Diving into Decentralized Communication

matthew@matrix.org | amandine@matrix.org | cel@celehner.com

Matrix

Secure Scuttlebutt

Mastodon

Status

Vuvuzela

Briar

Matrix

Started	May 2014
Main Uses	Public & private chatrooms, VoIP calling, arbitrary PubSub
Architecture	Decentralised Servers + Thin Clients
Data primitives	Conversation History (Directed Acyclic Graphs), Key-Value data, Ephemeral messages, Store & Forward messages.
Encryption	Double Ratchet (Olm), Group conversations via Megolm (shared AES ratchet)
Identity Model	Matrix IDs currently DNS; moving to public keys per-room Identity lookup currently centralised ☹
Transport	HTTPS + JSON (but extensible)
Maturity	Late Beta (1.0 due Aug 2018)
Platforms	Web, iOS, Android, Desktop…
Total users	~5.5M (~1M non-bridged)

Secure Scuttlebutt

Started	May 2014
Main Uses	Inbox, social feed, Git, DNS, Whois
Architecture	Gossip-based P2P; Pubs used for rendezvous
Data primitives	Append-only logs of signed JSON
Encryption	Private Box
Identity Model	Public keys with human attestations on every message
Transport	Secret Handshake
Maturity	18.1.1
Platforms	Node (Electron for Patchwork)
Total users	~20K in the largest strong set

Mastodon

Started	2016
Main Uses	Microblogging
Architecture	ActivityPub (originally OStatus) + Thin Client
Data primitives	Streams of JSON LD (Activity Pub) or RSS (OStatus)
Encryption	No E2E encryption yet.
Identity Model	@user@domain
Transport	HTTPS
Maturity	2.4.3
Platforms	Web (and clients on Android, iOS)
Total users	1.4M

Status

Started	2016
Main Uses	1:1 and Group Messaging (and DApp browsing & payments)
Architecture	Whisper (Ethereum Pubsub)
Data primitives	Whisper objects
Encryption	Double Ratchet experiments
Identity Model	Ethereum address and ENS
Transport	Whisper
Maturity	Beta 0.9.21
Platforms	Android, iOS (Desktop via React Native Qt in dev)
Total users	?

Vuvuzela

Started	2015
Main Uses	Metadata-resistant 1:1 messaging
Architecture	Mixnet + Anytrust Private Key Generator servers. **Not exactly decentralised.**
Data primitives	Message passing
Encryption	Rotating static key
Identity Model	Email addresses + Identity Based Encryption!
Transport	TCP
Maturity	? /call doesn't seem to work currently.
Platforms	Command Line
Total users	?

Briar

Started	2011
Main Uses	1:1 chat, Private groups, Forums, Blogs…
Architecture	Entirely P2P, inc mesh networks, built on the Bramble stack
Data primitives	BSP: Directed Acyclic Graphs called Groups
Encryption	Rotated static keys
Identity Model	(Invisible) public keys verified by QR code
Transport	Bramble Transport Protocol (BTP) binary packed protocol over TCP (over Tor)
Maturity	1.0 (May 2018)
Platforms	Android
Total users	?