[matrix]

The future of decentralised communication, identity and reputation with Matrix

matthew@matrix.org
http://www.matrix.org

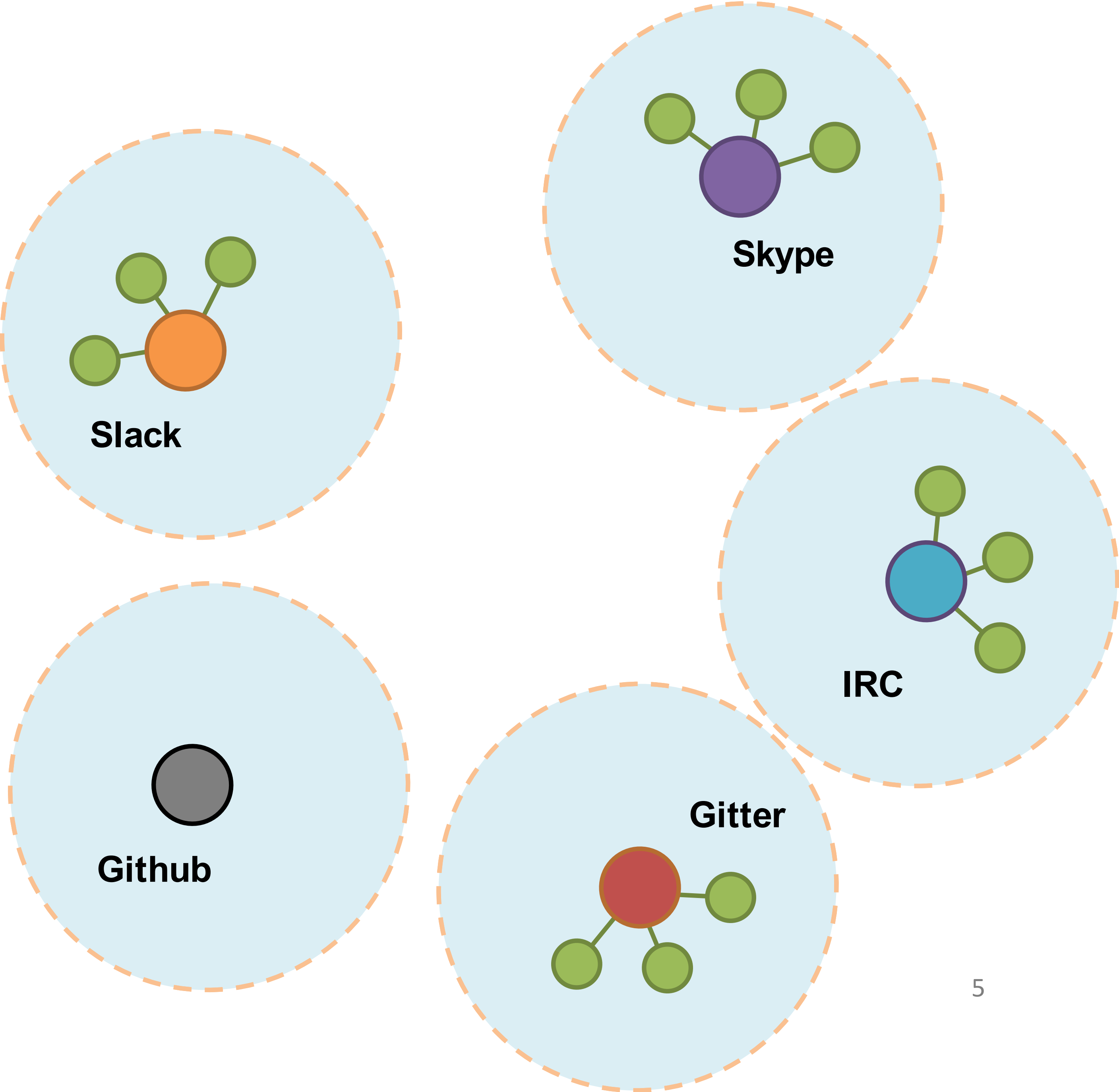
Matrix today:

