

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

IMPERCCE

Sammy Javed

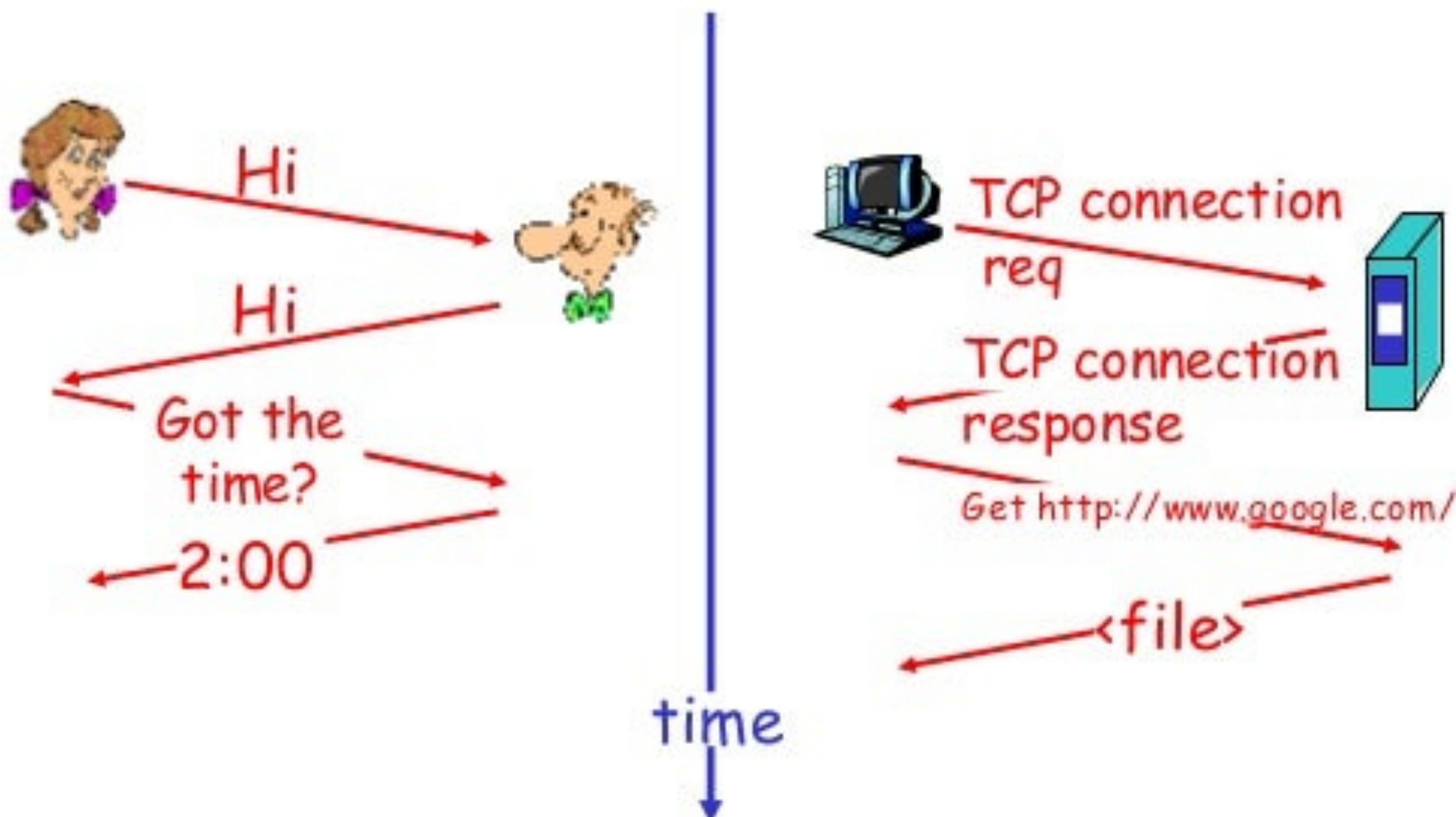
Agenda Topics

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



What's a protocol?

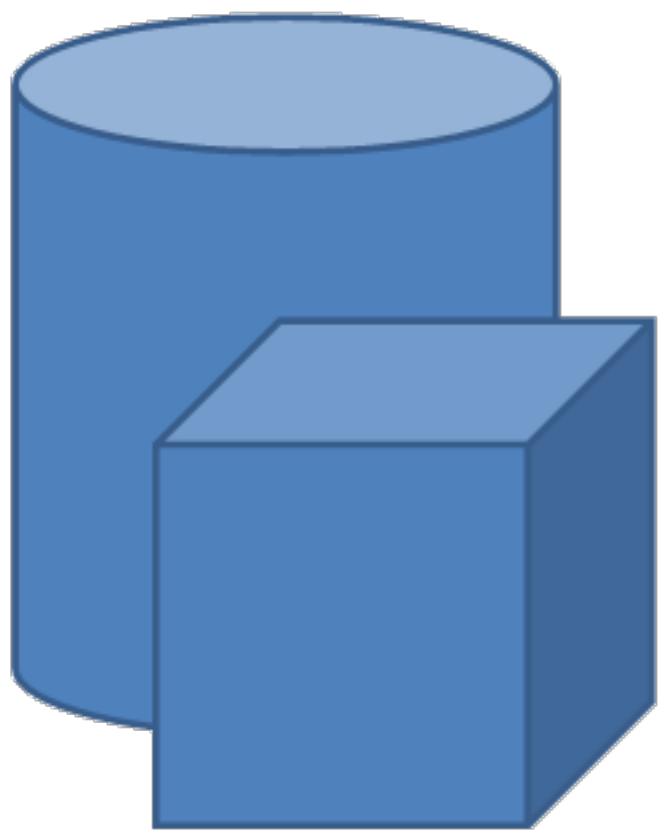
a human protocol and a computer network protocol:



Network Protocols

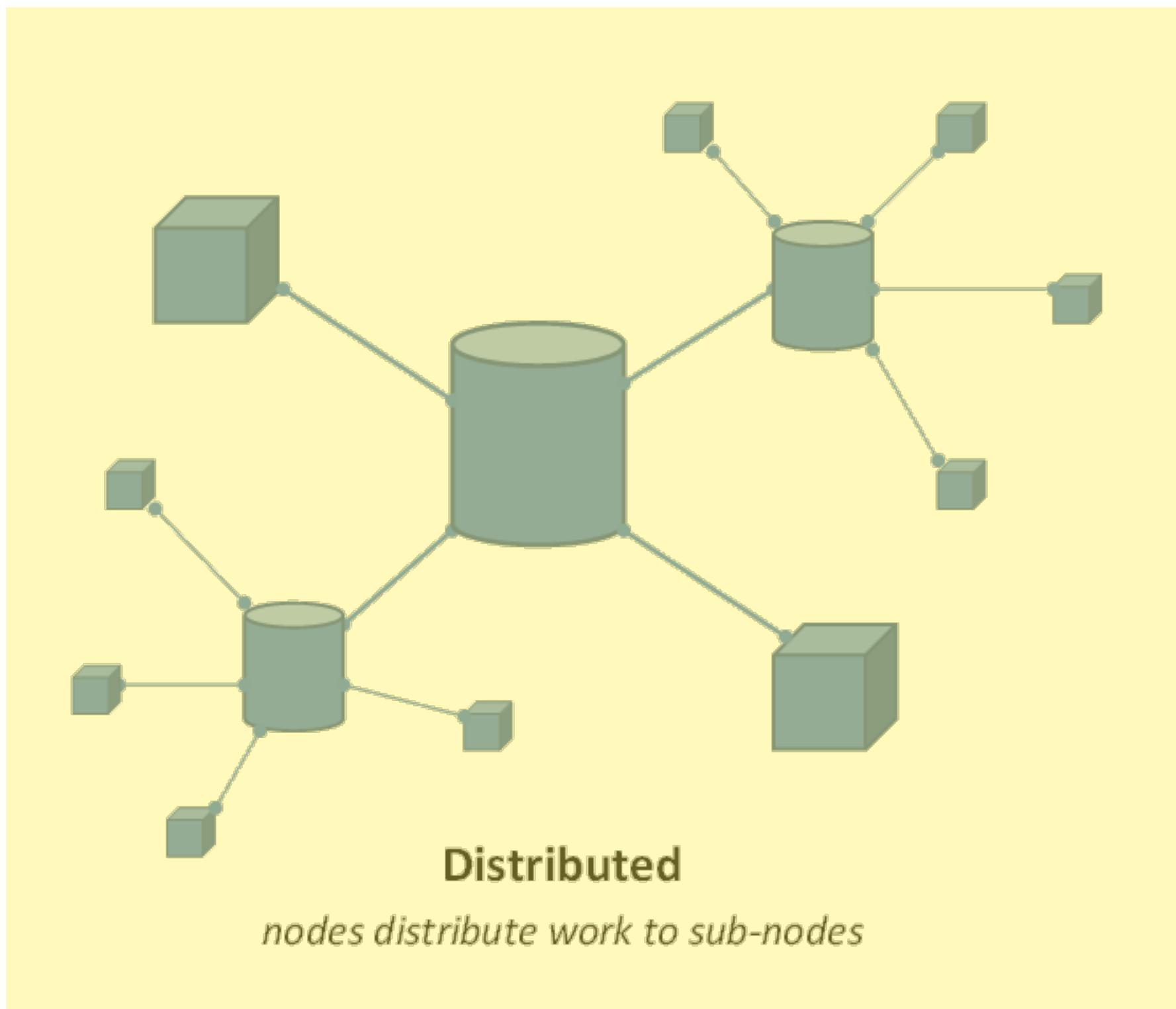
OSI Ref Model	TCP / IP Protocol Suite	
Application	HTTP, HTTPS, SSL, FTP, Telenet Email: SMTP, POP, IMAP	Nostr
Presentation		
Session	TCP, UDP	
Transport		
Network	IP	
Datalink	Ethernet, PPP	
Physical		

