It doesn't rely on any trusted central server, hence it is resilient;

it is based on cryptographic keys and signatures, so it is tamperproof;

it does not rely on P2P techniques, and therefore it works.

Nostr

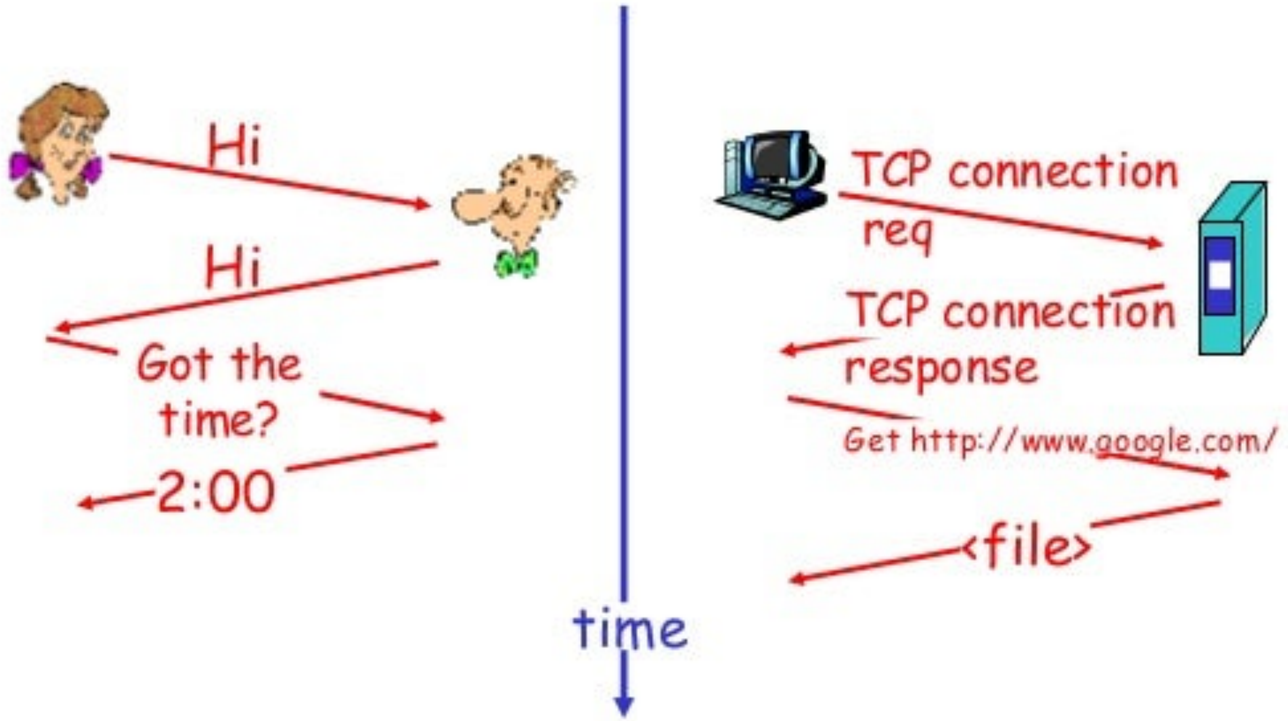
Sammy Javed

Agenda Topics

- What
- Demo
- Why
- How
- Future Possibilities
- Q&A

What's a protocol?

a human protocol and a computer network protocol:

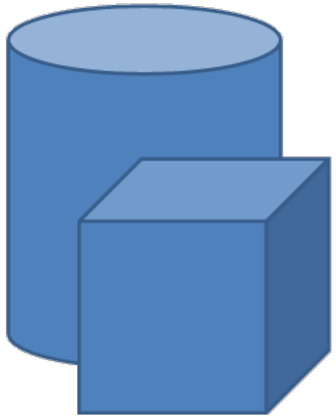


Network Protocols

OSI Ref Model	TCP / IP Protocol Suite
Application	HTTP, HTTPS, SSL, FTP, Telenet Email: SMTP, POP, IMAP
Presentation	
Session	TCP, UDP
Transport	
Network	IP
Datalink	Ethernet, PPP
Physical	

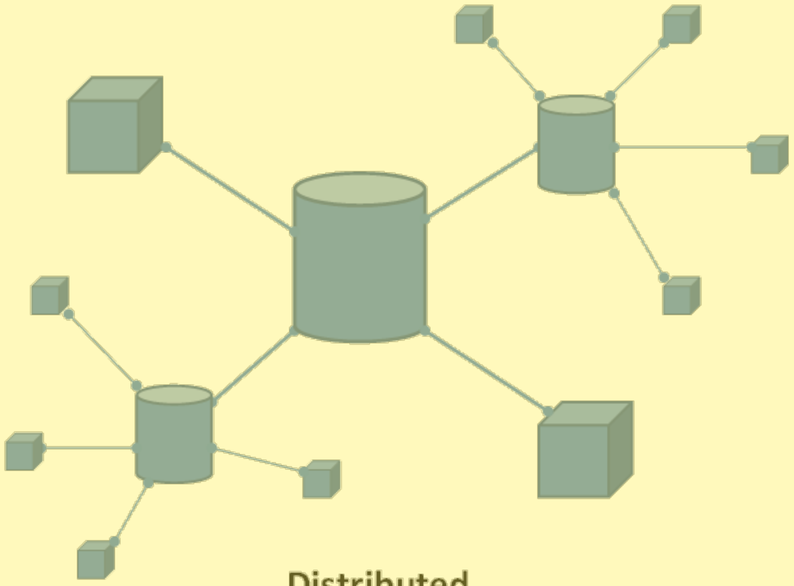
Nostr

Types of Networks



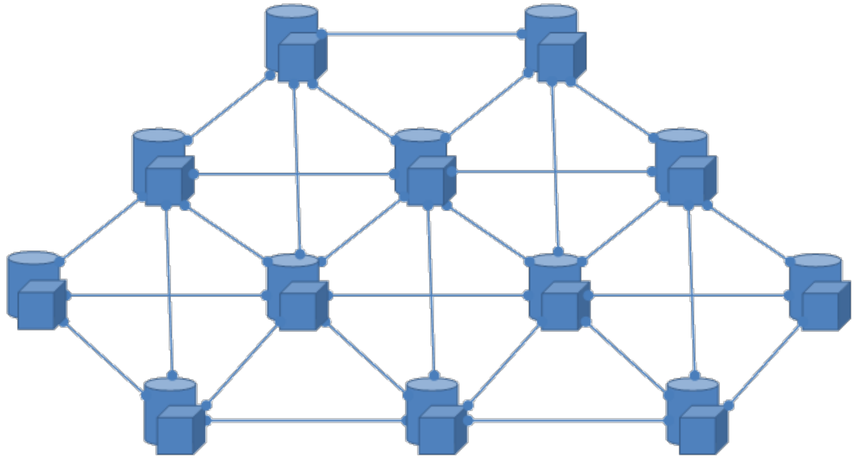
Centralized

one node does everything



Distributed

nodes distribute work to sub-nodes



Decentralized

nodes are only connected to peers

CENTRALIZED NETWORK

WHAT IS CENTRALIZATION?

In a centralized network, there is a central authority that governs and handles the network.

ADVANTAGES

- Command chain
- Reduced costs
- Consistent output

DISADVANTAGES

- Not 100% Trustable
- Single point of failure
- Scalability limitation

DECENTRALIZED NETWORK

WHAT IS DECENTRALIZATION?

In a decentralized network, there is no central authority that governs and handles the network.

ADVANTAGES

- Full control
- Immutable data
- High security

DISADVANTAGES

- Costly
- Misuse of authority
- Volatility

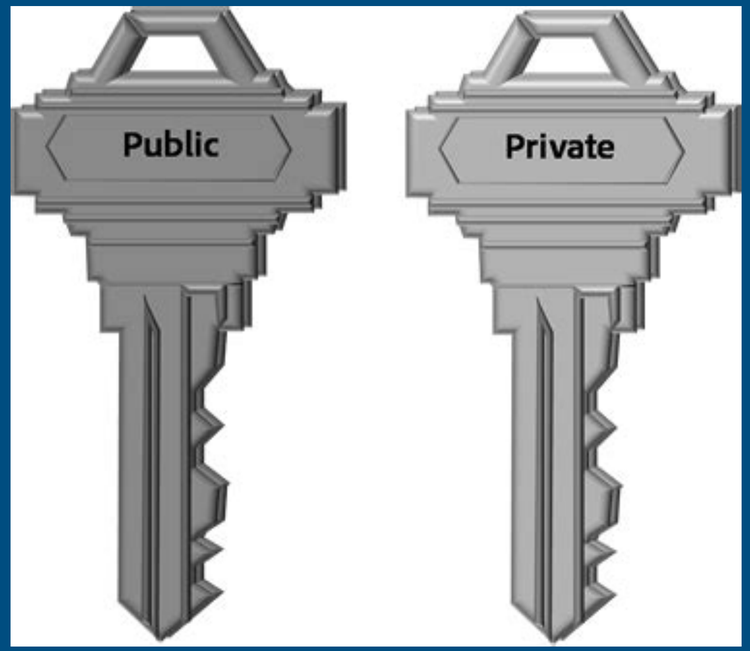
CENTRALIZED VS. DECENTRALIZED

	CENTRALIZED	DECENTRALIZED	
Third-Party Involvement	Yes	No	
Control	Full control stays with the central authority	Control stays with the user itself	
Hackable	More prone to hacks and data leaks	Less prone to hacks and data leaks	
Single Point of Failure	Yes	No	
Ease of Use	Intuitive and easy to use	Not easy to use	
Exchange Fees	Higher fees	Less fees	