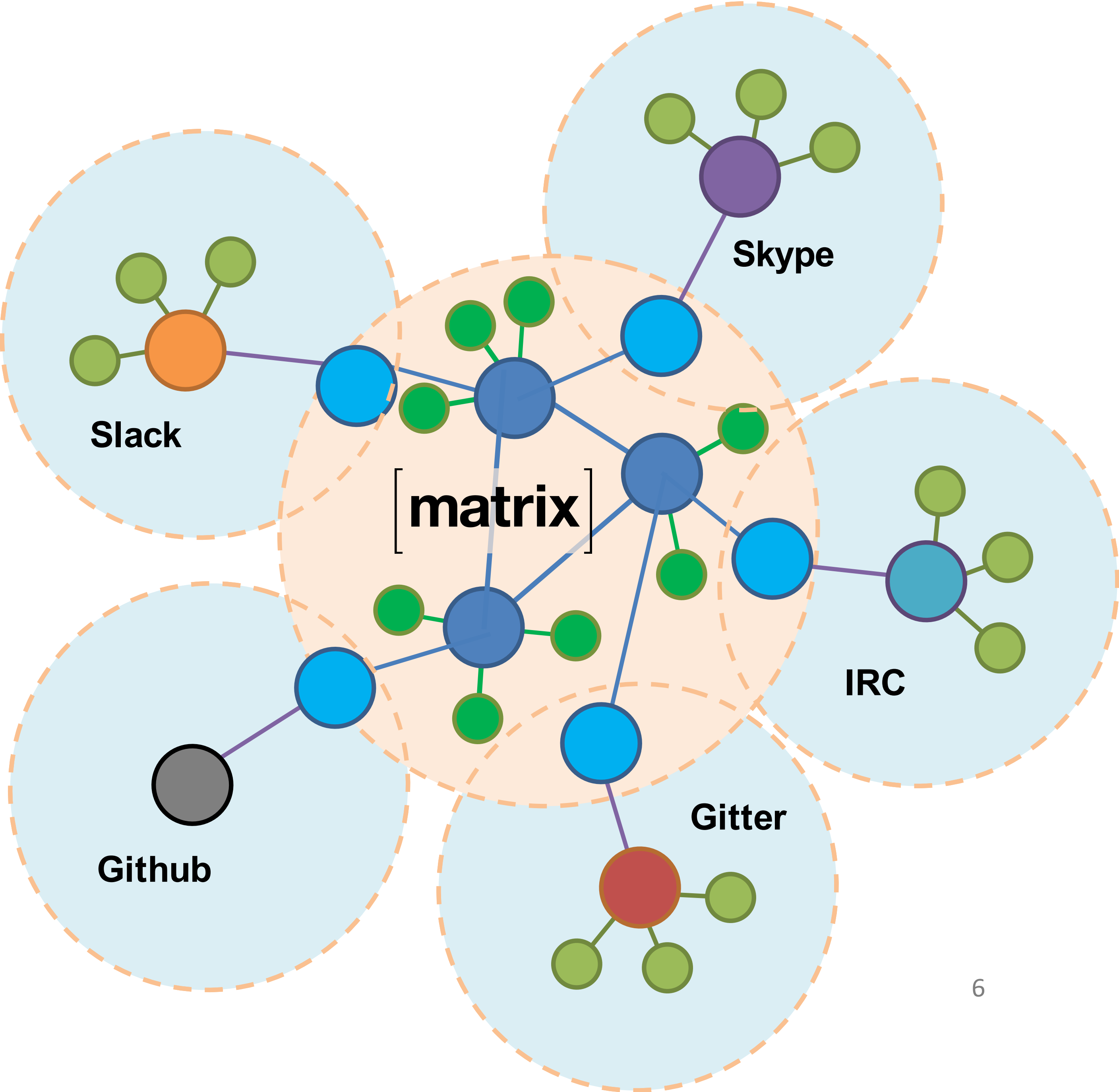
[matrix]

A non-profit open standard for defragmenting communication

Creating a global encrypted communication meta-network that bridges all the existing silos & liberates our communication to be controlled only by us.

[matrix]




Skype
Slack
[matrix]
IRC
Github
Gitter

No single party owns your conversations.

Conversations are shared over all participants.

Use Matrix for:

- Group Chat (and 1:1)
- WebRTC Signalling
- Bridging Comms Silos
- Internet of Things Data

…and anything else which needs to pubsub persistent data to the world.

Why are you re-inventing XMPP!?!?

WE ARE NOT.

How is this different to XMPP?

- **Completely** different philosophy & architecture:
  - A single, monolithic, consistent, spec.
  - Different primitives:
    - Syncing decentralised conversation history (not message passing / pubsub)
    - Group conversation as a first class citizen
    - E2E crypto as a first class citizen
  - HTTP+JSON as the baseline API **(but you can use other transports too!)**
  - Core focus on defragmentation and bridging (hence the name “matrix”).