Types of Networks



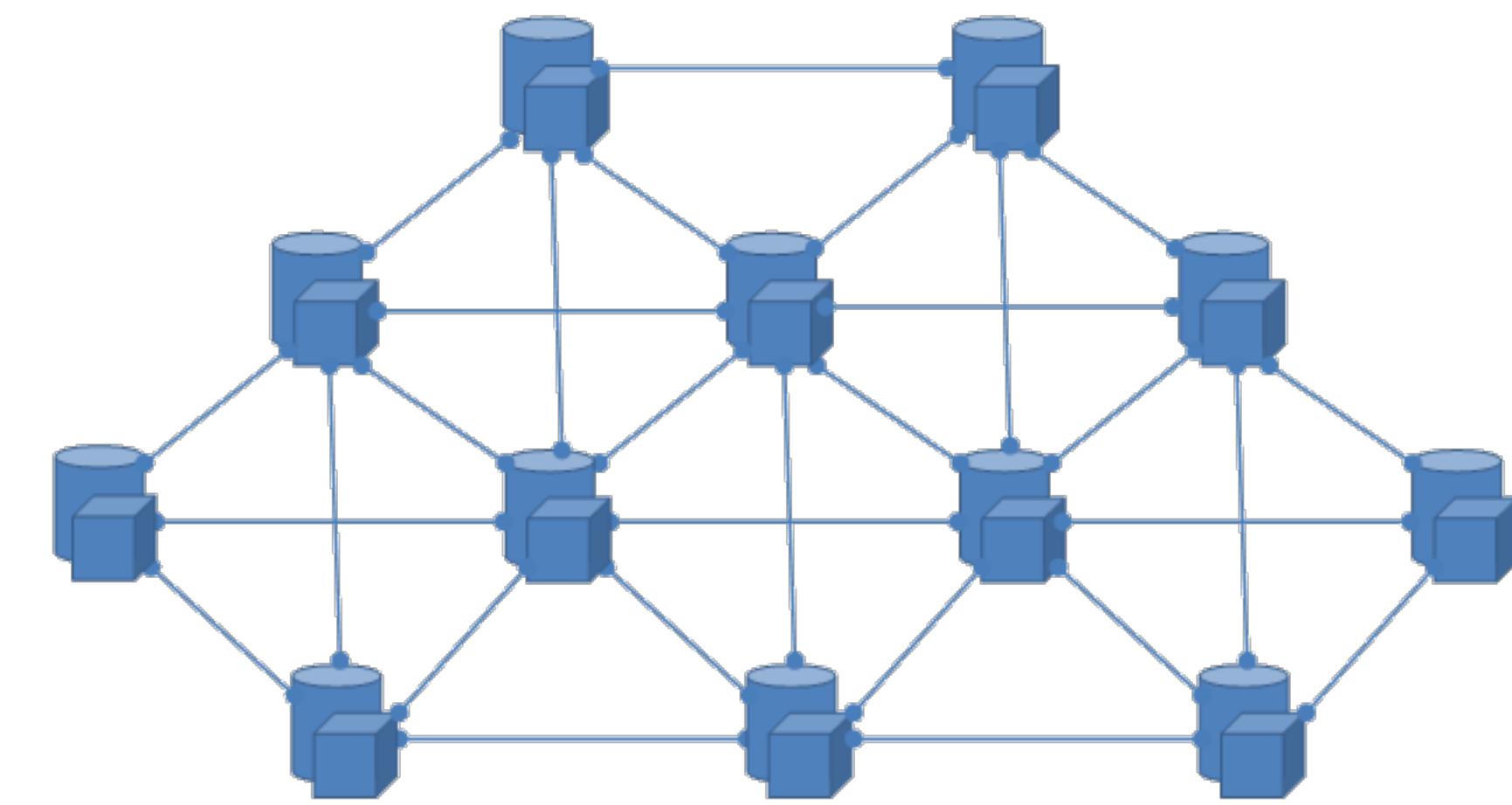
Centralized

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.

WHAT IS DECENTRALIZATION?

In a decentralized network, there is no 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

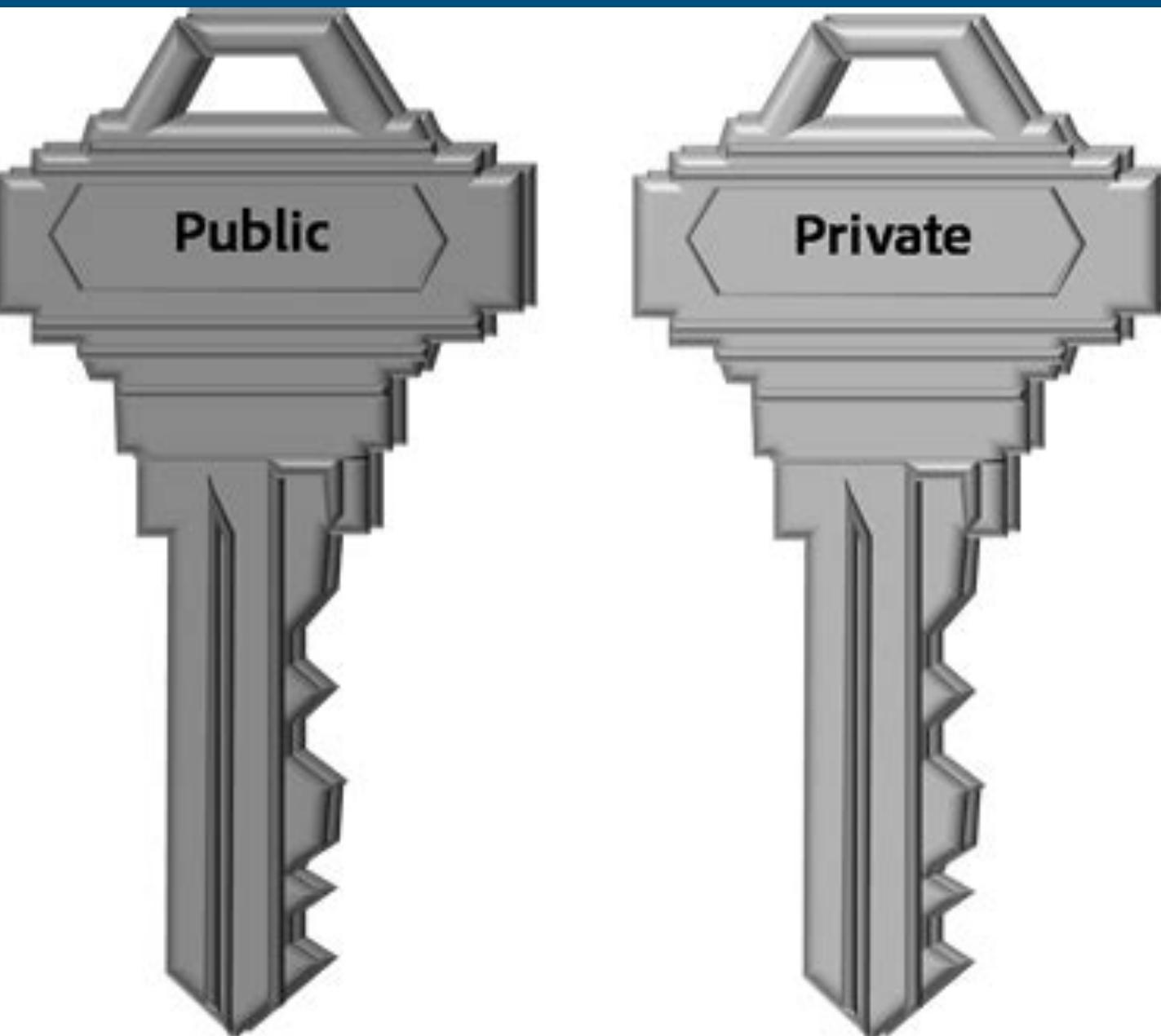
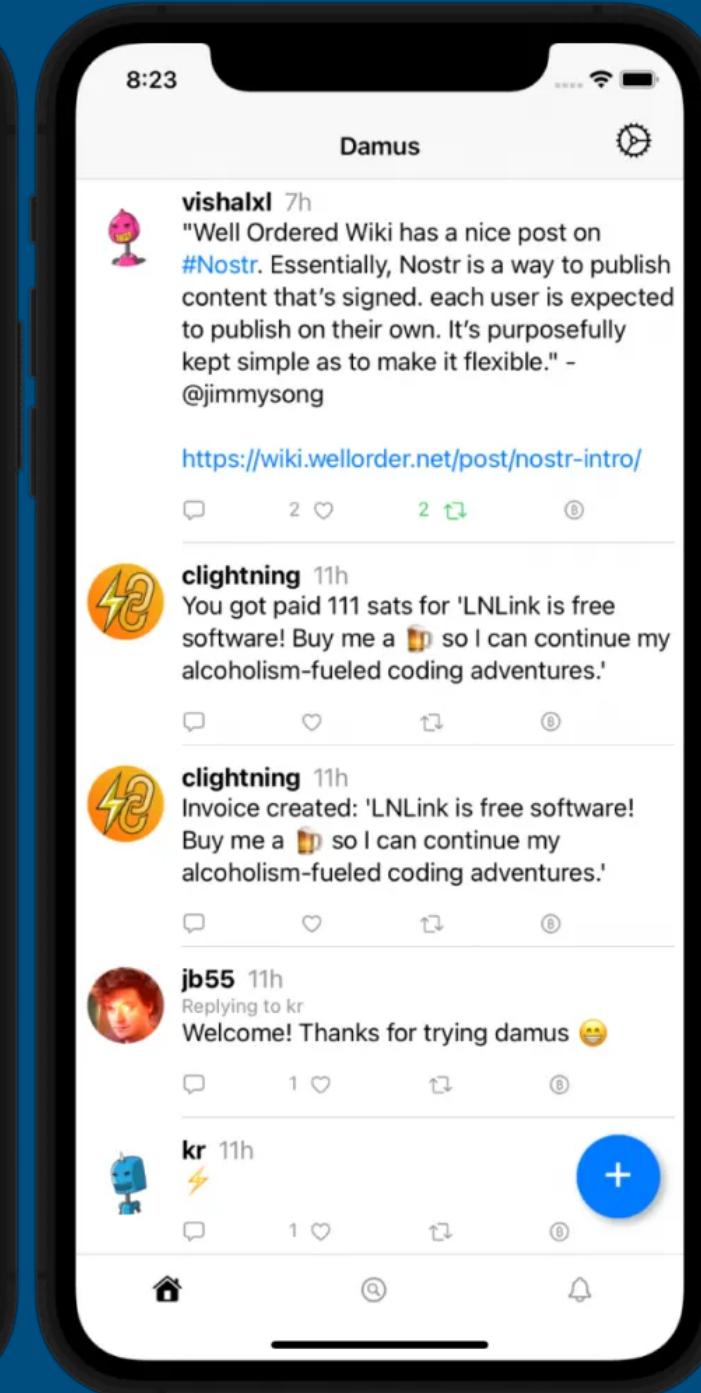
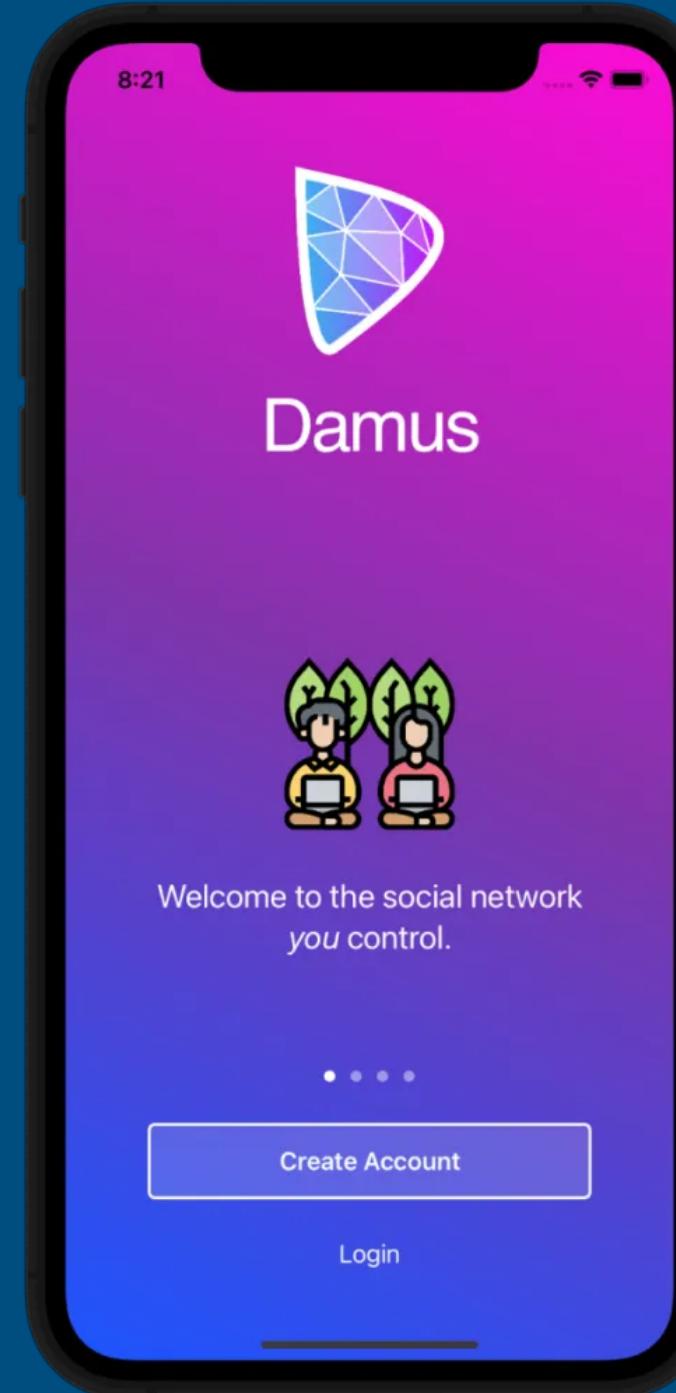