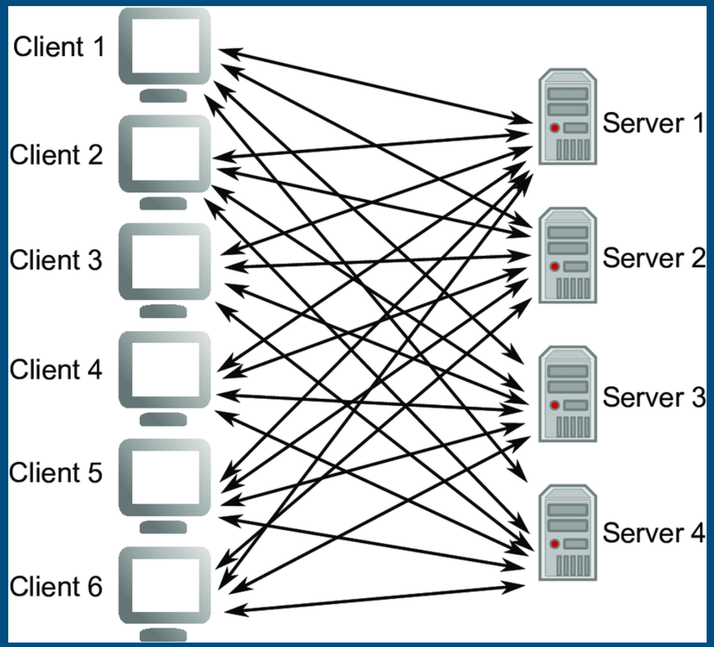
Nostr in 3 Steps

Use Nostr Client

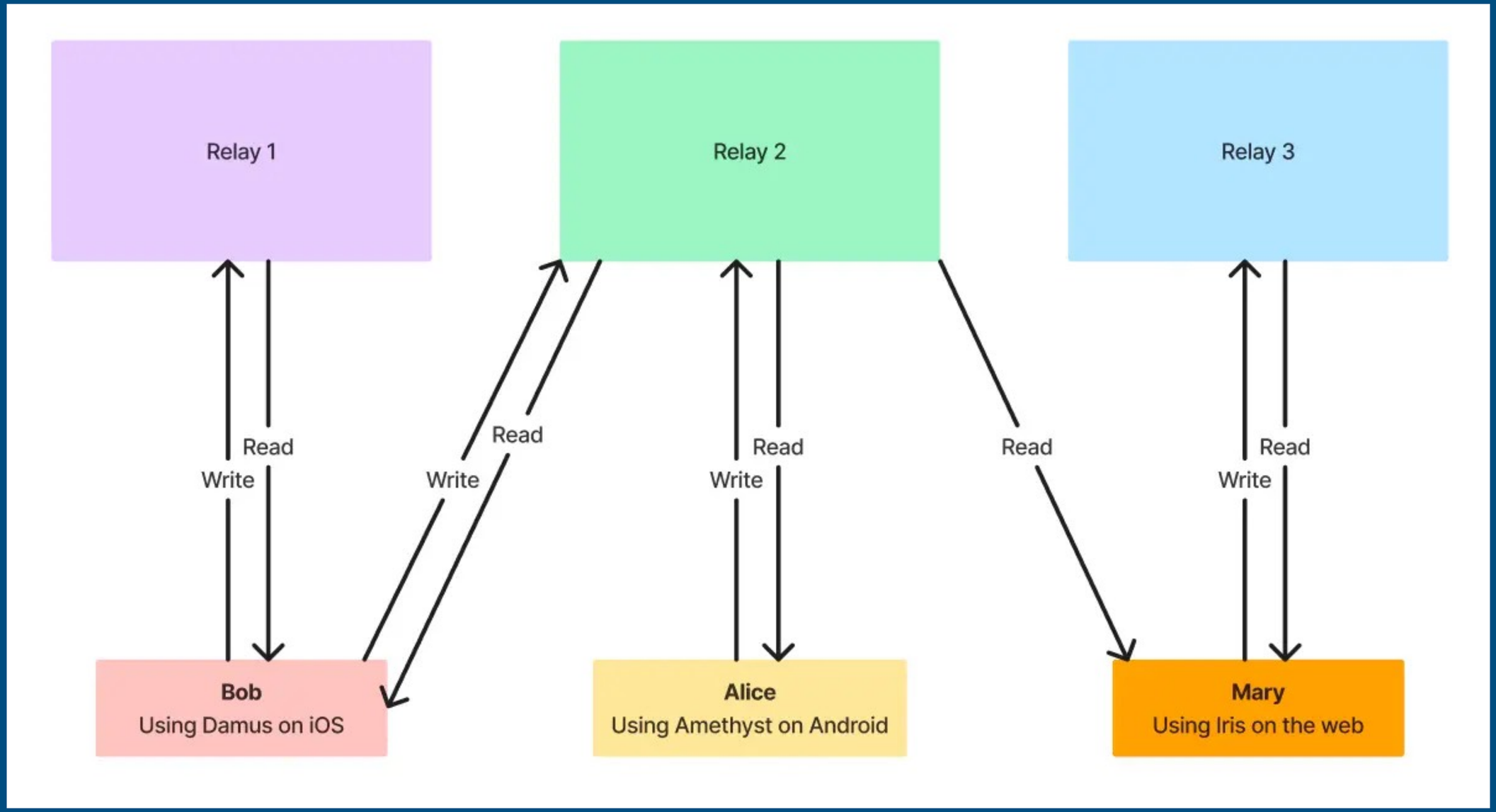
Crypto Identity



Publish to Relays



Nostr Model

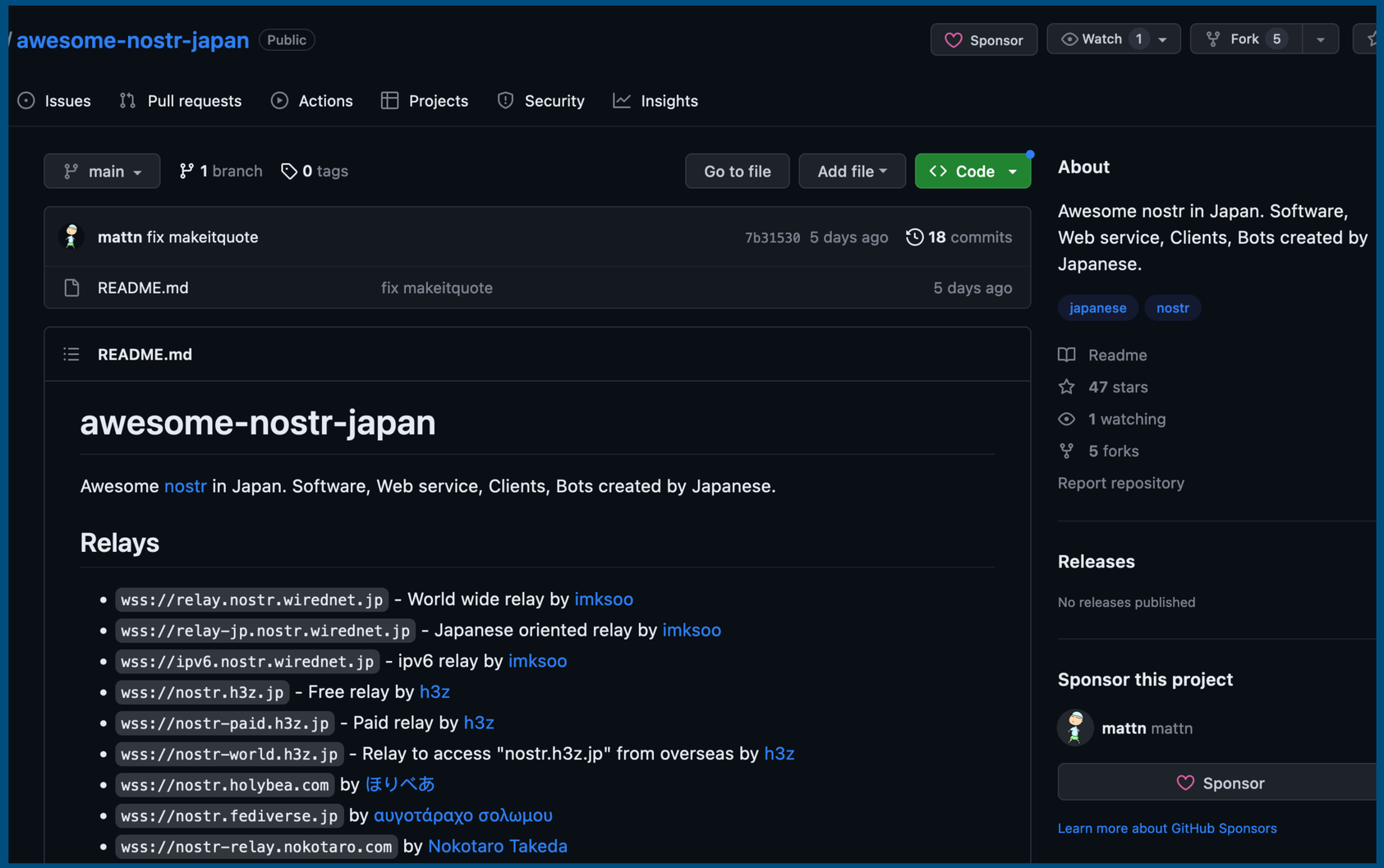

Relay 1
Relay 2
Relay 3
Read
Write
Read
Write
Read
Write
Read
Write
Bob
Using Damus on iOS
Alice
Using Amethyst on Android
Mary
Using Iris on the web

DEMO


8:21
Damus
Welcome to the social network
you control.
Create Account
Login
8:23
Damus
vishalxl 7h
"Well Ordered Wiki has a nice post on #Nostr. Essentially, Nostr is a way to publish content that's signed. each user is expected to publish on their own. It's purposefully kept simple as to make it flexible." - @jimmysong
https://wiki.wellorder.net/post/nostr-intro/
2
2
clightning 11h
You got paid 111 sats for 'LNLink is free software! Buy me a so I can continue my alcoholism-fueled coding adventures.'
clightning 11h
Invoice created: 'LNLink is free software! Buy me a so I can continue my alcoholism-fueled coding adventures.'
jb55 11h
Replying to kr
Welcome! Thanks for trying damus
1
kr 11h
1

Nostr in Japan

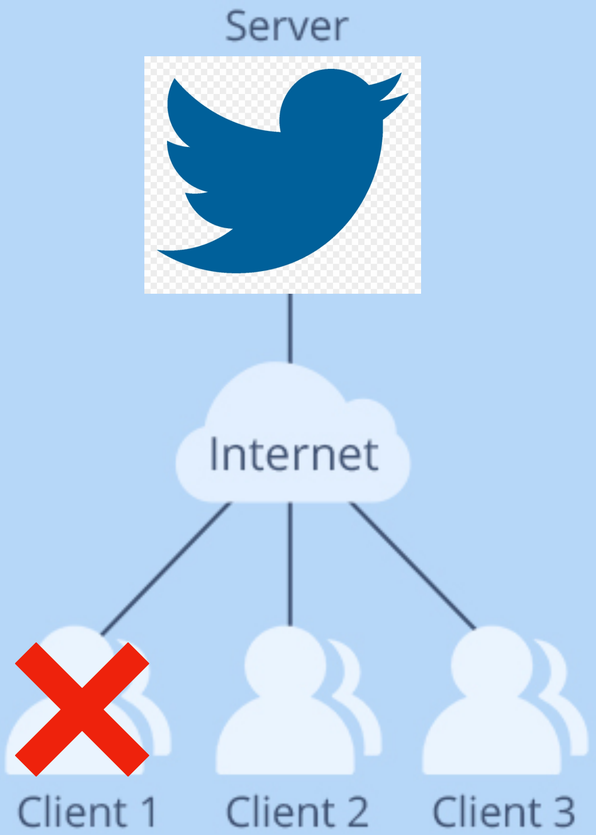
https://github.com/mattn/awesome-nostr-japan



WHY

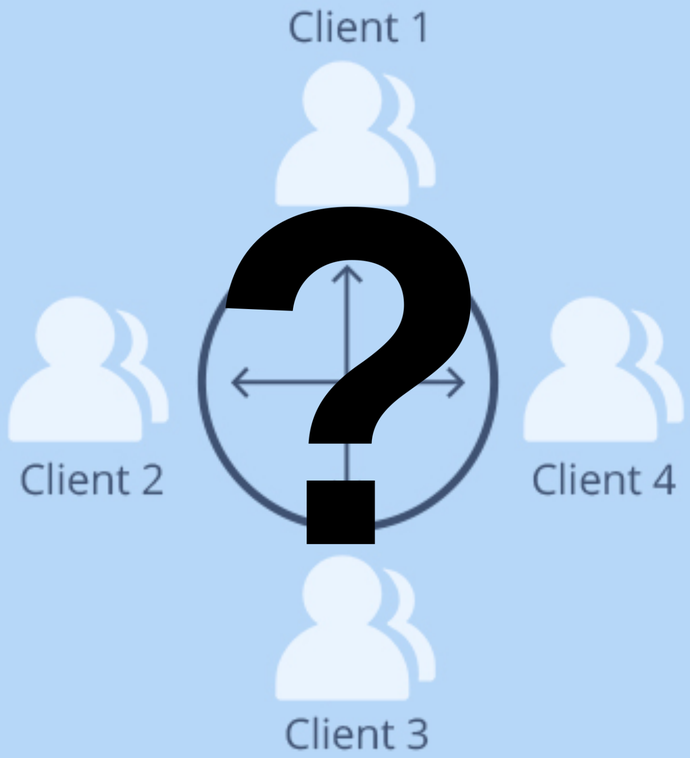
Censorship Resistance

Client-Server Network



VS

Peer-to-Peer Network



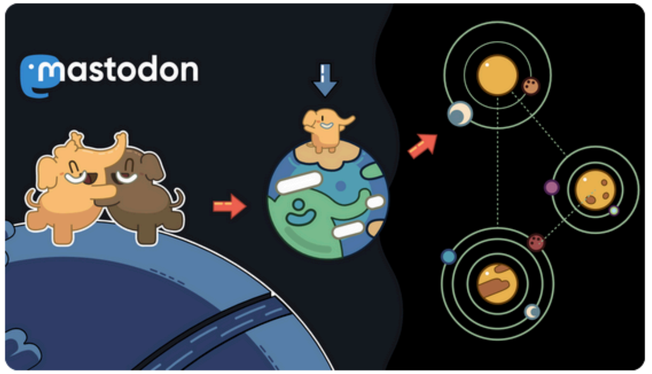
Identity & Instance

GENERAL

mastodon.social

The original server operated by the Mastodon gGmbH non-profit

Create account



GENERAL

mstdn.social

A general-purpose Mastodon server with a 500 character limit. All languages are welcome.