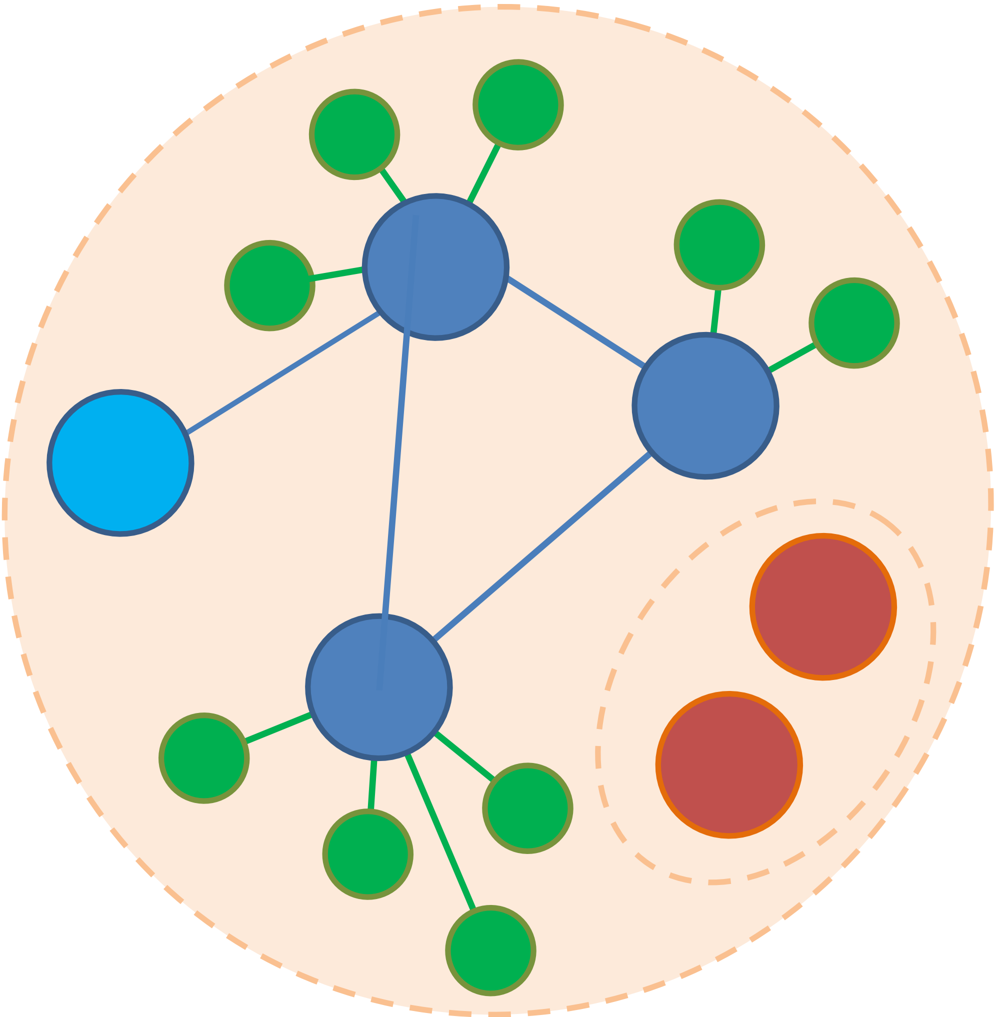
Matrix Architecture

● Clients

● Home Servers

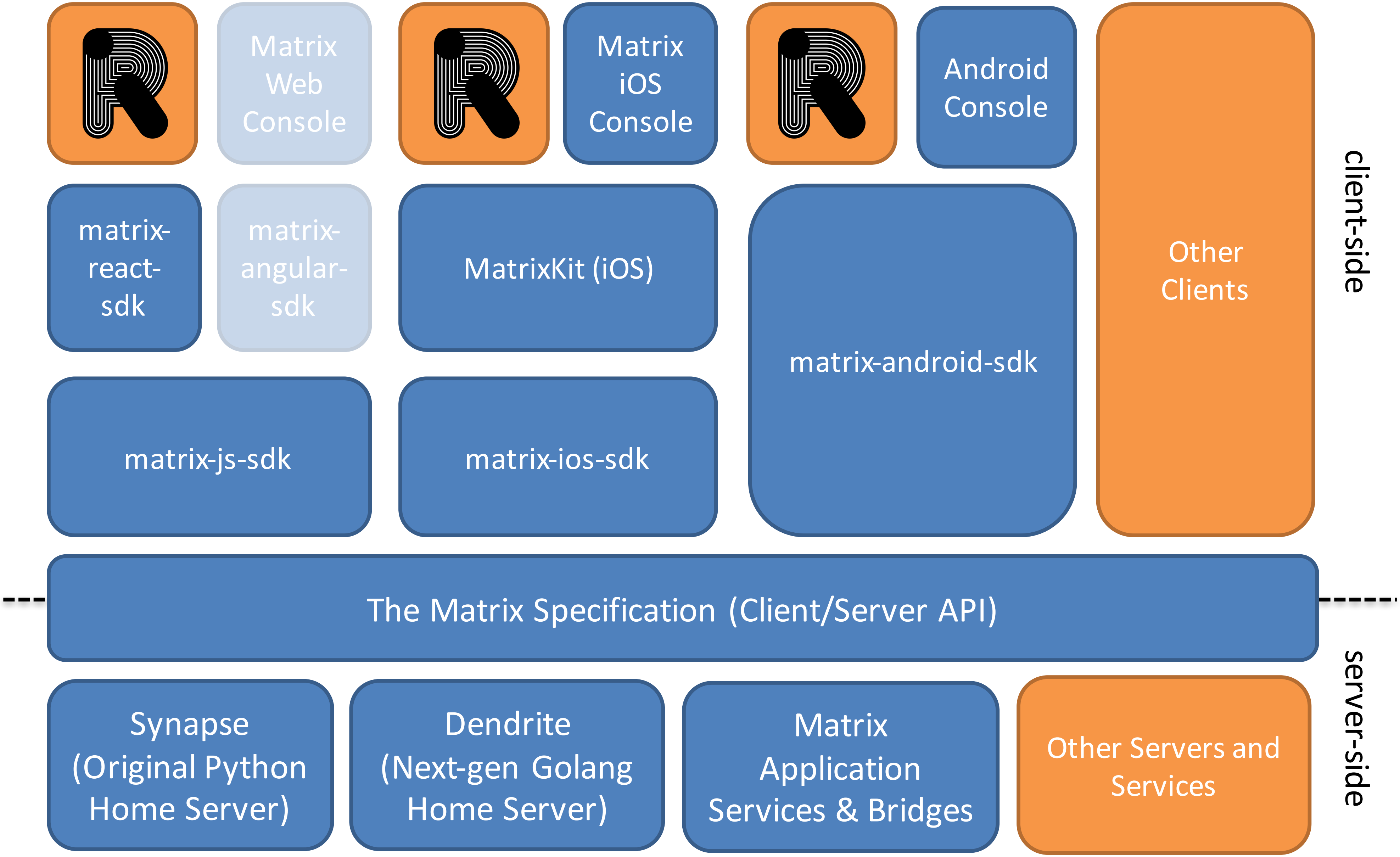
● Application Servers

● Identity Servers



matrix

The Matrix Ecosystem



Matrix Web Console

Matrix iOS Console

Android Console

matrix-react-sdk

matrix-angular-sdk

MatrixKit (iOS)

matrix-android-sdk

Other Clients

matrix-js-sdk

matrix-ios-sdk

client-side

The Matrix Specification (Client/Server API)

server-side

Synapse (Original Python Home Server)