CENTRALIZED VS. DECENTRALIZED

	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	

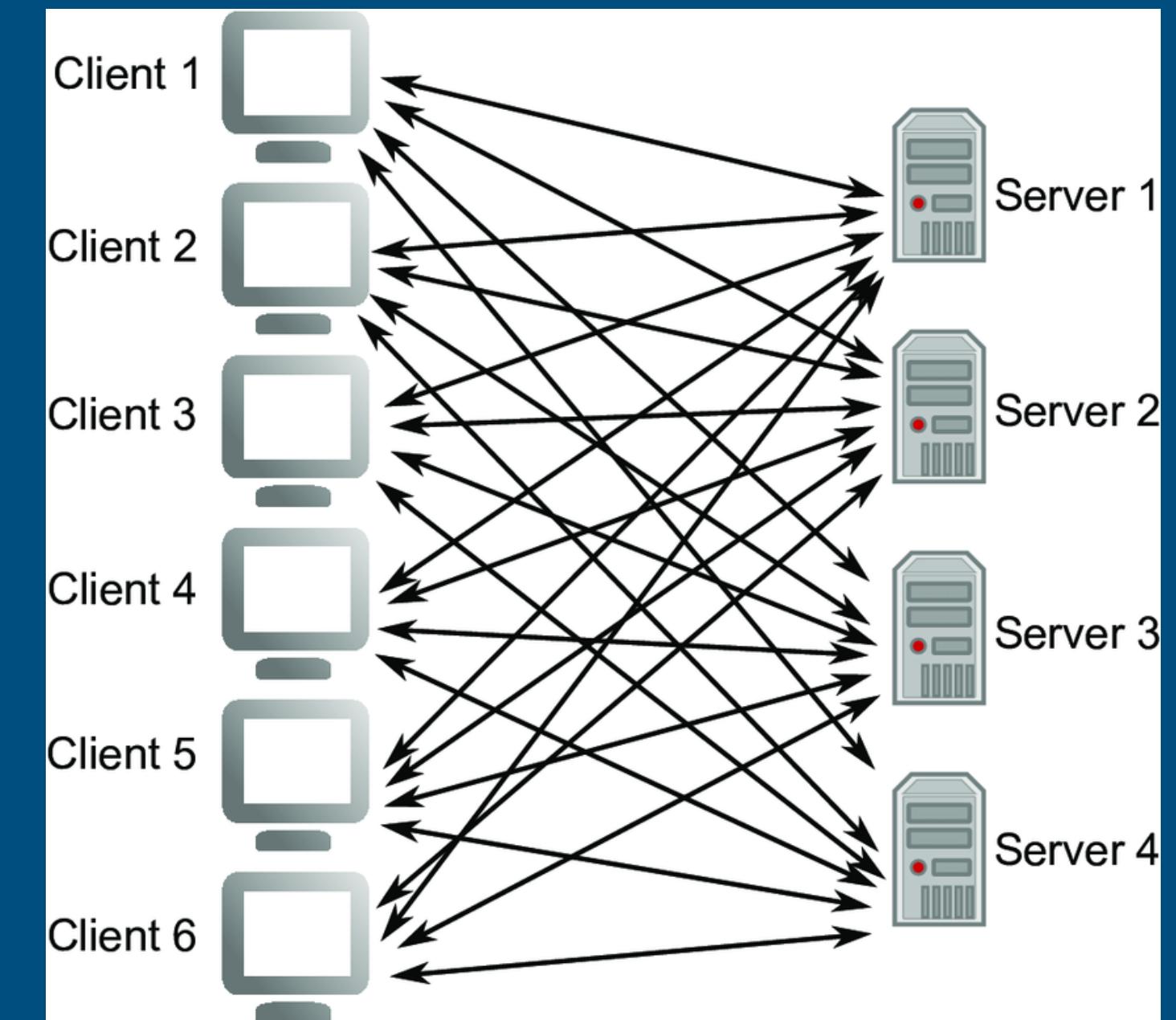
Nostr in 3 Steps

Use Nostr
Client

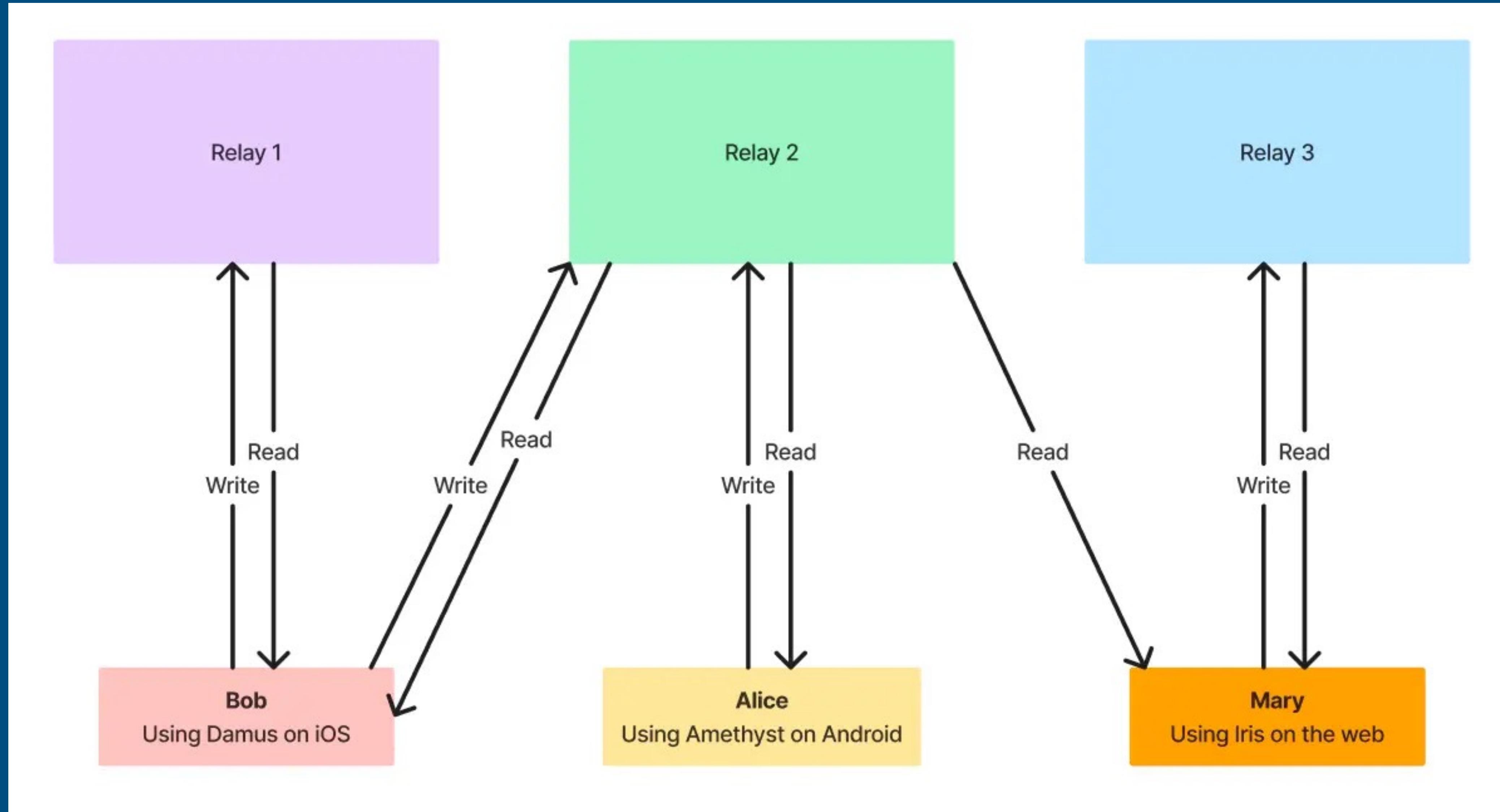


Crypto Identity

Publish to Relays



Nostr Model



DEMO



Nostr in Japan

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

The screenshot shows the GitHub repository page for 'awesome-nostr-japan'. The repository is public and has 1 branch and 0 tags. The main branch is 'main'. The 'Code' tab is selected. The repository description is: 'Awesome nostr in Japan. Software, Web service, Clients, Bots created by Japanese.' It features a 'Japanese' and 'nostr' tag. The repository has 47 stars, 1 watcher, and 5 forks. There are no releases published. A 'Sponsor' button is available. The repository was last updated 5 days ago with 18 commits. The README.md file contains the following content:

```
awesome-nostr-japan

Awesome nostr in Japan. Software, Web service, Clients, Bots created by Japanese.

Relays



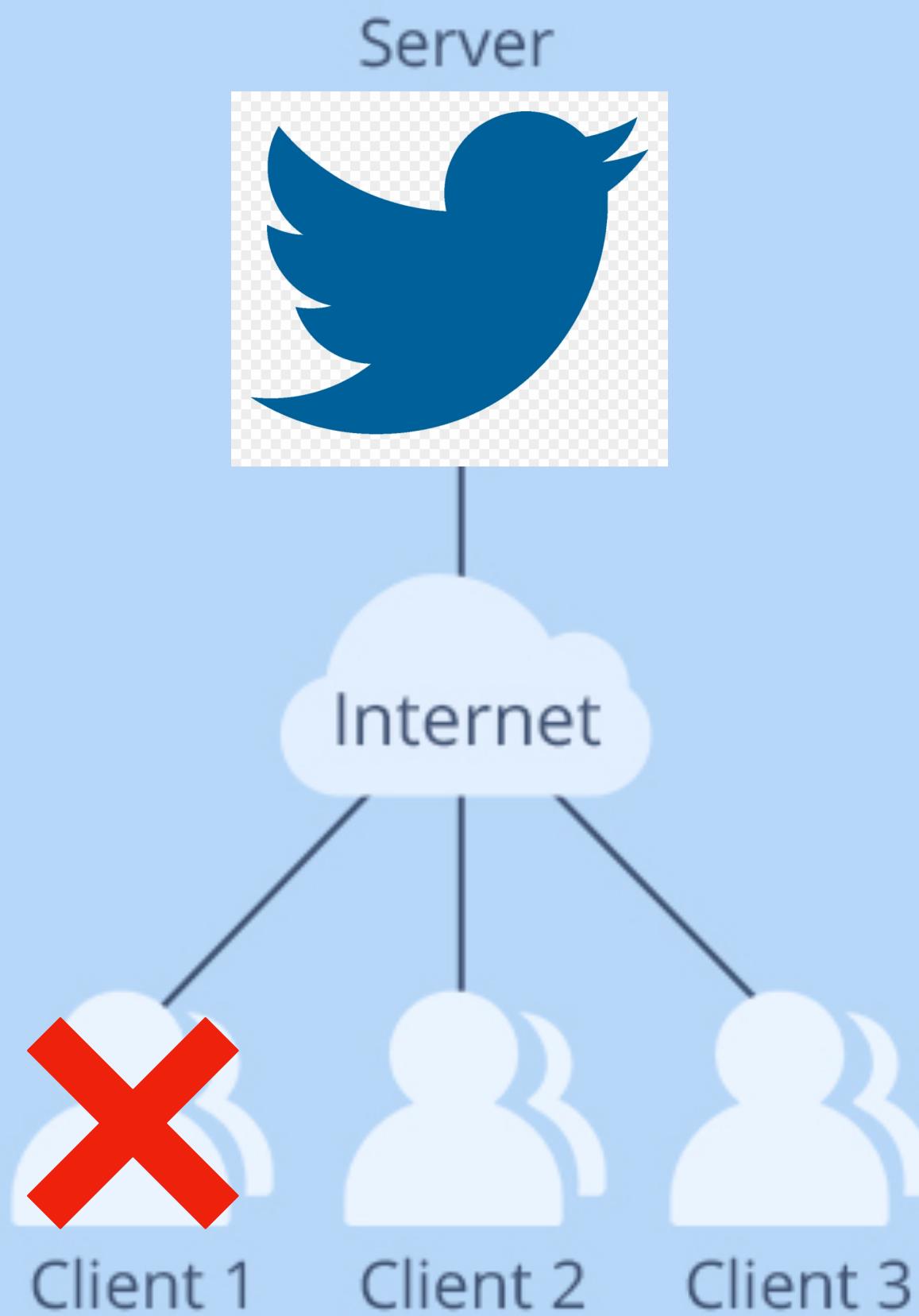
- wss://relay.nostr.wirednet.jp - World wide relay by imksoo
- wss://relay-jp.nostr.wirednet.jp - Japanese oriented relay by imksoo
- wss://ipv6.nostr.wirednet.jp - ipv6 relay by imksoo
- wss://nostr.h3z.jp - Free relay by h3z
- wss://nostr-paid.h3z.jp - Paid relay by h3z
- wss://nostr-world.h3z.jp - Relay to access "nostr.h3z.jp" from overseas by h3z
- wss://nostr.holybea.com by ほりべあ
- wss://nostr.fediverse.jp by αυγοτάραχο σολωμου
- wss://nostr-relay.nokotaro.com by Nokotaro Takeda