Create account

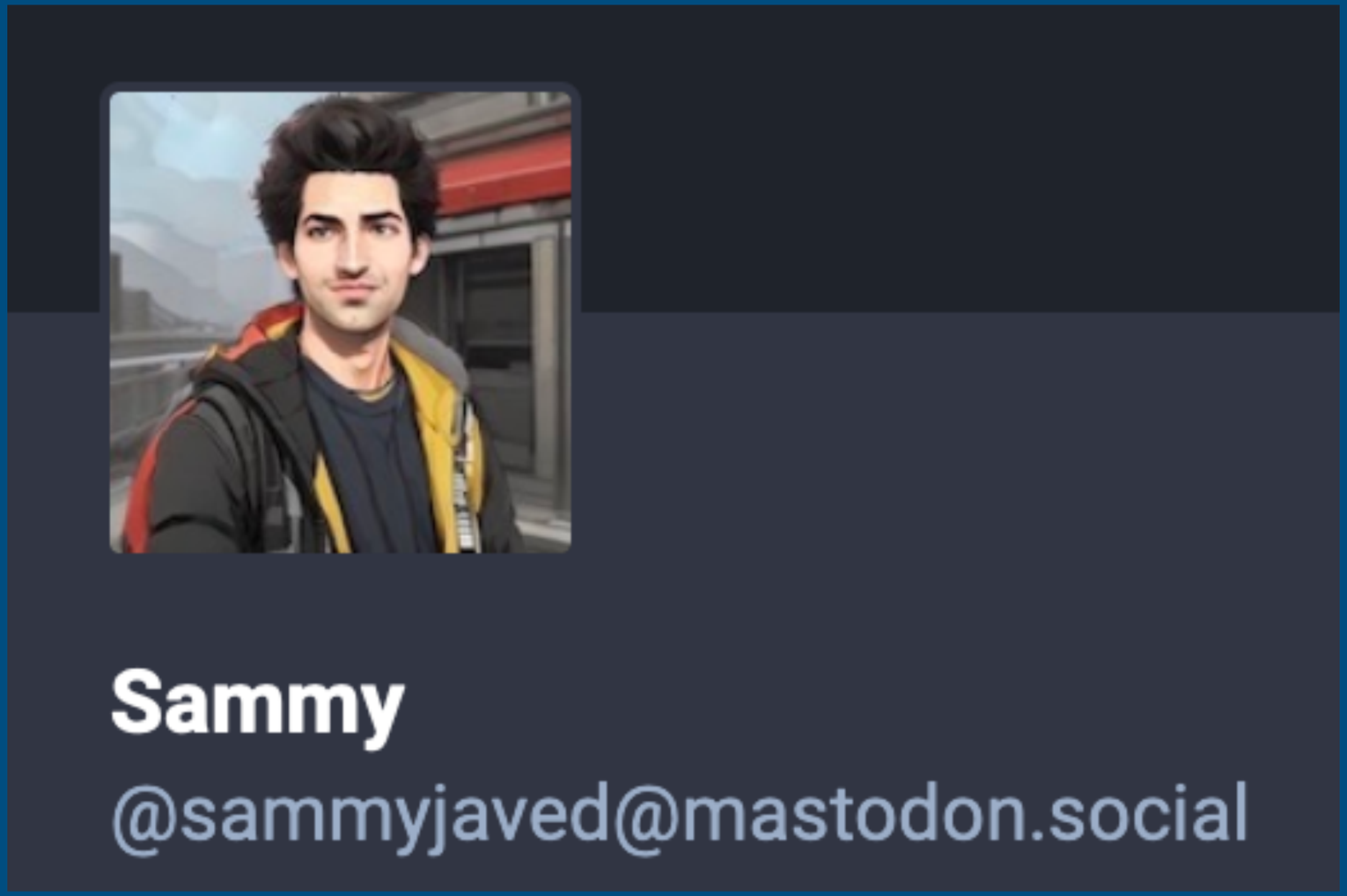
GENERAL

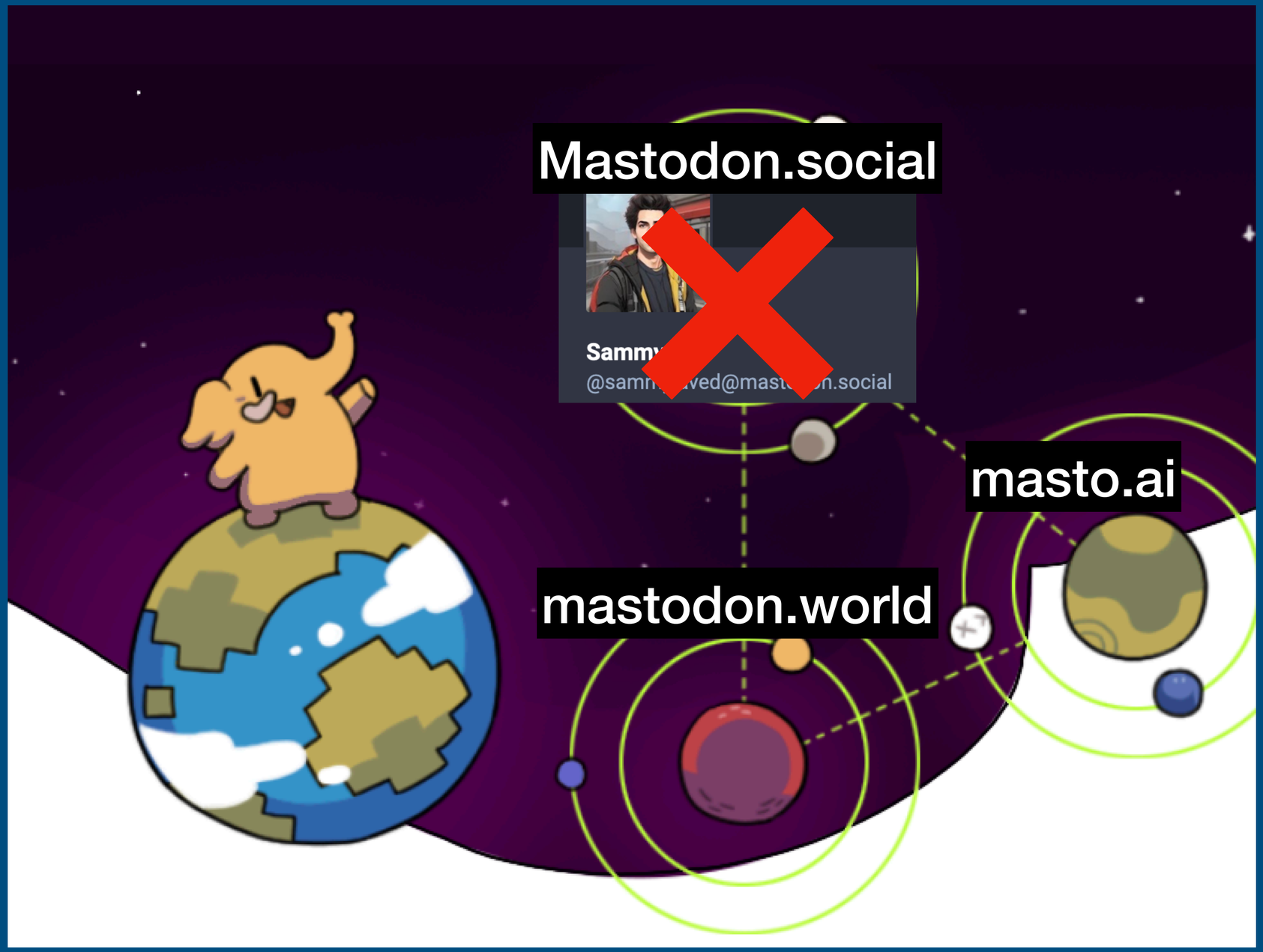
mastodon.world

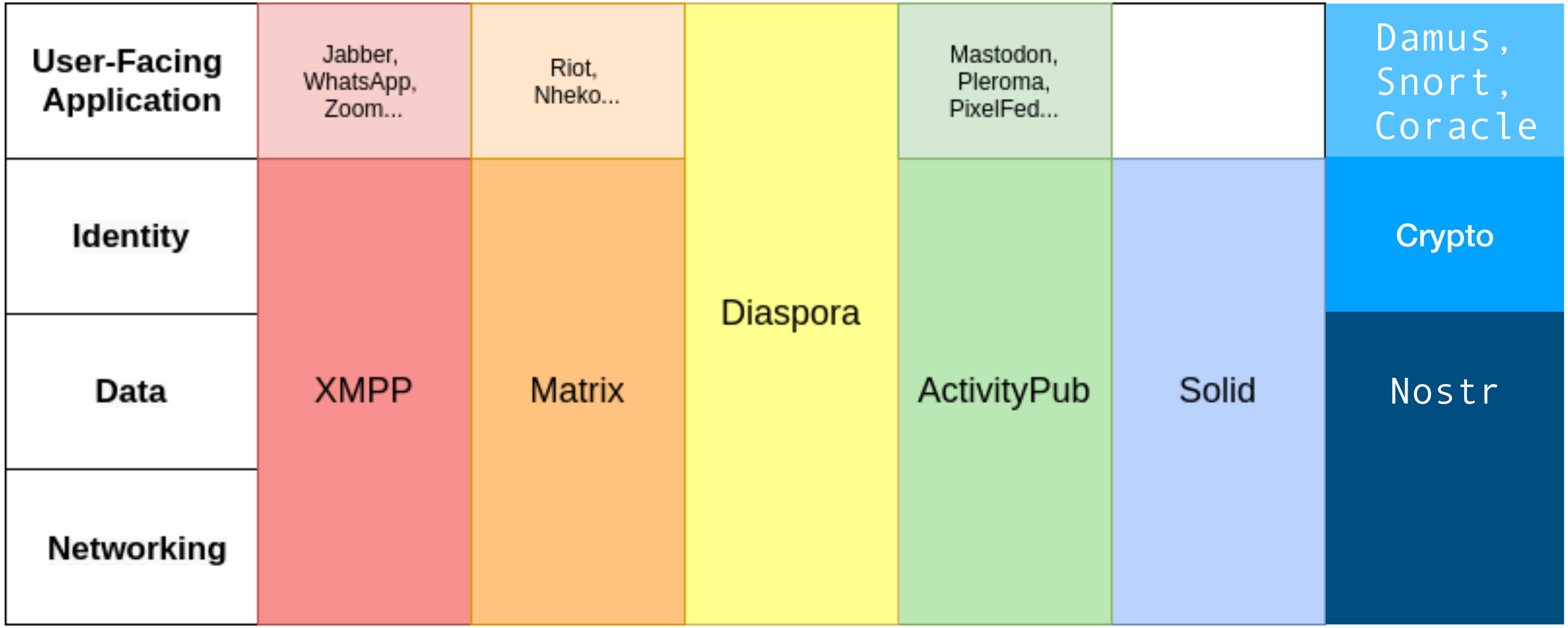
Generic Mastodon server for anyone to use.