Dendrite (Next-gen Golang Home Server)

Matrix Application Services & Bridges

Other Servers and Services

What do you get in the spec?

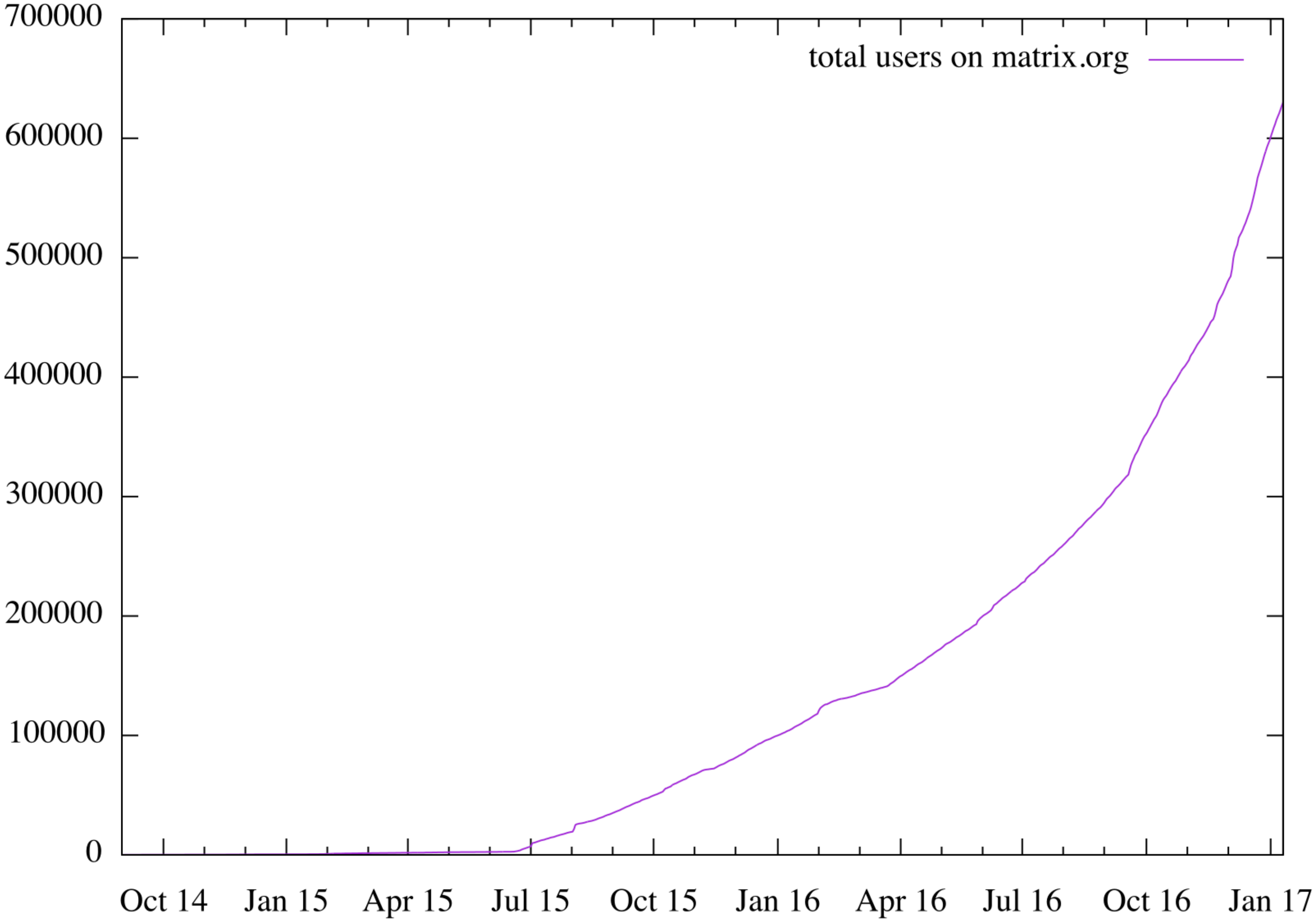
- Decentralised conversation history (timeline and key-value stores)
- Group Messaging
- **End-to-end Encryption**
- VoIP signalling for WebRTC
- Server-side push notification rules
- Server-side search
- Read receipts, Typing Notifs, Presence
- Synchronised read state and unread counts
- Decentralised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