```

WHY

Censorship Resistance

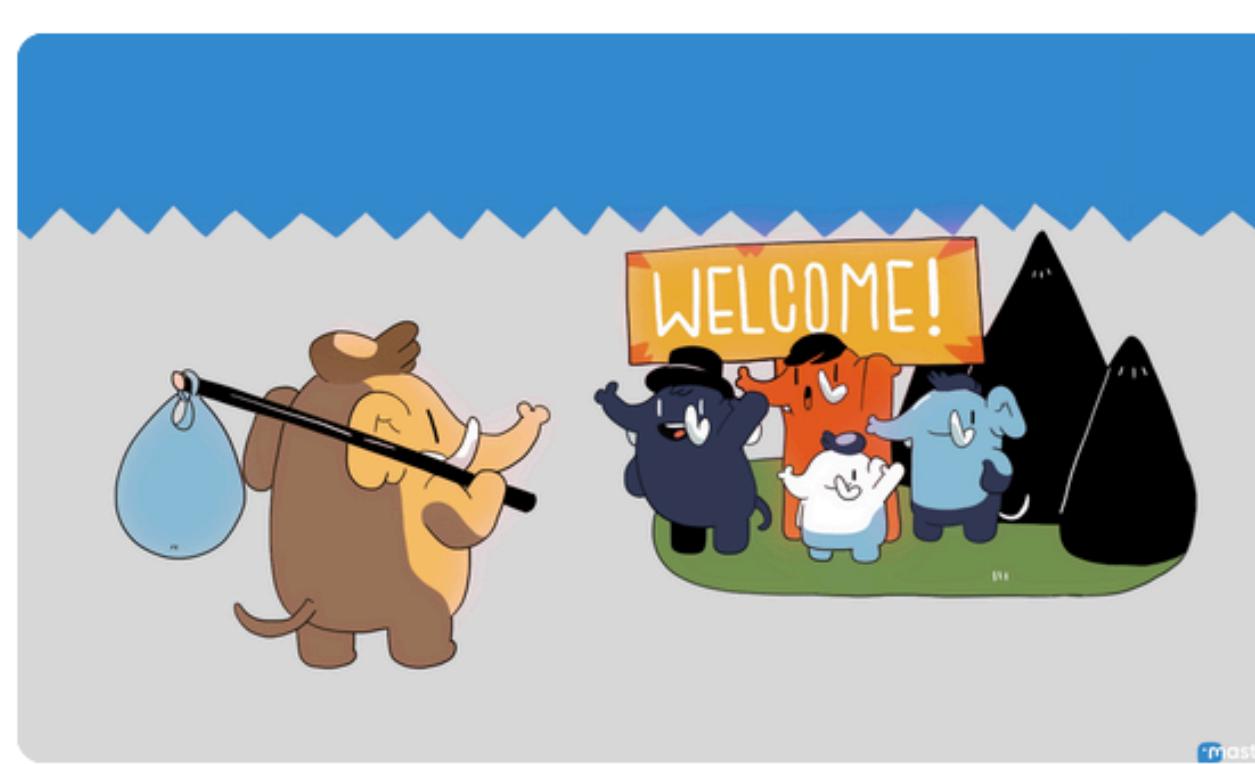
Client-Server Network



Peer-to-Peer Network



Identity & Instance

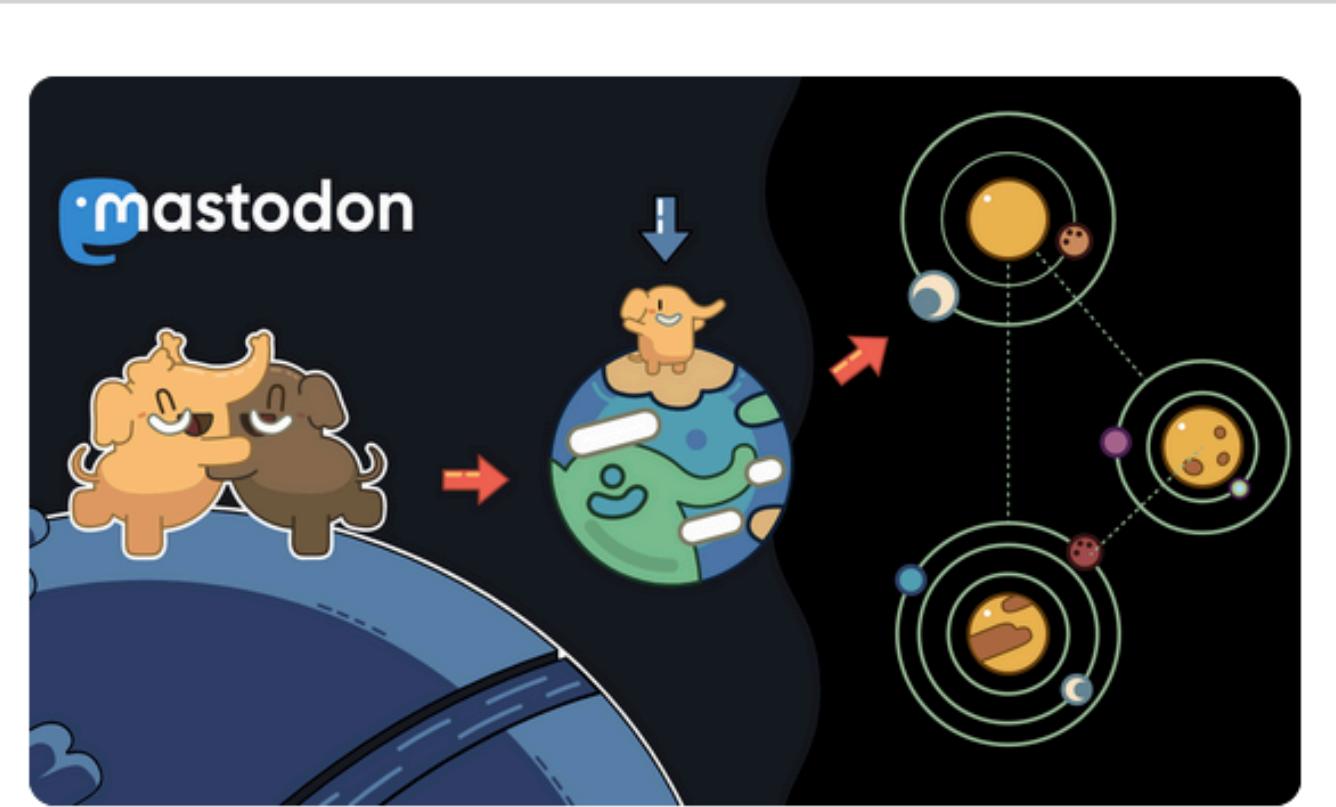


GENERAL

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.

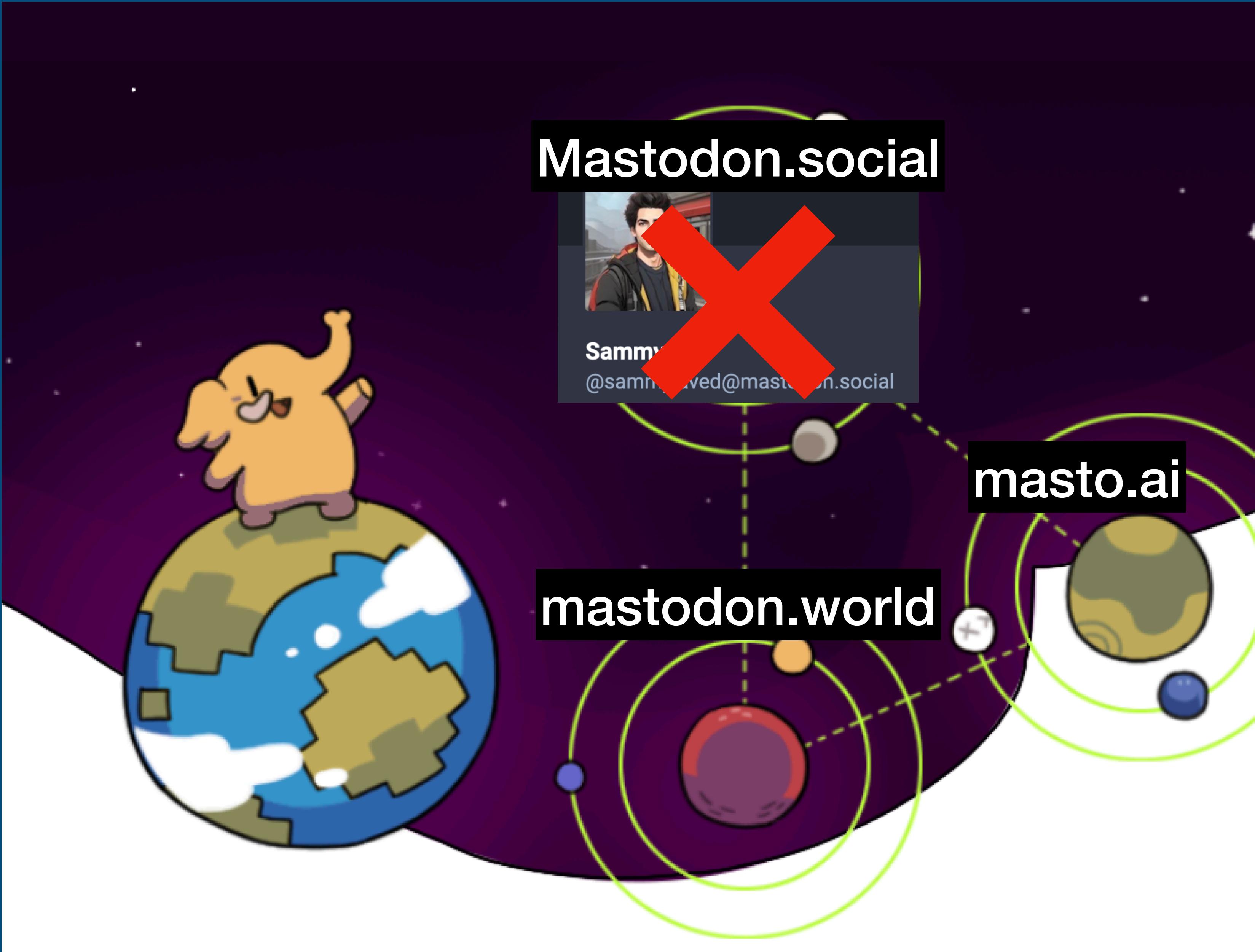
[Create account](#)

Identity tied to server