Create account

Identity tied to server




Mastodon.social
masto.ai
mastodon.world

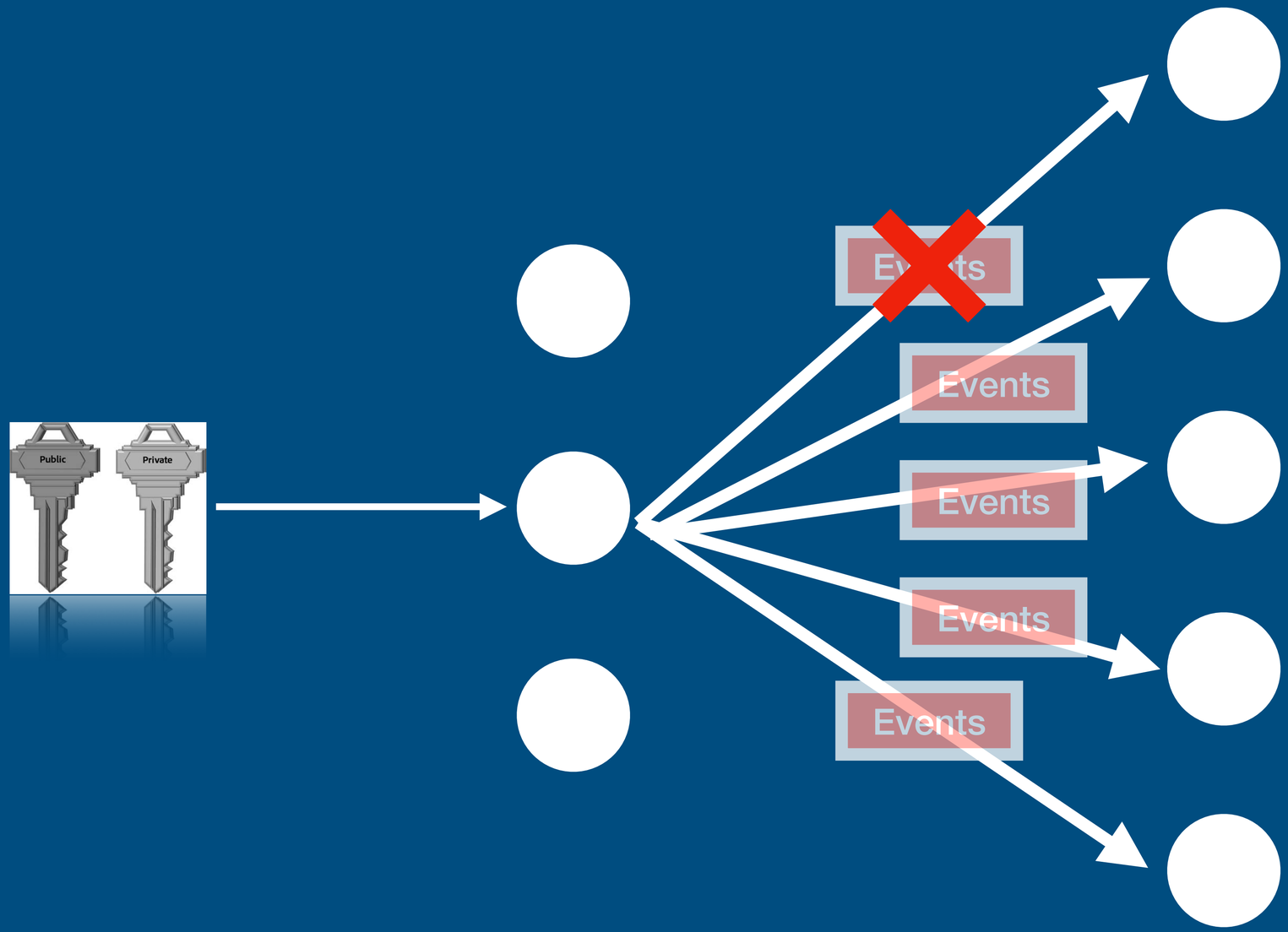

User-Facing Application
Identity
Data
Networking
Jabber, WhatsApp, Zoom...
Riot, Nheko...
Mastodon, Pleroma, PixelFed...
Damus, Snort, Coracle
Crypto
Nostr
XMPP
Matrix
Diaspora
ActivityPub
Solid

Protocol		ActivityPub	XMPP	The AT Protocol
Identity	Crypto	Domain Username + Instance @alice@mastodon.social	Domain alice@example.com	Domain + Crypto?
Network	Distributed	Federated	?	Federated?
Broadcasting	Yes	Possible	Possible	Possible?
Applications	Damus, Snort, etc.		Cisco Jabber Collaborate with video, voice, instant messaging and presence	Bluesky

ID

Client

Relay



HOW

Snort

Login

Your key

nsec, npub, nip-05, hex, mnemonic

Only the secret key can be used to publish (sign events), everything else logs you in read-only mode.

Login

OR

Create an Account

Generate a public / private key pair. Do not share your private key with anyone, this acts as your password. Once lost, it cannot be “reset” or recovered. Keep safe!

Generate Key

Save your keys!

Your private key is your password. If you lose this key, you will lose access to your account! Copy it and keep it in a safe place. There is no way to reset your private key.