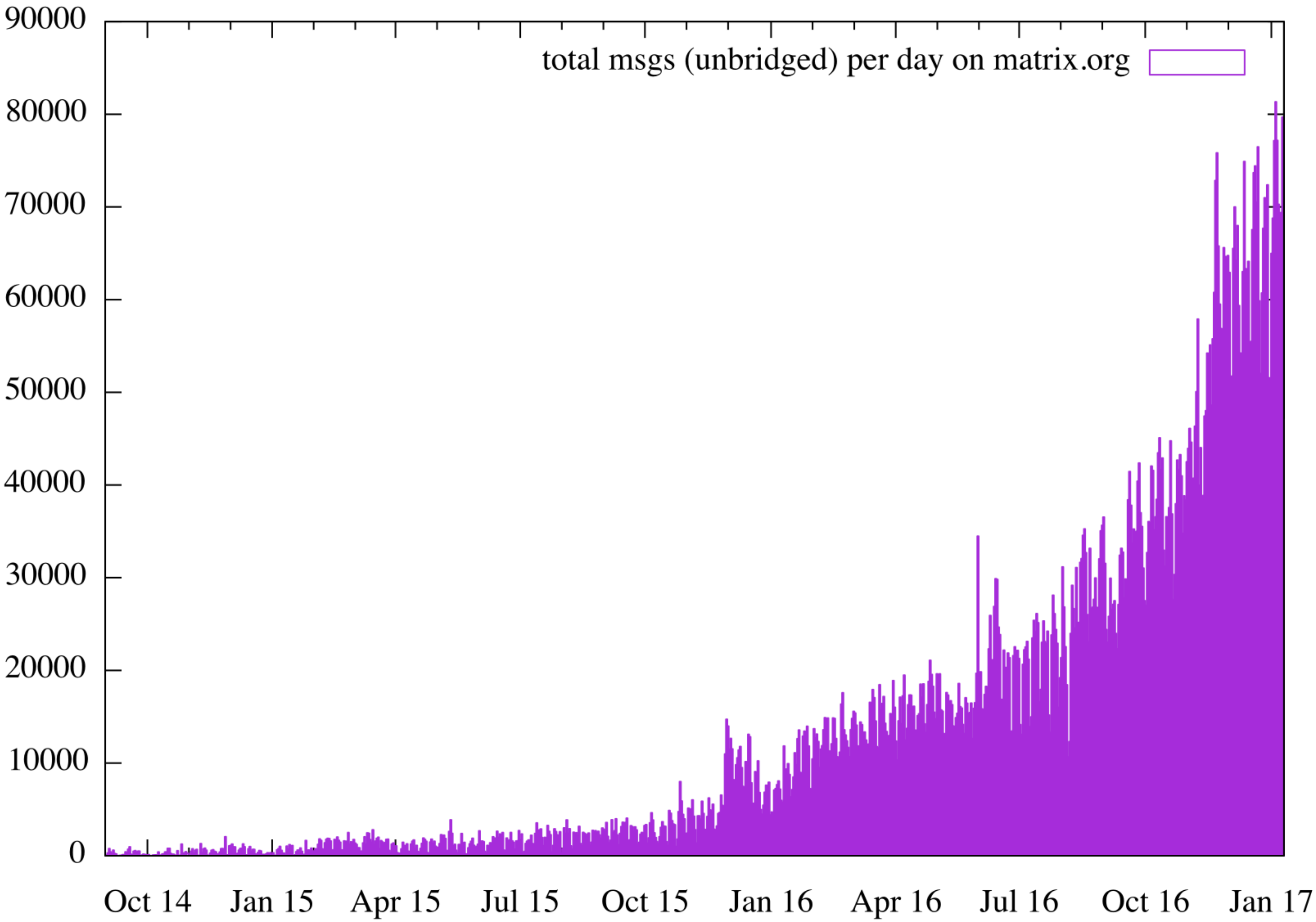
What does it look like?

https://riot.im

Community Status

- Started out in Sept 2014
- Currently in very late beta
- ~700K user accounts on the Matrix.org homeserver
- ~700K messages per day
- ~100K unbridged accounts
- ~100K unbridged messages per day
- ~70K rooms that Matrix.org participates in
- ~1500 federated servers
- ~1000 msgs/s out, ~10 msgs/s in on Matrix.org
- ~50 companies building on Matrix


total users on matrix.org
700000
600000
500000
400000
300000
200000
100000
0
Oct 14
Jan 15
Apr 15
Jul 15
Oct 15
Jan 16
Apr 16
Jul 16
Oct 16
Jan 17


total msgs (unbridged) per day on matrix.org
90000
80000
70000
60000
50000
40000
30000
20000
10000
0
Oct 14
Jan 15
Apr 15
Jul 15
Oct 15
Jan 16
Apr 16
Jul 16
Oct 16
Jan 17

Matrix in the future:

What are today’s limits?

- Centralised Identity servers.
- Centralised Accounts.
- Spam.
- Reputation.
- Metadata Protection.

Identity Servers

- Matrix has its own opaque “MXIDs”, e.g.
  @matthew:matrix.org
- These are **not** meant to be human visible
- Instead, we should identify users when inviting via whatever **3rd Party IDs (3PIDs)** we know already:
  - Email addresses
  - Phone numbers
  - Facebook IDs
  - Skype IDs
  - LDAP usernames
  - etc.

Identity Servers

- Map from 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.