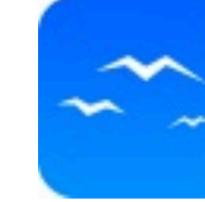


Sammy

@sammyjaved@mastodon.social



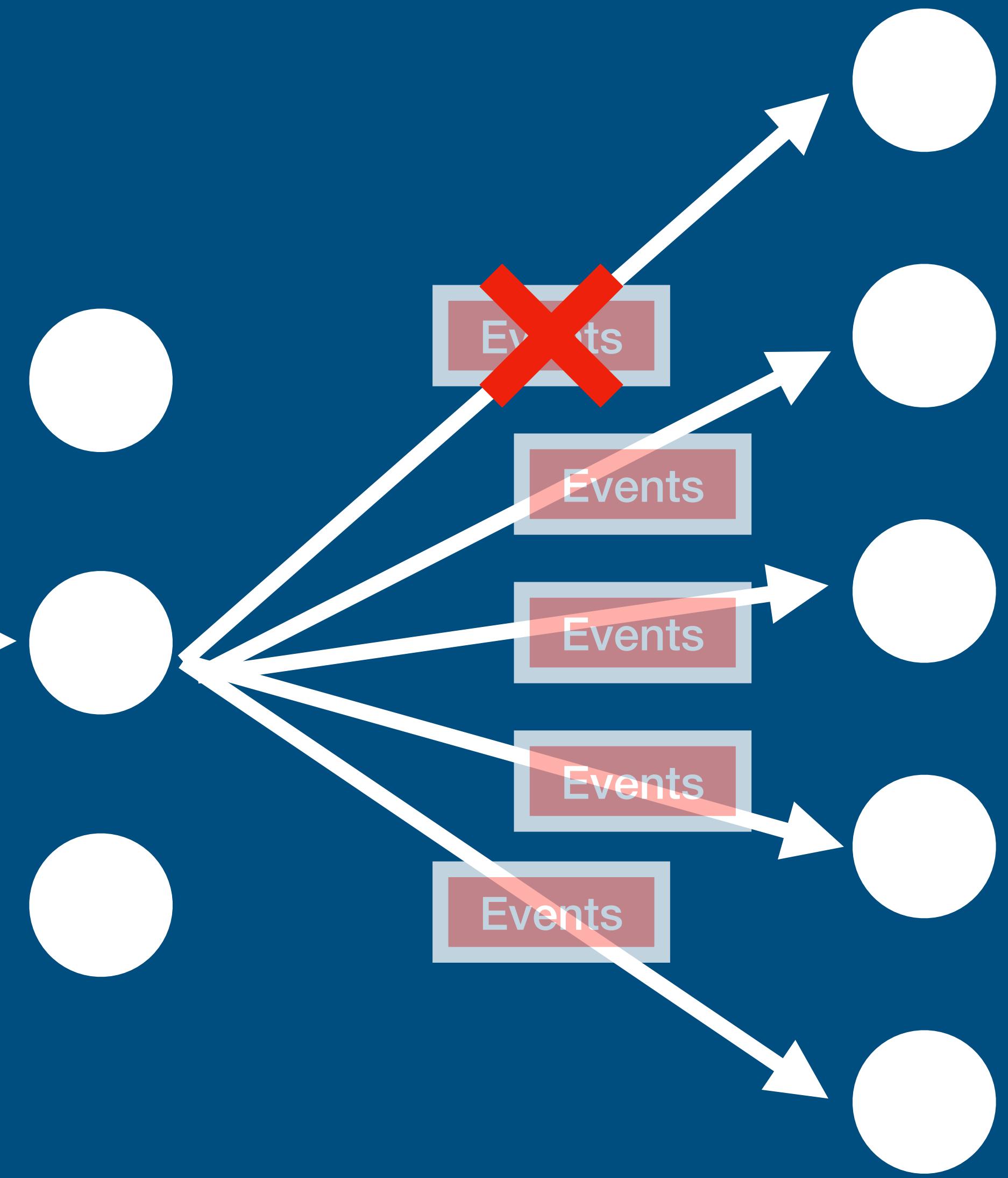
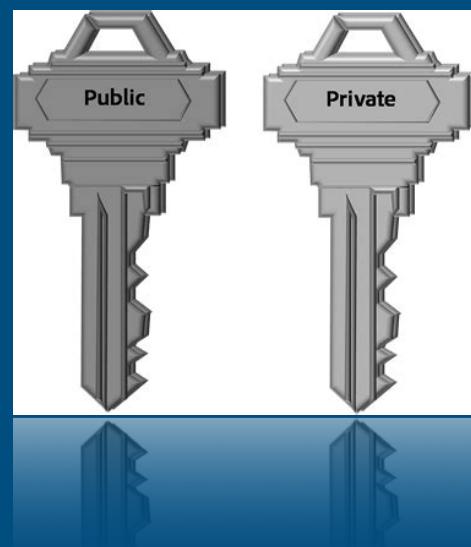
User-Facing Application	Jabber, WhatsApp, Zoom...	Riot, Nheko...	Diaspora	Mastodon, Pleroma, PixelFed...		Damus , Snort , Coracle
Identity						Crypto
Data	XMPP	Matrix		ActivityPub	Solid	Nostr
Networking						