Your public key

npub1etpsfzfy9lk...ngq9qfd63q2rz3gj

Your private key

nsec1986kcfzxnkl...aa4glluwqs082d4y

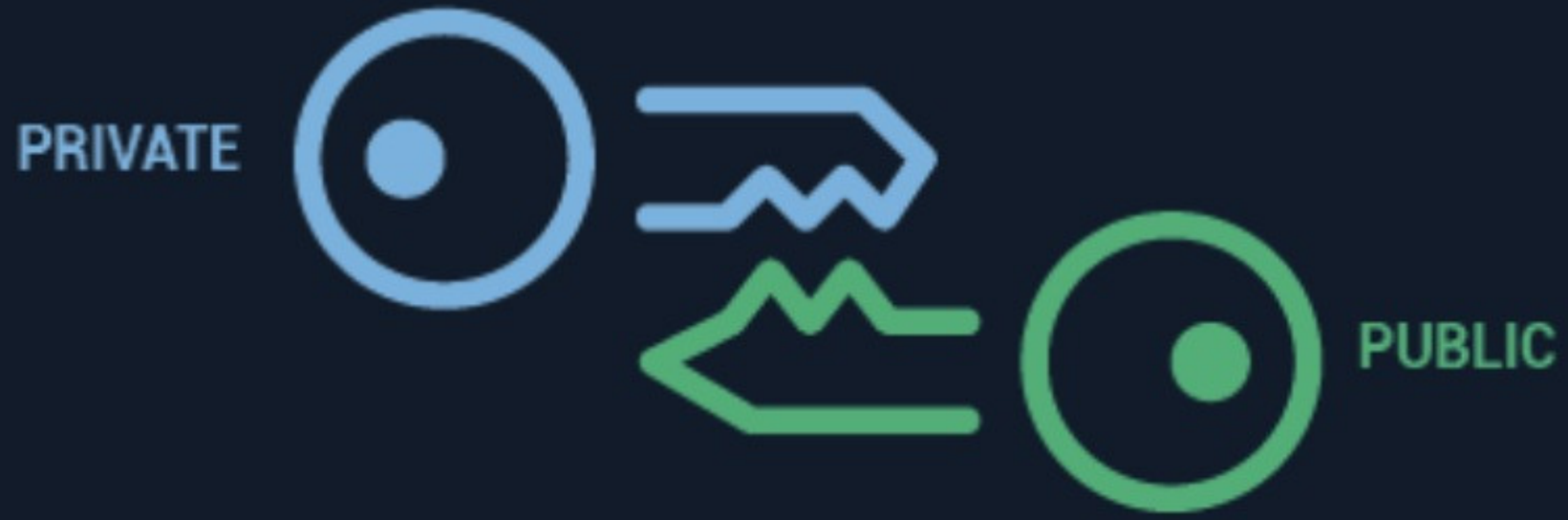
Your mnemonic phrase

buyer toss elega...al net bone pipe

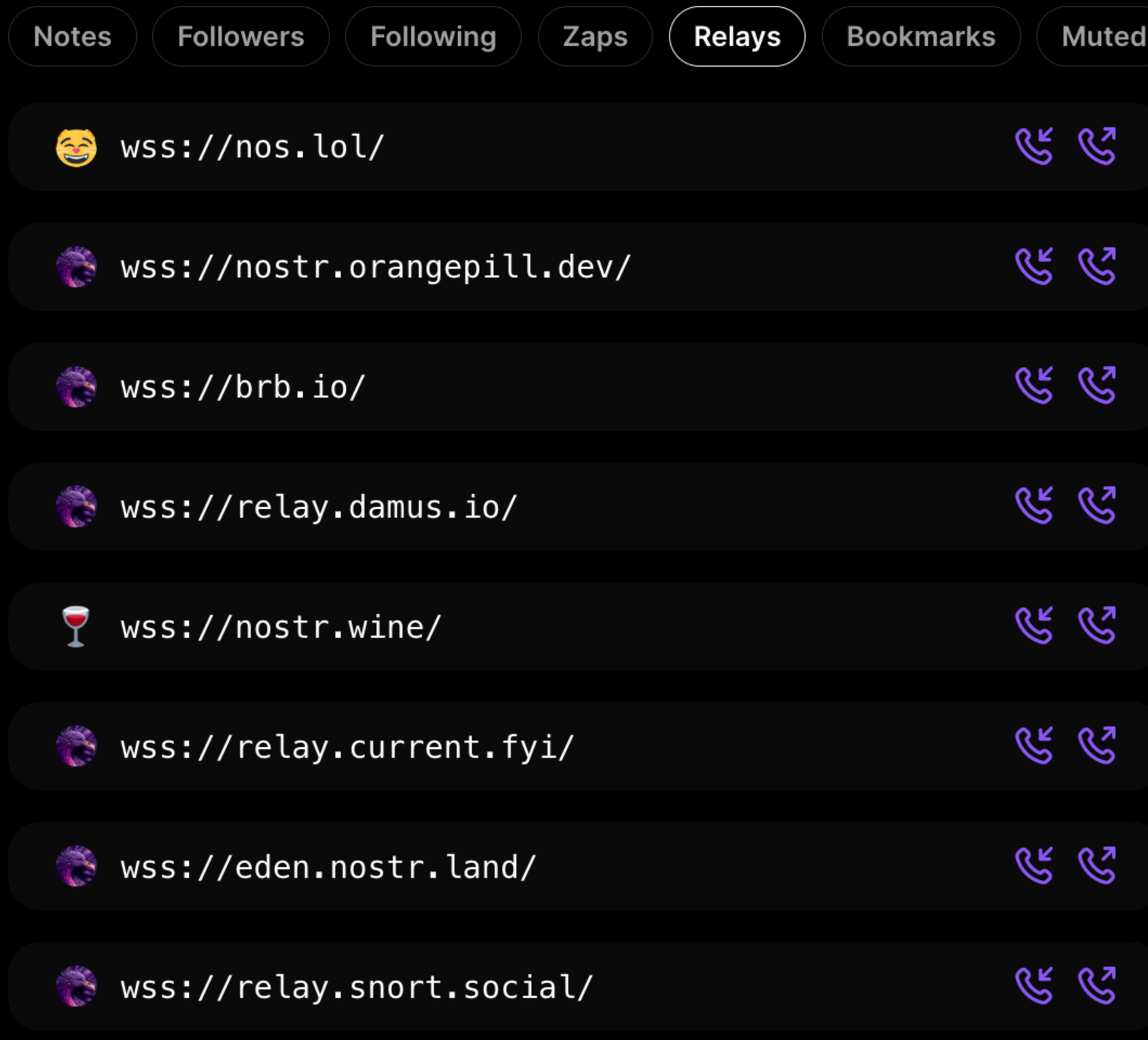
A KEY PAIR

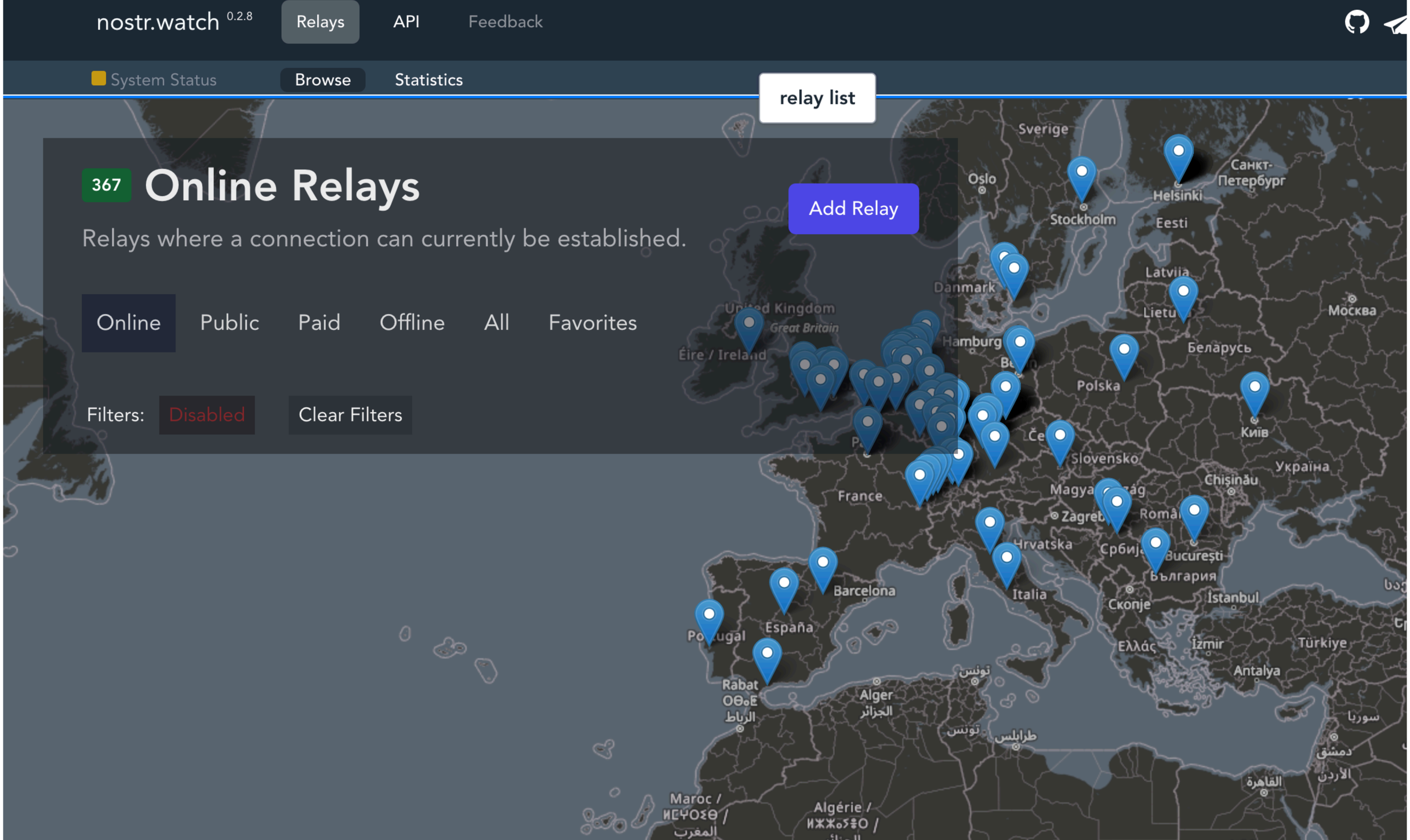
what one key does → *the other will validate*

PUBLIC encrypts	→	**PRIVATE** decrypts
PRIVATE digitally signs	→	**PUBLIC** verifies the signature
PRIVATE authenticates	→	**PUBLIC** verifies the authentication



Connect to relays




nostr.watch 0.2.8
Relays
API
Feedback
System Status
Browse
Statistics
relay list
367 Online Relays
Relays where a connection can currently be established.
Add Relay
Online
Public
Paid
Offline
All
Favorites
Filters: Disabled
Clear Filters
Sverige
Oslo
Stockholm
Helsinki
Санкт-Петербург
Eesti
Latvija
Lietu
Беларусь
Москва
Danmark
United Kingdom
Great Britain
Éire / Ireland
Hamburg
Polska
Київ
Slovensko
Україна
Chișinău
France
Magya
Zagreb
Hrvatska
Србија
București
България
Italia
Barcelona
España
Portugal
Rabat
Alger
الجزائر
تونس
طرابلس
Ελλάς
Skonje
İstanbul
İzmir
Türkiye
Antalya
سوريا
دمشق
الأردن
القاهرة
Maroc /
المغرب
Algérie /

Paid Relay Service Providers

Signup for paid relays, learn what Pay 2 Relay is and why it's important, and visit our FAQ for more info.

Gain Access	Relay wss	Access Fee ⚡	Relay Operator
Pay 2 Relay	wss://eden.nostr.land	5,000	npub16k7j4mwsqm8hakjl8x5ycrqmhx89lxkfwz2xxxcw75eav7sd8ztqy2rwdn
Pay 2 Relay	wss://nostr.milou.lol	1,000	npub1rvg76s0gz535txd9ypg2dfqv0x7a80ar6e096j3v343xdxyrt4ksmkxrck
Pay 2 Relay	wss://puravida.nostr.land	10,000	npub16k7j4mwsqm8hakjl8x5ycrqmhx89lxkfwz2xxxcw75eav7sd8ztqy2rwdn
Pay 2 Relay	wss://relay.nostr.com.au	6,969	npub1qqqqqrre3jxkuyj3s4m59usdyvm0umgm0lpy6cqjtwpt649sdews5q3hw7
Pay 2 Relay	wss://relay.orangepill.dev	4,500	npub16jzr7npgp2a684pasnkhjf9j2e7hc9n0teefskulqmf42cqmt4uqwszk52