Identity Servers: the Future

- Possible solutions:
  - **Keybase.io**
    (but not decentralised; doesn't map email)
  - **Blockstack**
    (but technically need bitcoin to add entries, and identity validators are blindly trusted)
  - **Webfist** (email only; DKIM for assertions)
  - **Mozilla Persona** (RIP)
  - Other decentralised ledgers: **Sovrin, uPort, Stellar, Namecoin**… (don't solve validator trust)
  - DNS-style systems: **GNS, DNSSEC ENUM**?
  - Matrix community innovation – e.g. **mxisd**

This isn’t just Matrix:
Everybody needs this.

e.g. “How do I map an email address to a bitcoin ID?”

Decentralised Accounts

- Matrix's rooms are entirely decentralised.
- Matrix accounts are currently not:
  - @matthew:matrix.org is stuck on Matrix.org.
- Problems:
  - Dependent on DNS
  - Can't have backup homeserver(s) (like SMTP secondary MX's)
  - Can't migrate between providers(!)

Decentralised Accounts

- Possible futures:
  - Use identity server to provide MXID indirection?
  - @matthew:matrix.org -> {@matthew:matrix.org, @matthew:arasphere.net}
  - Still dependent on DNS. What if domains expire?
- Alternatively:
  - Decouple user IDs from DNS
  - Use fingerprint of user public key?
  - Today's MXIDs become type of 3PID for compat:
    - @matthew:matrix.org -> 2f2878c485cb681e3
  - Use a DHT to discover HSes that host that ID?

Spam

- Low-grade spam problem here already.
- Mostly bridged (from IRC), but also native.
- We require invite handshake before 1:1s (unlike email), so spam is either:
  - Invite spam (name & avatar of inviter)
  - Public room spam (user joins & spams room)
- E2E Crypto means no content filtering.
- To fix spam, one solution is to assign reputation to users.

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...)

Spam solutions

- Spam can be modelled as reputation problem, or:
- Create a barrier to users to first speak.
  - e.g. spend money...
    - Make a donation to charity to prove you are real!
    - Buy reputation from a ID broker who then vouches for you
  - …or present proof of work...
  - ...or require users to explicitly have been vouched for (e.g. by reputation upvotes)
- Or some combination of all three (or more).
- (Thanks to Christian Grothoff for inspiration here!)
- Might be overengineered. And adds a lot of dependencies.

Again, this isn’t just Matrix:
Everybody needs this.

e.g. “If pay this bitcoin ID, is its owner going to fulfil my order?”

Metadata Privacy

- Matrix does not protect metadata currently…
- ...but it could.
- Come along to this afternoon's "**Encrypting Matrix**" talk (3pm, Janson) to find out how!

Matrix: What’s next?

- More hosted bridges, bots, services etc
- Threading
- Message tagging (e.g. “Like” support)
- Group ACLs
- File tagging and management
- Decentralised identity
- Fixing spam & reputation.

We need help!!

- **We need people to try running their own servers and join the federation.**
- **We need people to run gateways to their existing services**
- **We need feedback on the APIs.**
- **Consider native Matrix support for new apps**
- **Follow @matrixdotorg and spread the word!** 🐦

[matrix]

Thank you!

matthew@matrix.org
http://matrix.org
@matrixdotorg

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.message?access_token=ACCESS_TOKEN"
```

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

The client-server API

To set up a WebRTC call:

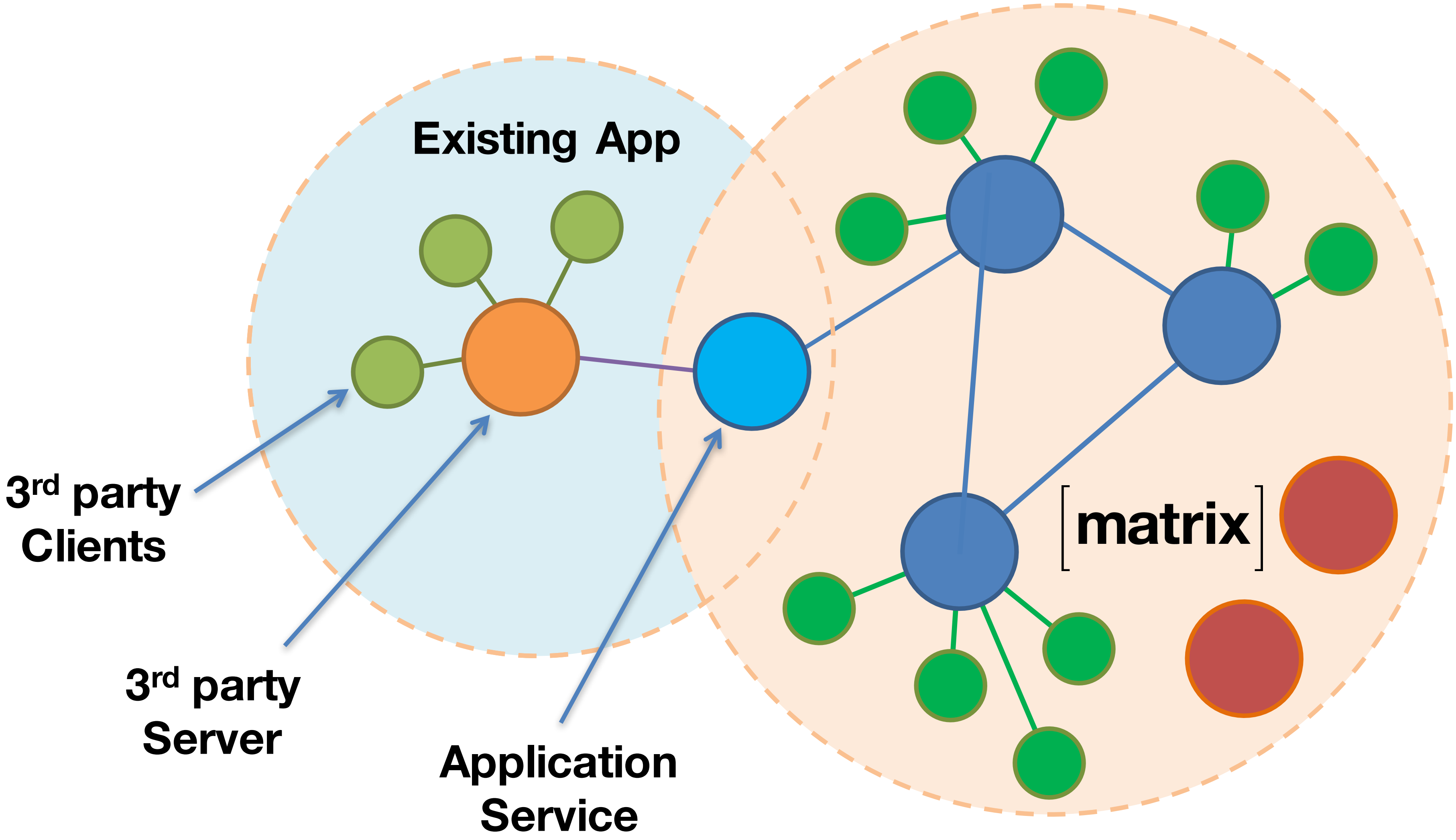
```
curl -XPOST –d '{\
  "version": 0, \
  "call_id": "12345”, \
  "offer": {
    "type" : "offer”,
    "sdp" : "v=0\r\no=- 658458 2 IN IP4 127.0.0.1…"
  }
}'
"https://alice.com:8448/_matrix/client/api/v1/rooms/ROOM_ID/send/m.call.invite?access_token=ACCESS_TOKEN"