Protocol		 ActivityPub	 XMPP	 The AT Protocol
Identity	Crypto	Domain Username + Instance <u>@alice@mastodon.social</u>	Domain <u>alice@example.com</u>	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

nsec1986kcfzxnl...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



[Notes](#)[Followers](#)[Following](#)[Zaps](#)[Relays](#)[Bookmarks](#)[Muted](#)

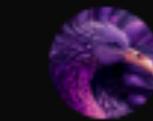
Connect to relays



wss://nos.lol/



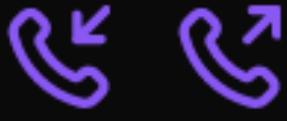
wss://nostr.orangepill.dev/



wss://brb.io/



wss://relay.damus.io/



wss://nostr.wine/



wss://relay.current.fyi/



wss://eden.nostr.land/



wss://relay.snort.social/



System Status

Browse

Statistics

relay list

367

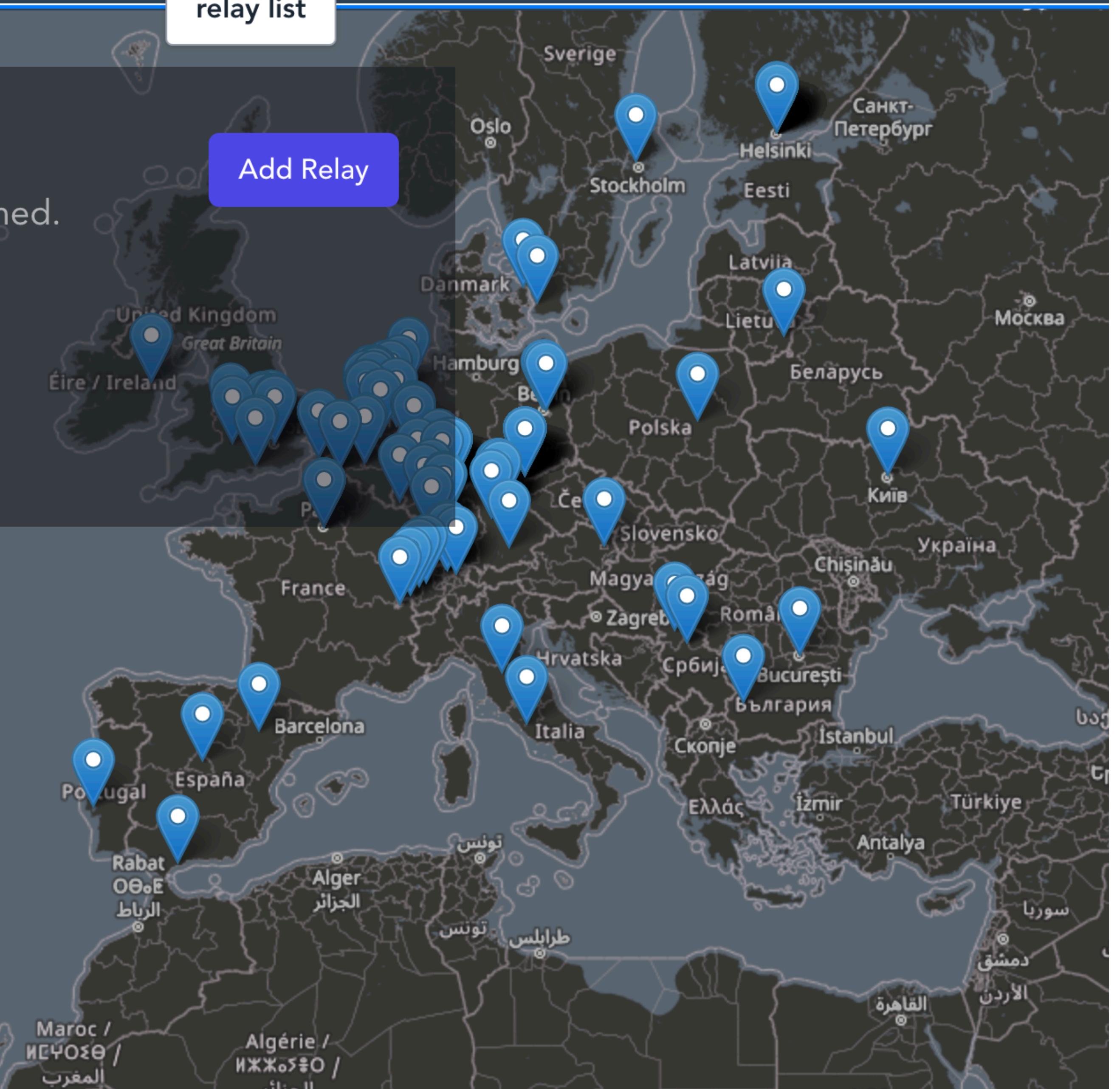
Online Relays

Relays where a connection can currently be established.

[Online](#)[Public](#)[Paid](#)[Offline](#)[All](#)[Favorites](#)

Filters:

Disabled

[Clear Filters](#)[Add Relay](#)

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	npub16k7j4mwsqm8hakjl8x 5ycrqmhx89lxkfz2xxxw7 5eav7sd8ztqy2rwdn
Pay 2 Relay	wss://nostr.milou.lol	1,000	npub1rvg76s0gz535txd9y pg2dfqv0x7a80ar6e096j3v 343xdxyrt4ksmkxrck
Pay 2 Relay	wss://puravida.nostr.land	10,000	npub16k7j4mwsqm8hakjl8x 5ycrqmhx89lxkfz2xxxw7 5eav7sd8ztqy2rwdn
Pay 2 Relay	wss://relay.nostr.com.au	6,969	npub1qqqqqrre3jxkuyj3s4m 59usdyvm0umgm0lpy6cqjt wpt649sdews5q3hw7
Pay 2 Relay	wss://relay.orangepill.dev	4,500	npub16jzr7npgp2a684pasn khjf9j2e7hc9n0teefskulqmf 42cqmt4uqwszk52

Settings

Relays

	no-str.org	Write <input checked="" type="checkbox"/>	Read <input checked="" type="checkbox"/>	
	⚡ 0 ms ✋ 0 ⚠ 0			
	nostr.pinkanki.org	Write <input checked="" type="checkbox"/>	Read <input checked="" type="checkbox"/>	
	⚡ 0 ms ✋ 0 ⚠ 0			
	nostr.hrmb.org	Write <input checked="" type="checkbox"/>	Read <input checked="" type="checkbox"/>	
	⚡ 0 ms ✋ 17 ⚠ 0			
	nostr.lu.ke	Write <input checked="" type="checkbox"/>	Read <input checked="" type="checkbox"/>	
	⚡ 0 ms ✋ 0 ⚠ 0			
	relay.snort.social	Write <input checked="" type="checkbox"/>	Read <input checked="" type="checkbox"/>	
	⚡ 0 ms ✋ 10 ⚠ 0			
	nostr.wine	Write <input type="checkbox"/>	Read <input checked="" type="checkbox"/>	
	⚡ 0 ms ✋ 0 ⚠ 0			
	nos.lol	Write <input checked="" type="checkbox"/>	Read <input checked="" type="checkbox"/>	
	⚡ 0 ms ✋ 0 ⚠ 0			

