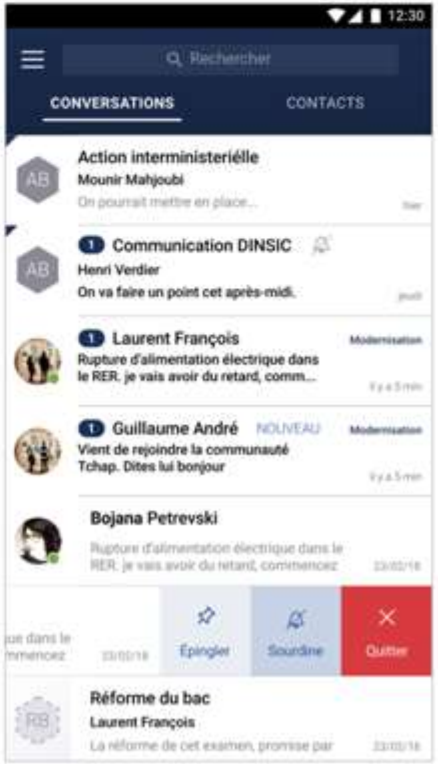
- ~10.0M global visible accounts
- ~2.5M messages per day
- ~4.5M unbridged accounts
- ~2.1M rooms that Matrix.org participates in
- ~20,000 federated servers
- ~3000 msgs/s out, ~30 msgs/s in on Matrix.org
- ~400 projects building on Matrix
- ~70 companies building on Matrix

X

Matrix and French Government

In 2018, Matrix was selected to provide self-sovereign, encrypted decentralized communication tools across government

- Requirements:
  - 100% Open source.
  - 5.5 Million users over > 30 operationally independent ministries
  - Initially private federation, but with scope to support public federation



Action interministeriélle
Mounir Mahjoubi
On pourrait mettre en place...
hier

1 Communication DINSIC
Henri Verdier
On va faire un point cet après-midi.
jeudi

1 Laurent François — Modernisation
Rupture d'alimentation électrique dans le RER. je vais avoir du retard, comm...
il y a 5 min

1 Guillaume André — NOUVEAU — Modernisation
Vient de rejoindre la communauté Tchap. Dites lui bonjour
il y a 5 min

Bojana Petrevski
Rupture d'alimentation électrique dans le RER. je vais avoir du retard, commencez
23/02/18

ue dans le
mmencez
23/02/18

Réforme du bac
Laurent François
La réforme de cet examen, promise par
23/02/18

Recent updates

Matrix 1.0

- Exited beta on June 11th 2019!
- All about security, correctness and spec completeness
- “*Make it work, make it work right*, make it fast”
- News:
    - New algorithm on how two servers agree on the room state
    - Room versioning to manage incompatible DAG format upgrades
    - Switch from Perspectives to X.509 for server auth (no more self-signing)
    - .well-known (RFC 5785) support for seamless configuration
    - Stable spec releases of all Matrix APIs
- Fun stuff comes next…

[matrix]

The Matrix.org Foundation

- 1.0 also marked the official launch of The Matrix.org Foundation
- UK Non-Profit (CIC): Neutral custodian of the protocol.
- Formal Manifesto, Mission, Values & Constitution for spec evolution
- 8 person Spec Core Team to review and evolve the spec
  - Many paid to work fulltime on Matrix by New Vector, the startup set up by the original Matrix team.
- 5 Guardians (Directors) to act as custodians and ensure neutrality:
  - Matthew Hodgson (Founder)
  - Amandine Le Pape (Founder)
  - Dr Jutta Steiner (CEO, Parity)
  - Prof Jon Crowcroft (cam.ac.uk)
  - Ross Schulman (New America)

Fun stuff

- Reactions and editable messages
- RiotX – entirely new mobile client for Android in Kotlin
  - A rewrite for iOS is in the works
- Verification for E2EE using Short Authentication Strings (SAS)
  - Use emoji instead of hex codes!
- Pantalaimon – client-side E2EE proxy
  - Makes any client E2EE capable (at the expense of some security drawbacks = you should know what you’re doing)
  - Searching in encrypted rooms is in the works
- E2EE cross-signing
  - Move from device-specific to user-specific trust

[matrix]

Privacy enhancements

- Make identity servers and integration managers entirely optional
- Garbage collect deleted data properly
- Per-room data retention policies (still in implementation)
- Don’t fall back to Google TURN (unless you want to)
- Fixing various stupid bugs

Identity Servers

- Map from 3rd party identifiers (3PIDs) to MXIDs
- Current solution is a placeholder:
  - Simple python “sydent” server.
  - Logically centralised (matrix.org & vector.im)
- Challenges:
  - Must not have to trust a centralised ID server
  - Stores a lot of sensitive data
  - Identity mappings must be trustworthy
  - Ideally need to track validator reputation

What’s Next?

What’s Next?

- First Time User Experience in Riot
- E2EE by default (pushing more clients to support it)
- Comprehensive moderation and abuse tools
- Decentralised Accounts (account portability)
- Launch RiotX (both Android and iOS)
- P2P Matrix
- Decentralised reputation

Reputation

- Users want to be able to filter out ‘low quality’ content (e.g. spam, offensive msgs)
- In a global neutral system like Matrix this **must** be morally relative:
  - One man’s spam is another’s direct marketing
  - Just because *I* want to filter out a certain political viewpoint doesn’t mean *you* do
- **We must not create filter bubbles**
  - Users must be able to visualise and curate algorithmic filtering

Spam/Reputation solutions

- Possible solution:
  - Let users rate messages.
  - Could be up-vote / down-vote
  - Could be emoji reactions
  - Could be tags (from a taxonomy or freeform)
- The richer the rating, the more risk of the rating itself needing moderation(!)
- Even a simple up-vote/down-vote can be abused: e.g. user accidentally posts a password; malicious voters upvote it for visibility.

Reputation solutions

- Possible solution (cont.)
  - Up/down-votes form an implicit social graph
  - Detect Sybil attacks and voting rings from clusters in that graph
  - Correlate clusters with content in public msgs, to visualise reputation?
    - “95% of users who liked this msg also like Trump”
  - Consider transitive trust through the social graph
    - “80% of your friends like this”
  - ...but let the user curate and visualise which trust sources they align with:
    - “70% of your friends like this, but 90% of the world hates it”
  - Graph **must** be anonymized somehow
  - Could also merge in other indicators (user rating; IP rating; ISP rating; traffic patterns...)

How you can help

Use Matrix!

Give Matrix a spin:

- Sign up via https://riot.im OR
- Try one of the clients at https://matrix.org/clients

- Run your own server
  - Self host OR
  - Use a provider like https://modular.im

Develop for Matrix!

- Contribute to clients code: https://matrix.org/clients
- More applications (bots, bridges, integration…)
    - SDKs: https://matrix.org/docs/projects/sdks
- Contribute to servers:
    - https://github.com/matrix-org/dendrite (“official” in Go)
    - https://github.com/ruma/ruma (“unofficial” in Rust)

[matrix]

Thank you!

@kitsune:matrix.org (https://matrix.to/#/@kitsune:matrix.org)
Twitter: @matrixdotorg, @aerusakov
https://matrix.org