{ "event_id": "ZruiCZBu” }
```

Basic 1:1 VoIP Matrix Signalling

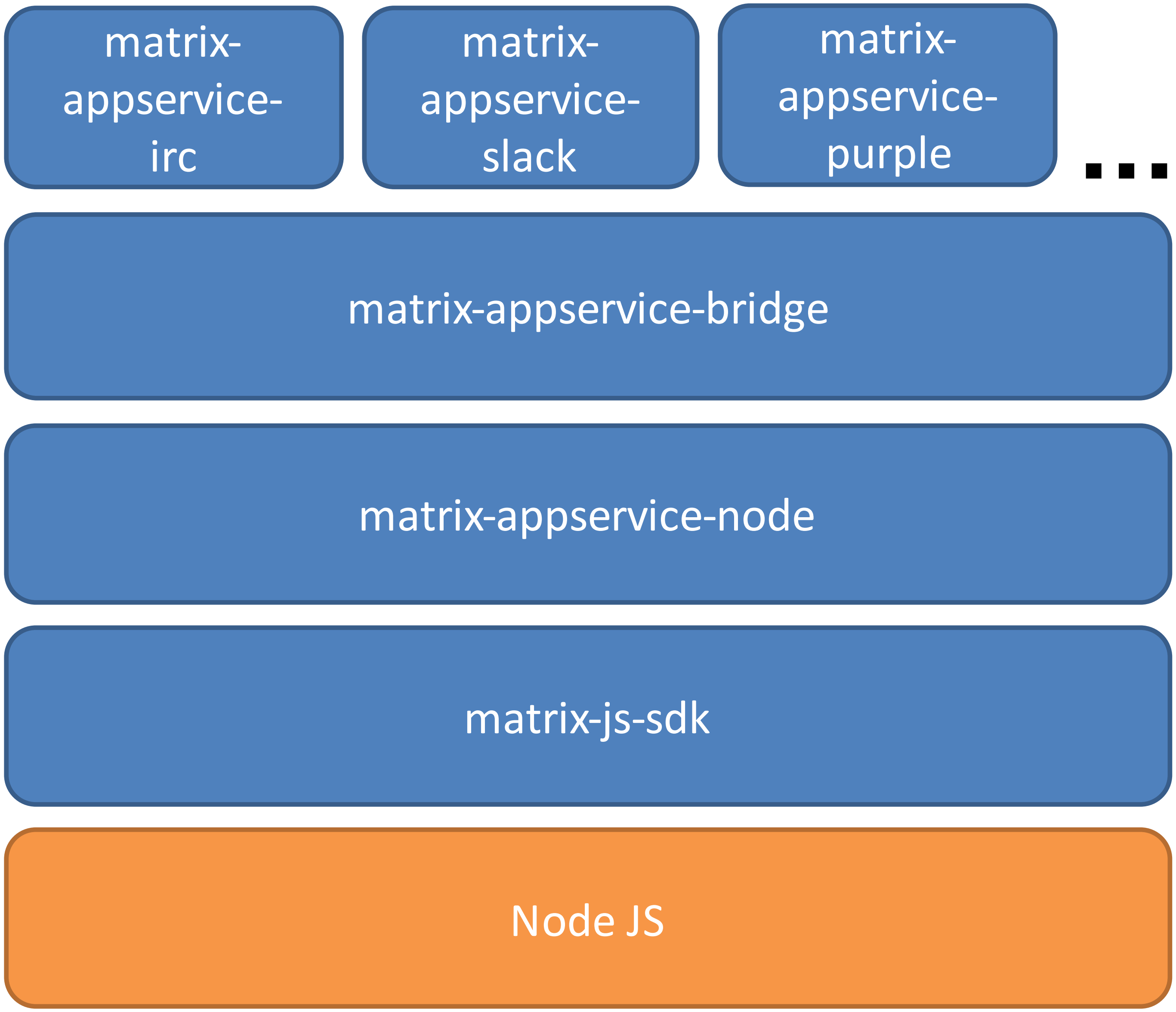
```
    Caller                        Callee
m.call.invite ----------->
m.call.candidate -------->
[more candidates events]
                        User answers call
                 <------ m.call.answer
              [media flows]
                 <------ m.call.hangup
```

[matrix]