Settings

Relays

no-str.org	0 ms	0 ⚠ 0	Write ☑ Read ☑
nostr.pinkanki.org	0 ms	0 ⚠ 0	Write ☑ Read ☑
nostr.hrmb.org	0 ms	17 ⚠ 0	Write ☑ Read ☑
nostr.lu.ke	0 ms	0 ⚠ 0	Write ☑ Read ☑
relay.snort.social	0 ms	10 ⚠ 0	Write ☑ Read ☑
nostr.wine	0 ms	0 ⚠ 0	Write ☒ Read ☑
nos.lol	0 ms	0 ⚠ 0	Write ☑ Read ☑

Save

Run your own relay

https://nostr.com/relays/implementations

Most used in the wild

- **nostr-rs-relay**, a minimalistic, optimized relay written in Rust that uses SQLite.
- **nostream**, A Nostr relay written in Typescript backed by PostgreSQL and Redis, optimized for load-balancing and fault-tolerance.
- **me.untethr.nostr-relay**, a very strict and performant relay written in Clojure, uses SQLite.
- **strfry**, a very performant relay written in C++, uses LMDB for data storage and comes with a built-in set-reconciliation mechanism for syncing.

Events and signatures

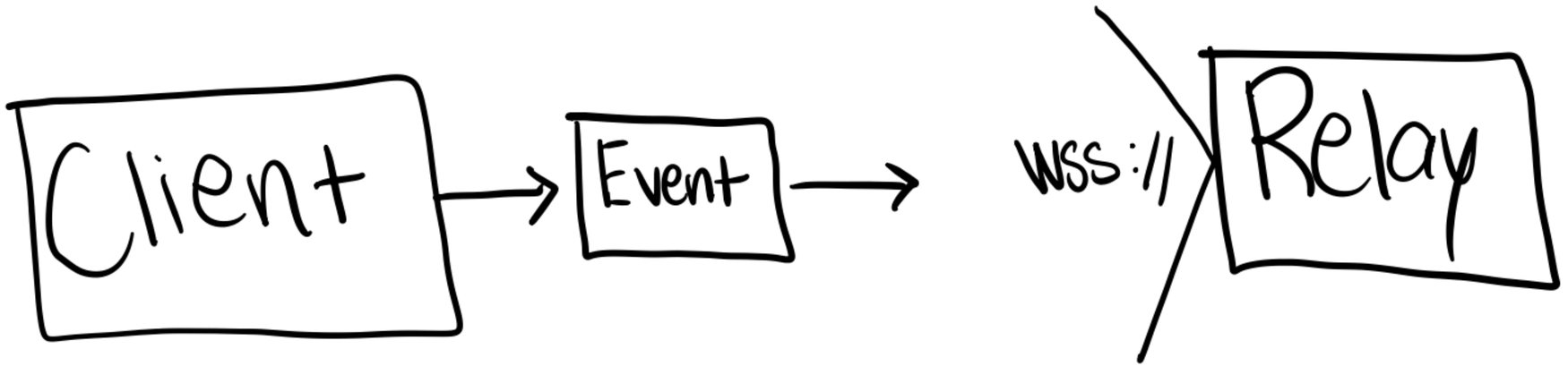
Each user has a keypair. Signatures, public key, and encodings are done according to the Schnorr signatures standard for the curve `secp256k1`.

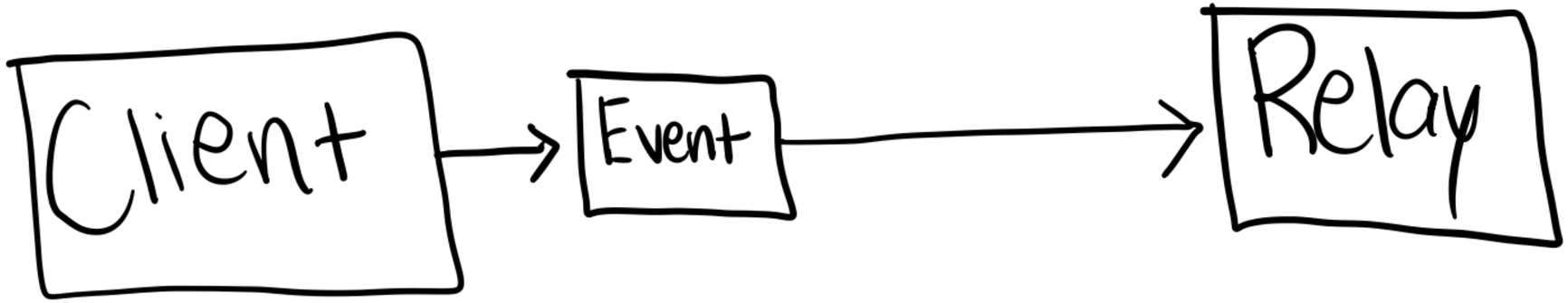
The only object type that exists is the `event`, which has the following format on the wire:

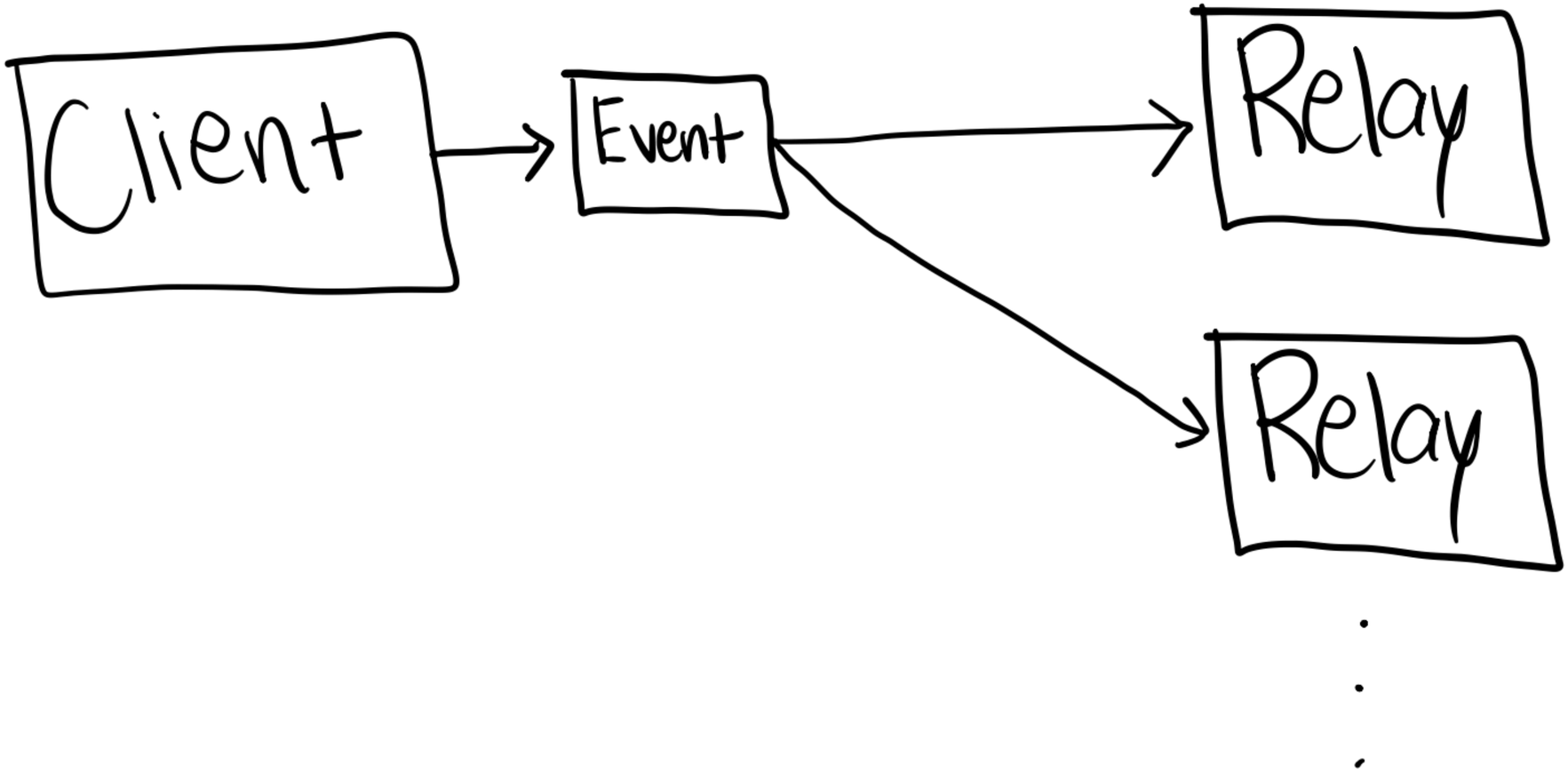
```
{
  "id": <32-bytes lowercase hex-encoded sha256 of the serialized event data>
  "pubkey": <32-bytes lowercase hex-encoded public key of the event creator>,
  "created_at": <unix timestamp in seconds>,
  "kind": <integer>,
  "tags": [
    ["e", <32-bytes hex of the id of another event>, <recommended relay URL>],
    ["p", <32-bytes hex of a pubkey>, <recommended relay URL>],
    ... // other kinds of tags may be included later
  ],
  "content": <arbitrary string>,
  "sig": <64-bytes hex of the signature of the sha256 hash of the serialized event data, which is the same as the "id" fie
}
```