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

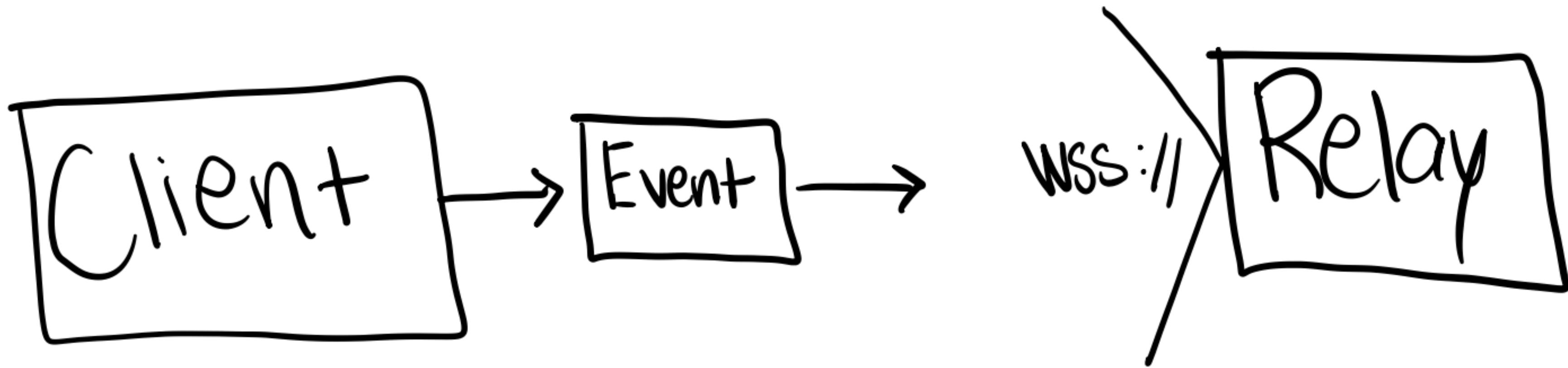
Each user has a keypair. Signatures, public key, and encodings are done according to the [Schnorr signatures standard for the curve secp256k1](#).

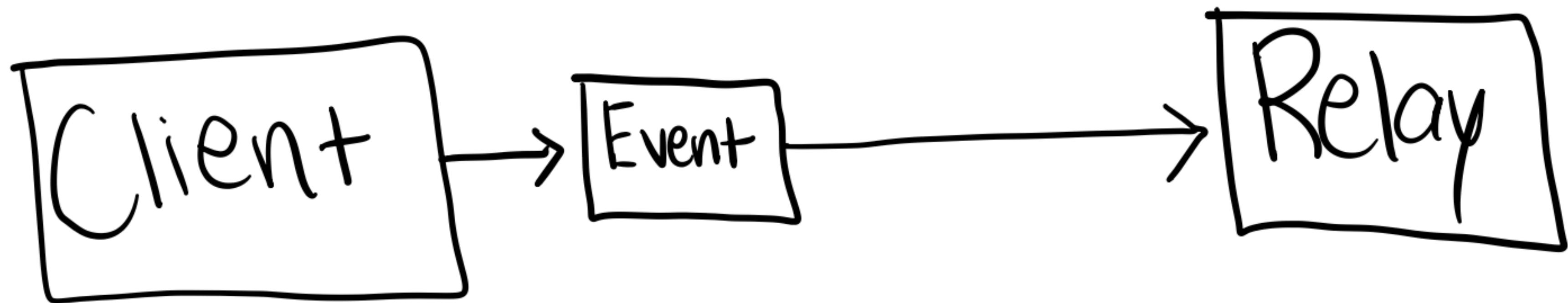
The only object type that exists is the `event`, which has the following format on the wire:

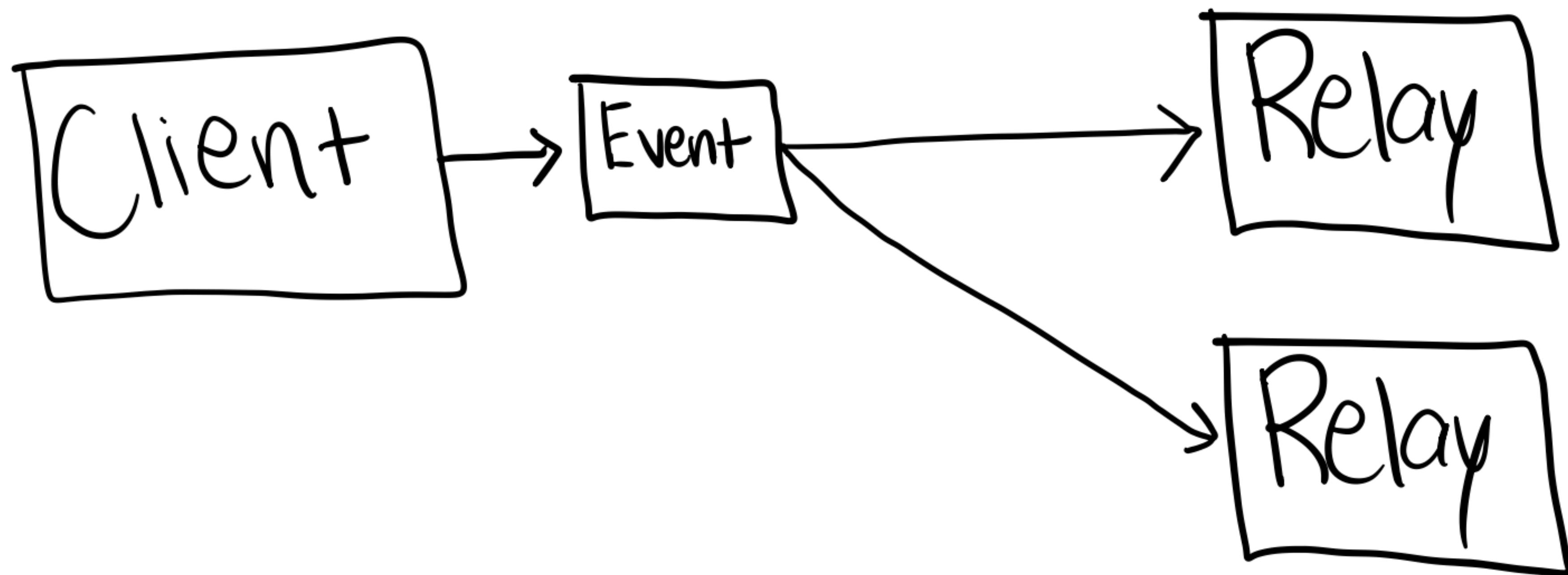
```
{  
  "id": <32-bytes lowercase hex-encoded sha256 of the serialized event data>  
  "pubkey": <32-bytes lowercase hex-encoded public key of the event creator>,  
  "created_at": <unix timestamp in seconds>,  
  "kind": <integer>,  
  "tags": [  
    ["e", <32-bytes hex of the id of another event>, <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" field>  
}
```