Bridges and Integrations



Typical Bridging Stack



matrix-appservice-irc

matrix-appservice-slack

matrix-appservice-purple

…

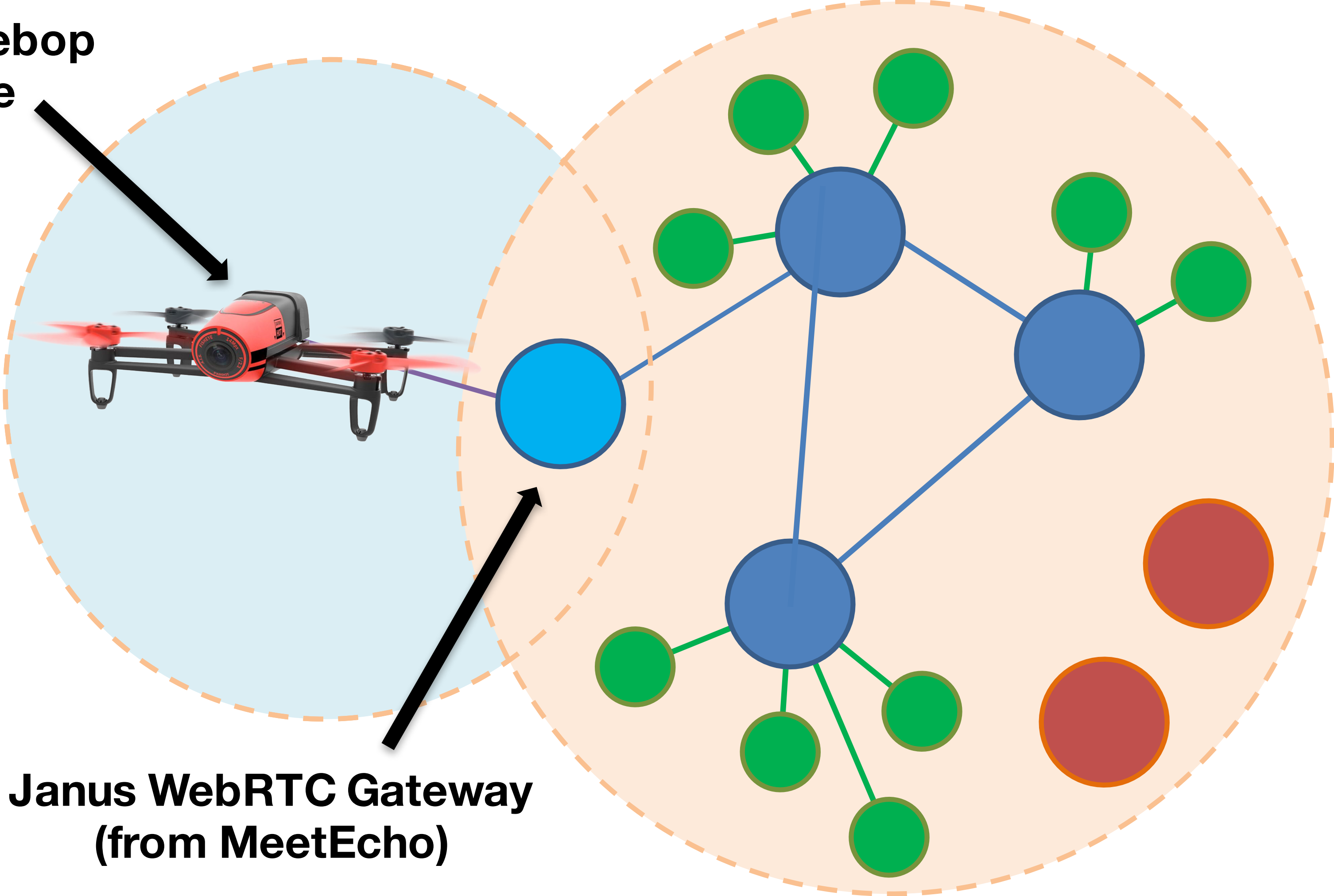
matrix-appservice-bridge

matrix-appservice-node

matrix-js-sdk

Node JS

Matrix to IOT…



Parrot Bebop Drone

Janus WebRTC Gateway (from MeetEcho)

https://www.youtube.com/watch?v=D7jZSYkXqt4&t=2649

Matrix and VR…