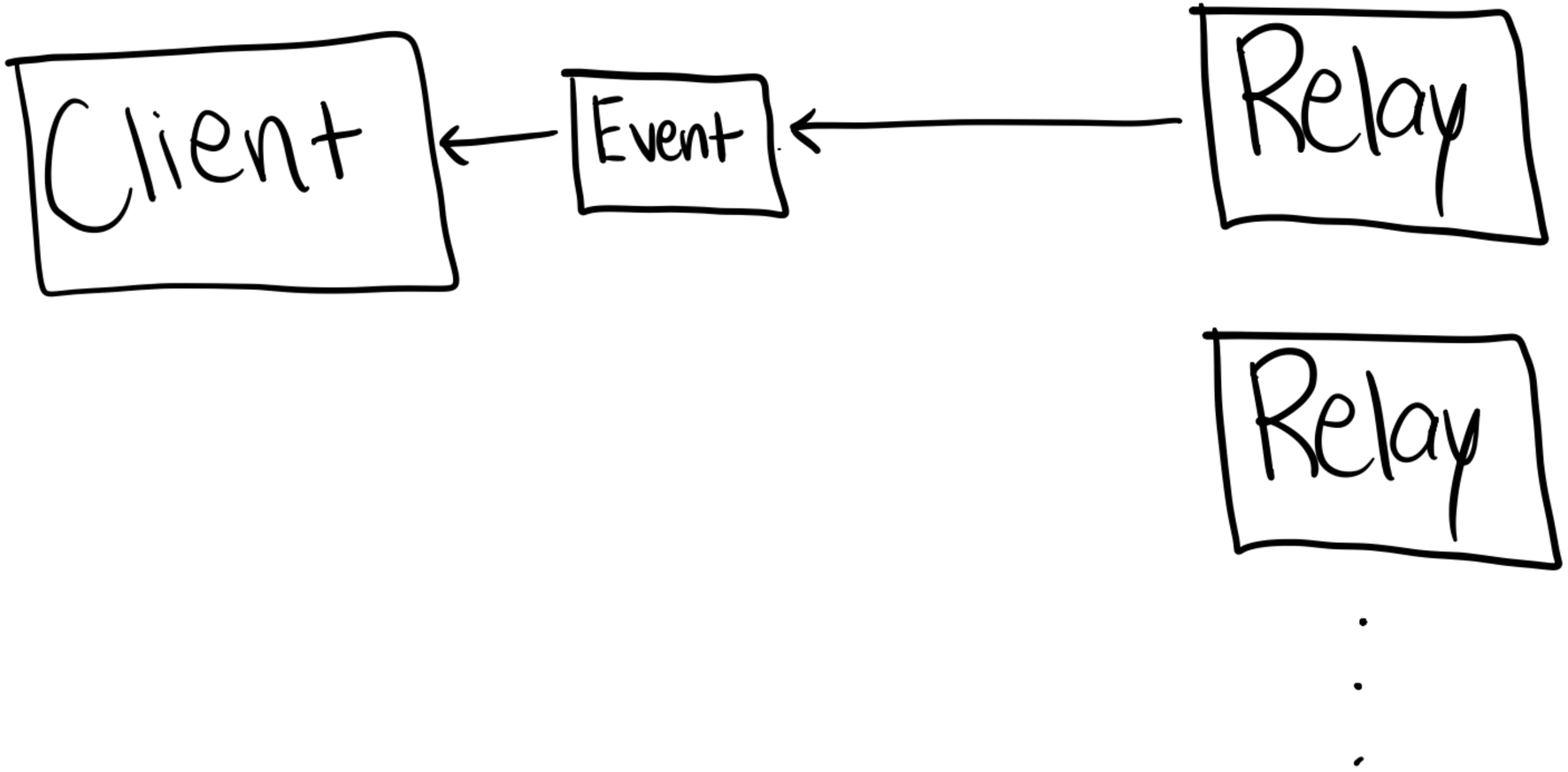

Client

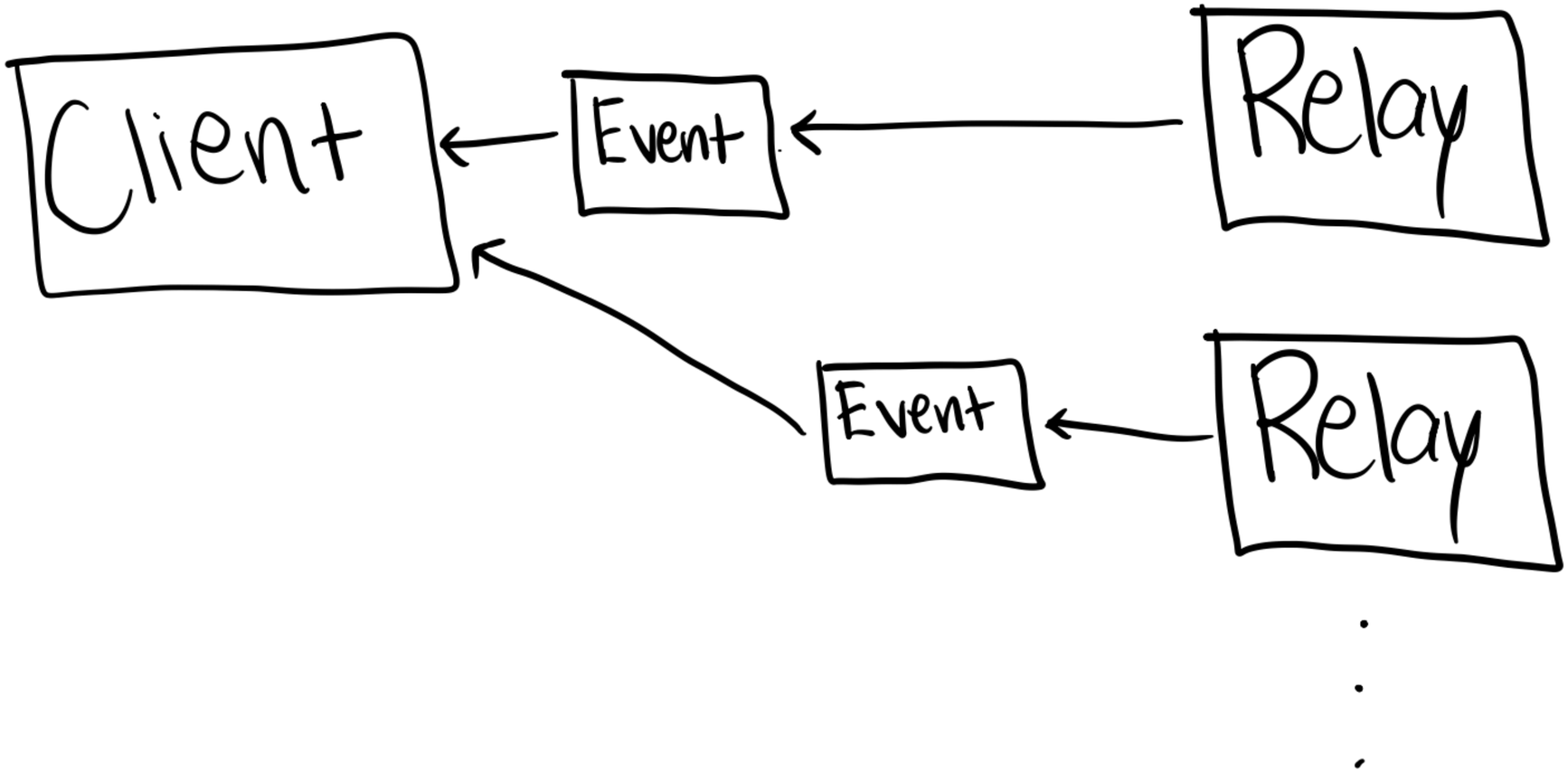

Relay

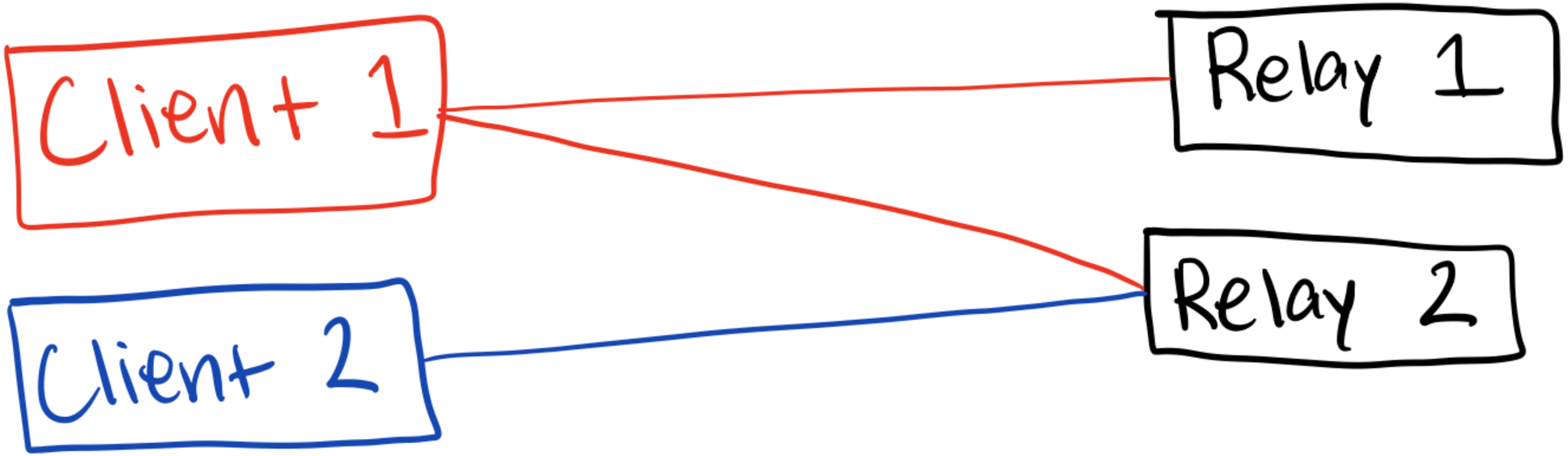

Client
Event
wss://
Relay

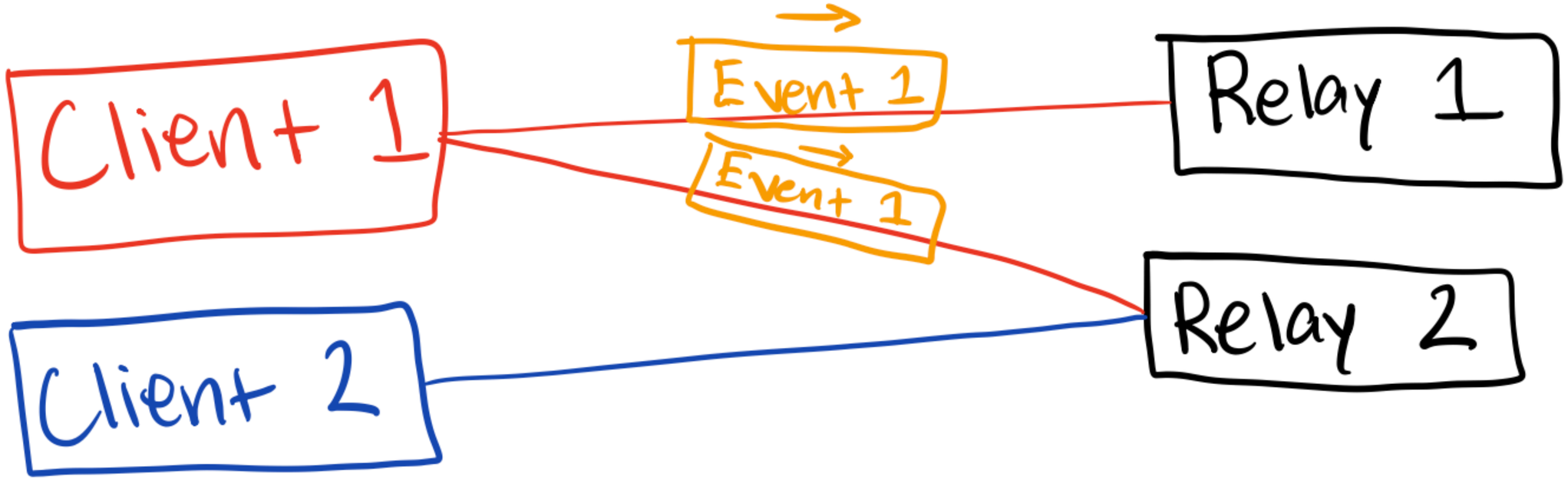

Client
Event
Relay

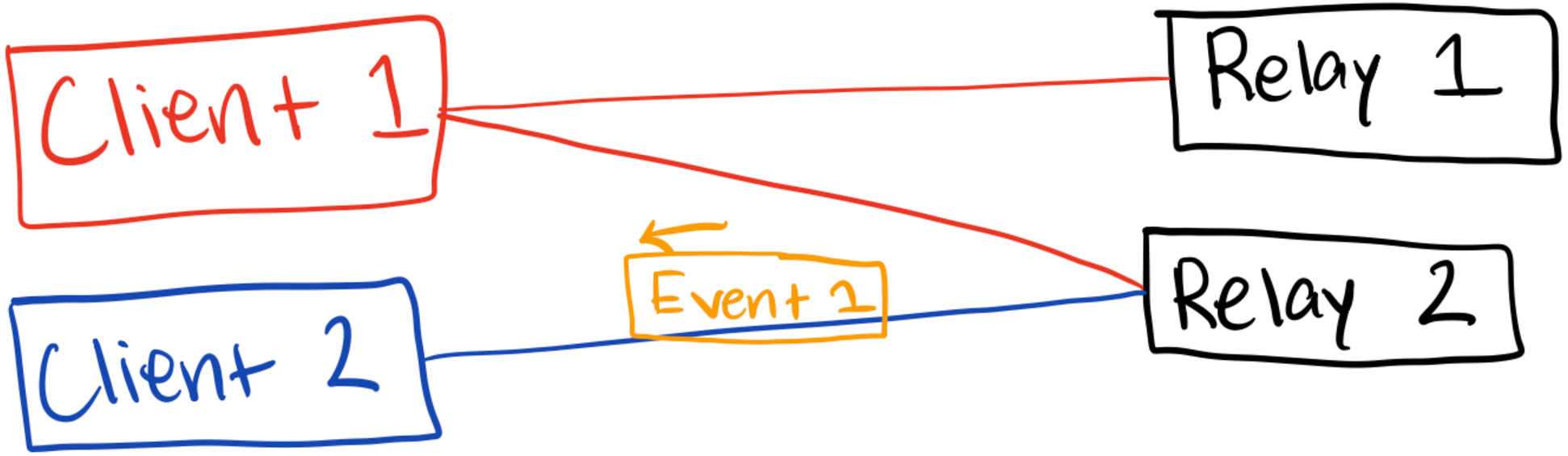

Client
Event
Relay
Relay

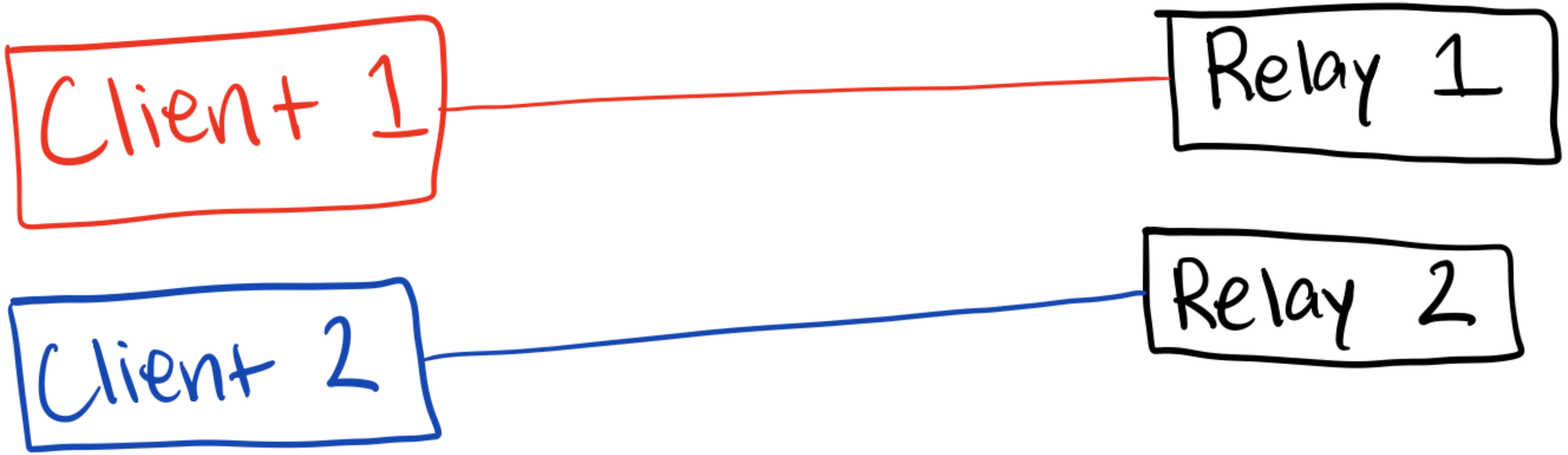

Client
Event
Relay
Relay

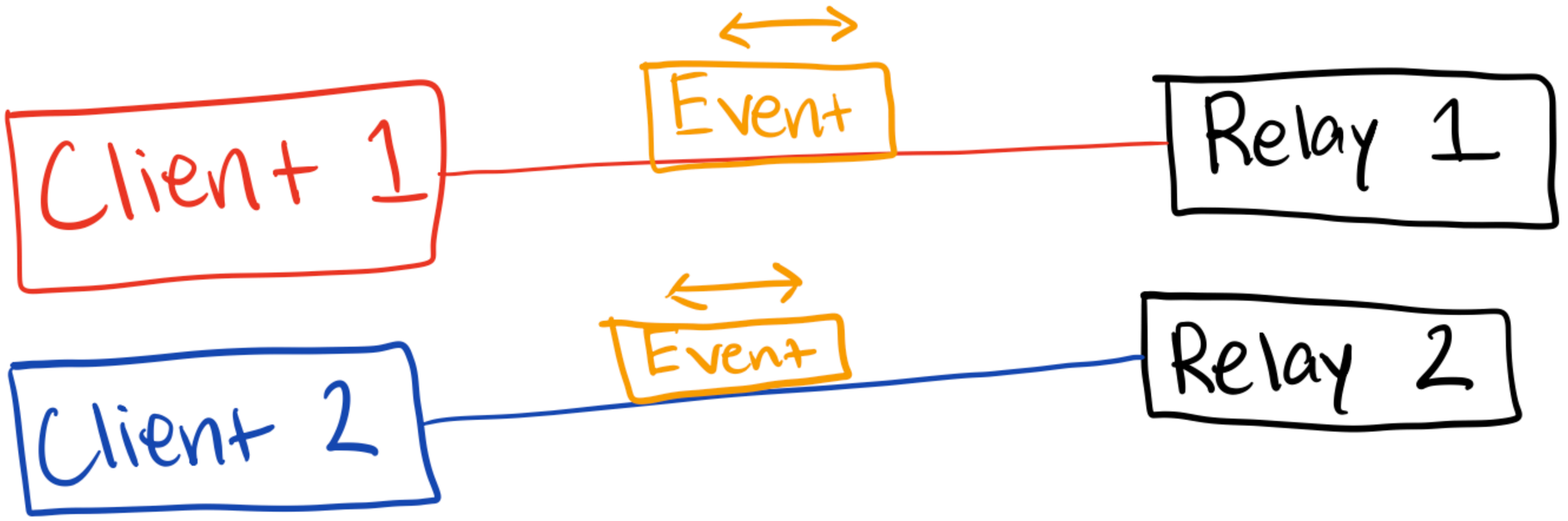

Client
Event
Relay
Event
Relay


Client 1
Client 2
Relay 1
Relay 2


Client 1
Client 2
Event 1
Event 1
Relay 1
Relay 2


Client 1
Client 2
Event 1
Relay 1
Relay 2


Client 1
Relay 1
Client 2
Relay 2



No Shared relays = No Shared events

FUTURE POSSIBILITIES

NIPs

NIPs stand for **Nostr Implementation Possibilities**. They exist to document what may be implemented by Nostr-compatible *relay* and *client* software.

- NIP-01: Basic protocol flow description
- NIP-02: Contact List and Petnames
- NIP-03: OpenTimestamps Attestations for Events
- NIP-04: Encrypted Direct Message
- NIP-05: Mapping Nostr keys to DNS-based internet identifiers
- NIP-06: Basic key derivation from mnemonic seed phrase
- NIP-07: `window.nostr` capability for web browsers
- NIP-08: Handling Mentions – `unrecommended`: deprecated in favor of NIP-27
- NIP-09: Event Deletion
- NIP-10: Conventions for clients' use of `e` and `p` tags in text events
- NIP-11: Relay Information Document
- NIP-12: Generic Tag Queries
- NIP-13: Proof of Work

https://github.com/nostr-protocol/nips

App Ecosystem

Social

Damus
A popular social client for iOS

Snort
Make Nostr sexy.

Iris
Nostr client for better social networks

Amethyst
Amethyst brings the best decentralized social network to your Android phone.

Writing

Habla
A long form content client for nostr notes.

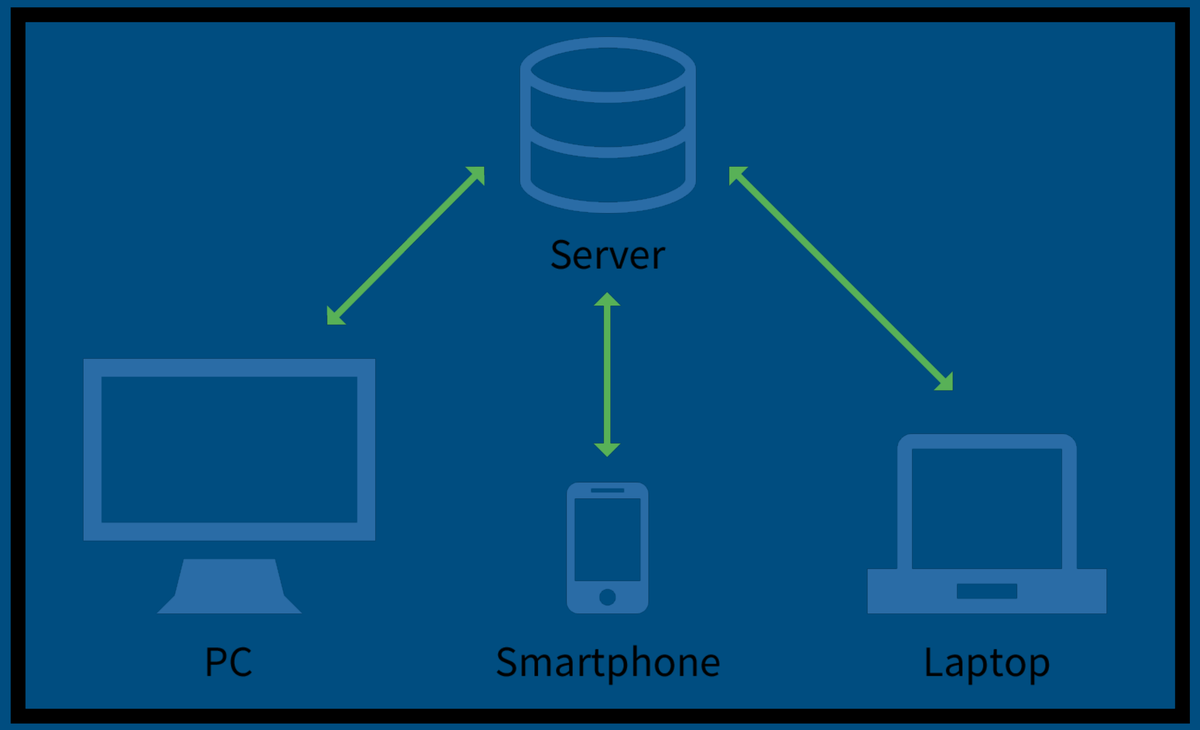
Blogstack
Decentralized blogs over relay using nostr w/ ⚡ lightning tips

Music & Podcasting

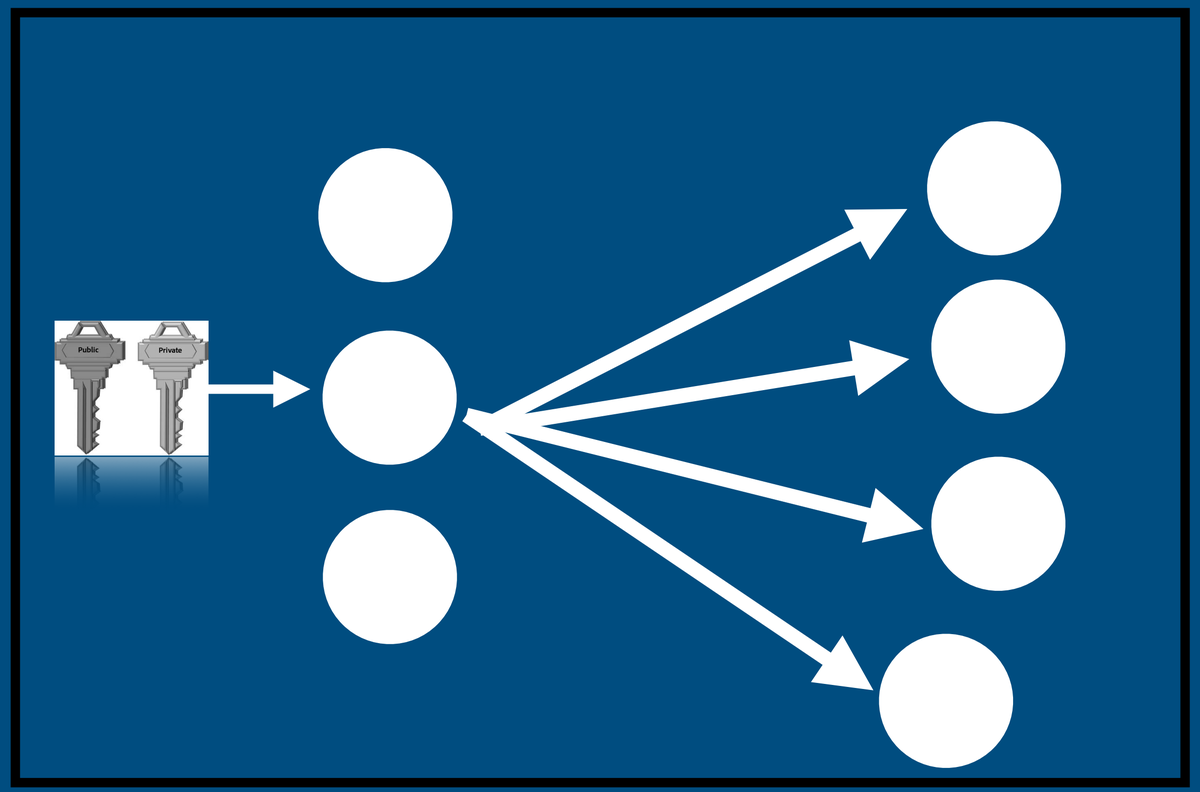
Fountain
The podcast app that pays.

Decoupling Identity, Frontend, Backend

Client-Server

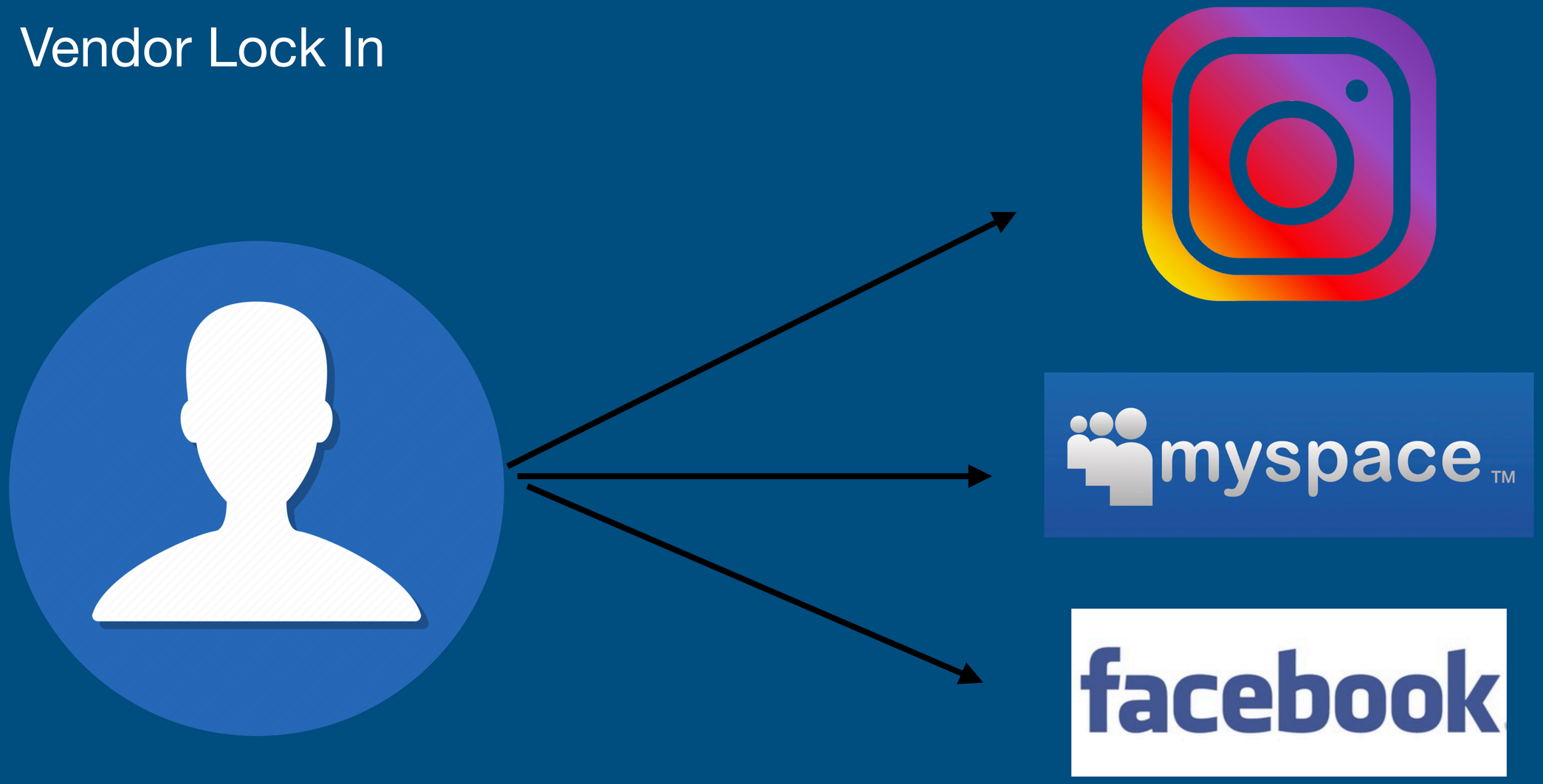


Clients-Relays



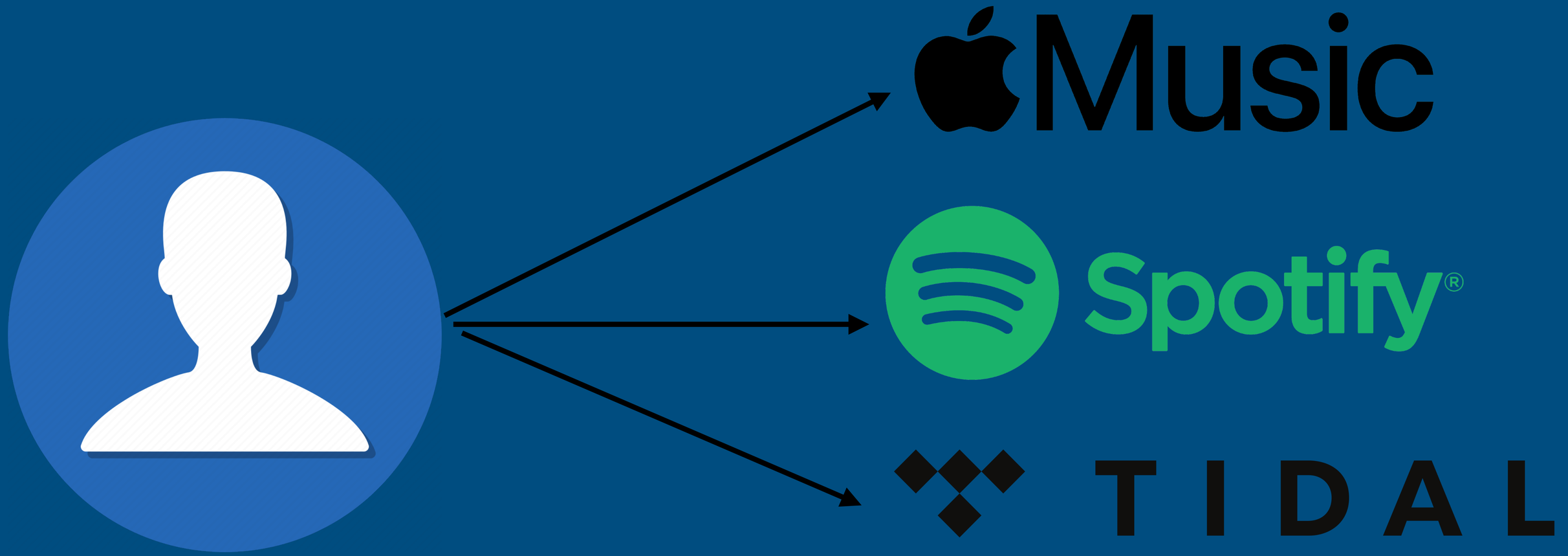
Social Media

Vendor Lock In



Music

Add song to library



Broadcast our ToS

Resources

Nostr and other distributed protocols

- Decentralized ecosystem overview from Bluesy
- A curated list of nostr projects and resources
- Learn more about Nostr: https://nostr.how/
- Bluesky @ AT Protocol: https://atproto.com/guides/overview
- Mastodon and the Fediverse: https://docs.joinmastodon.org/

Q & A