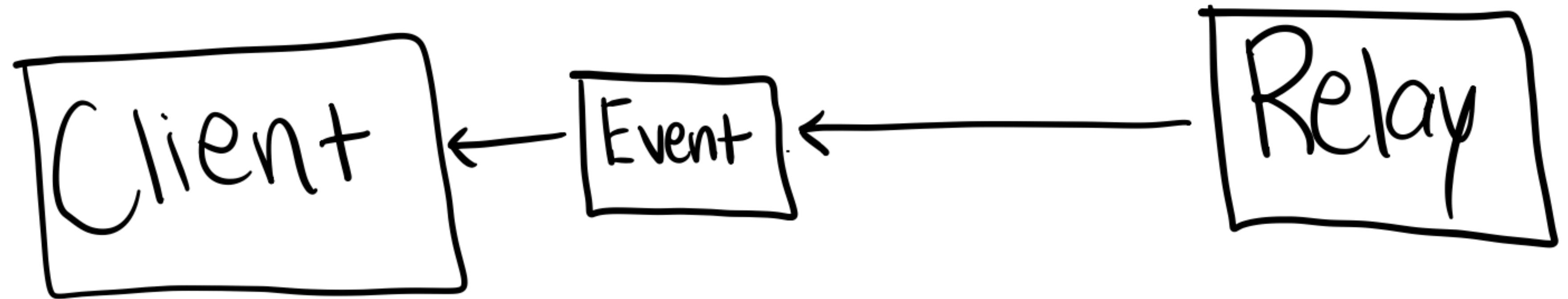
Client

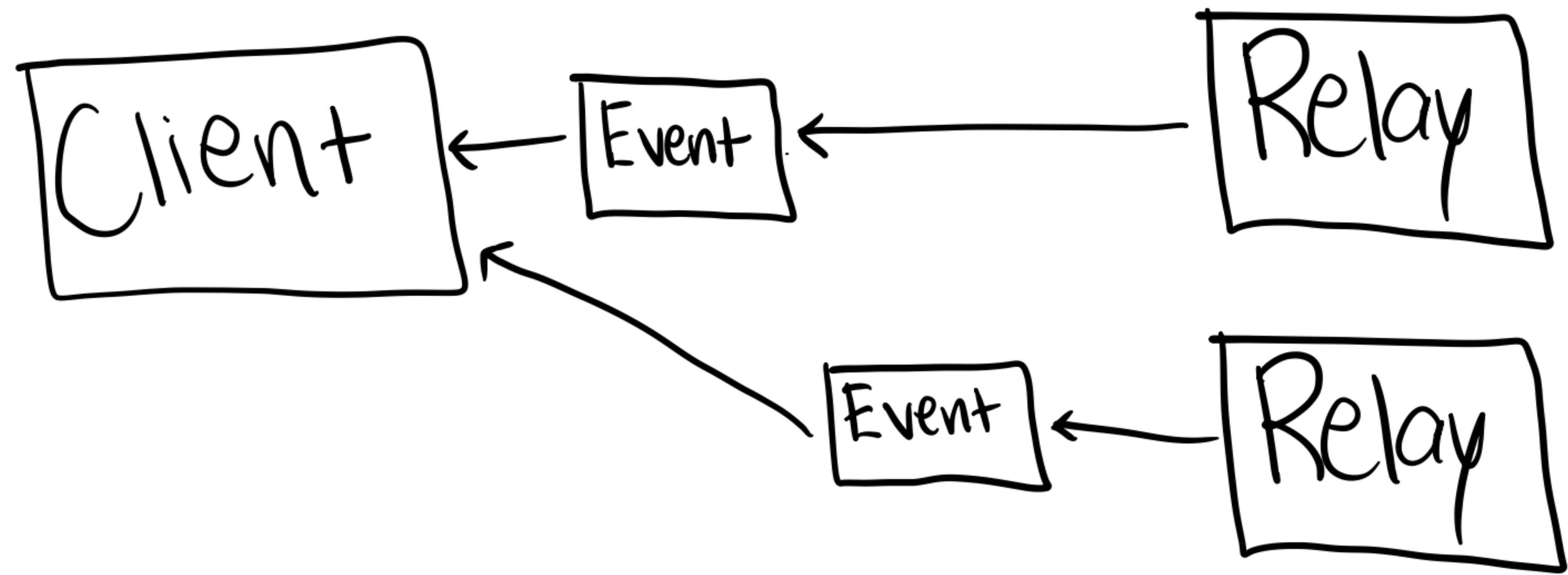
Relay

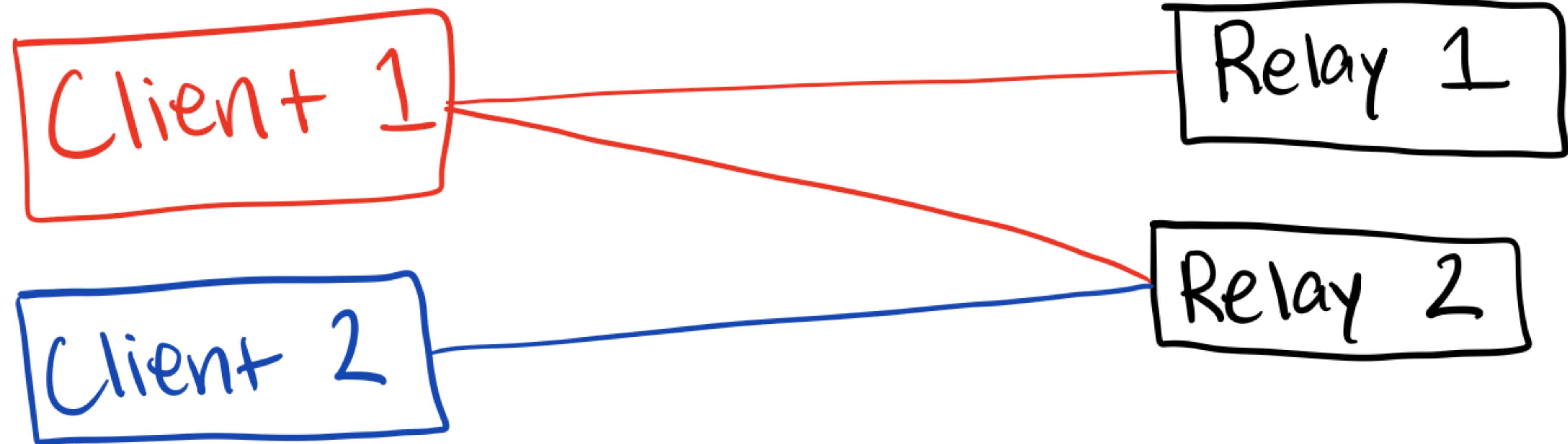


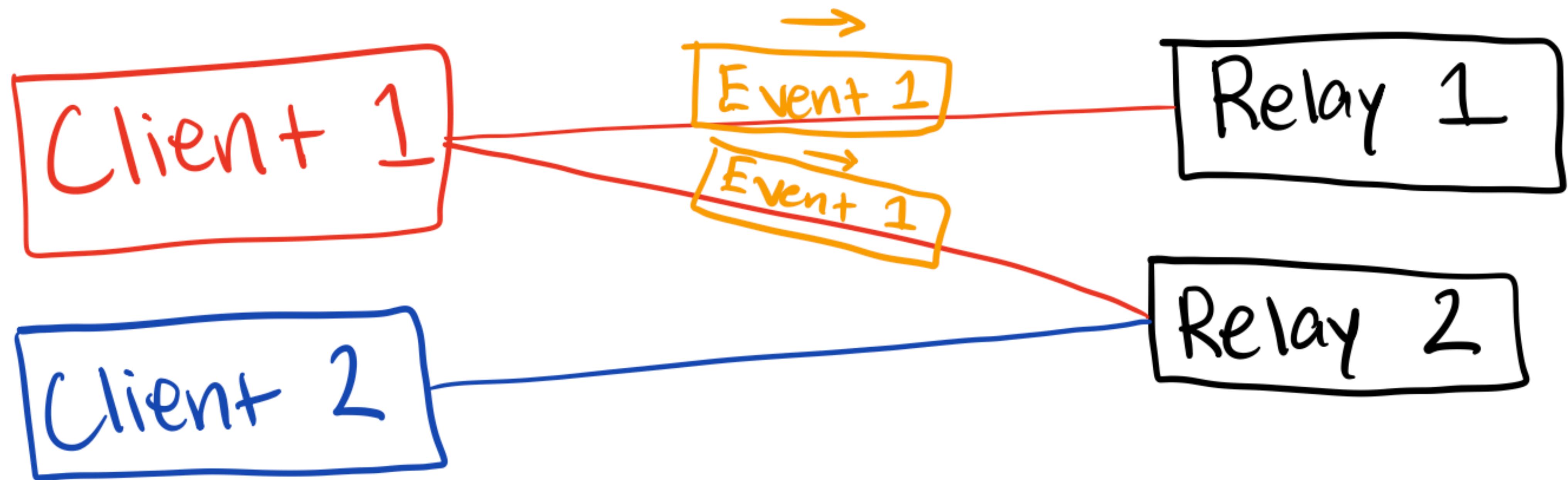


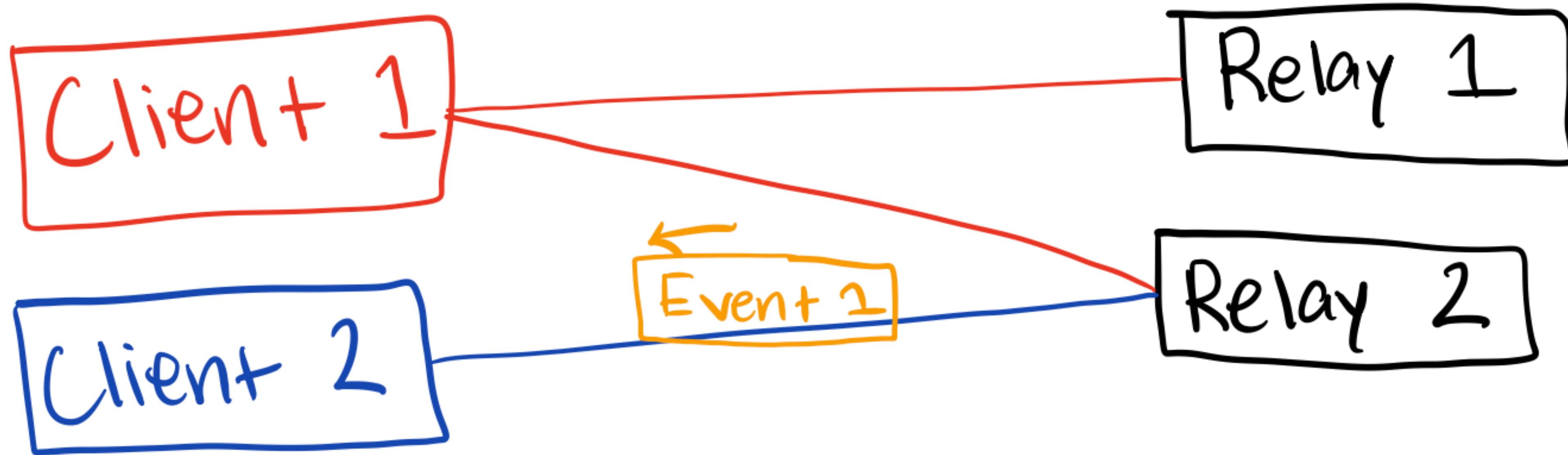


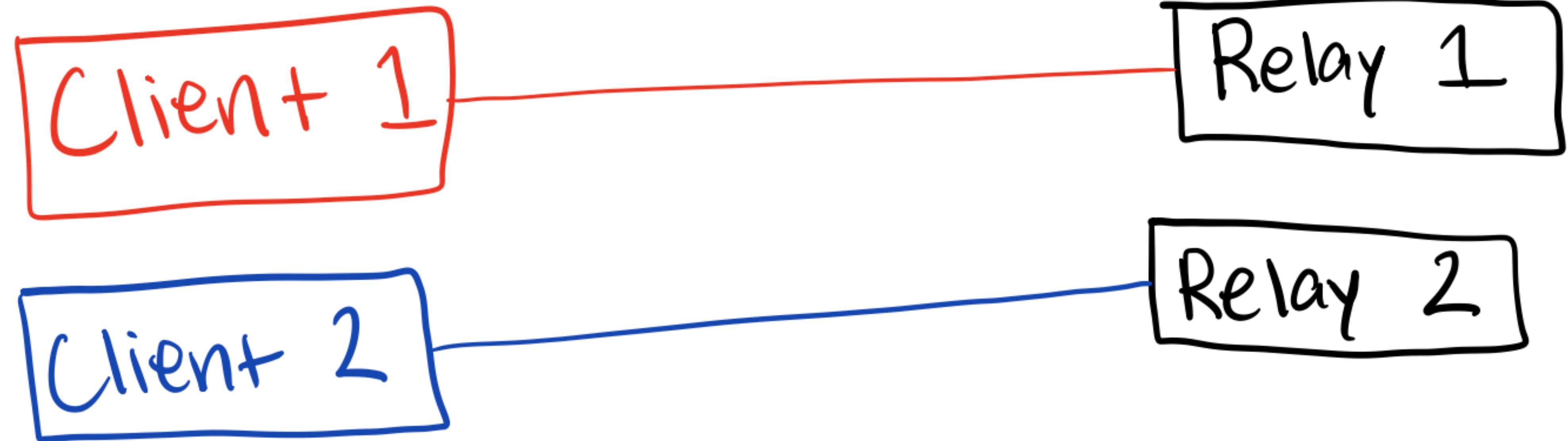


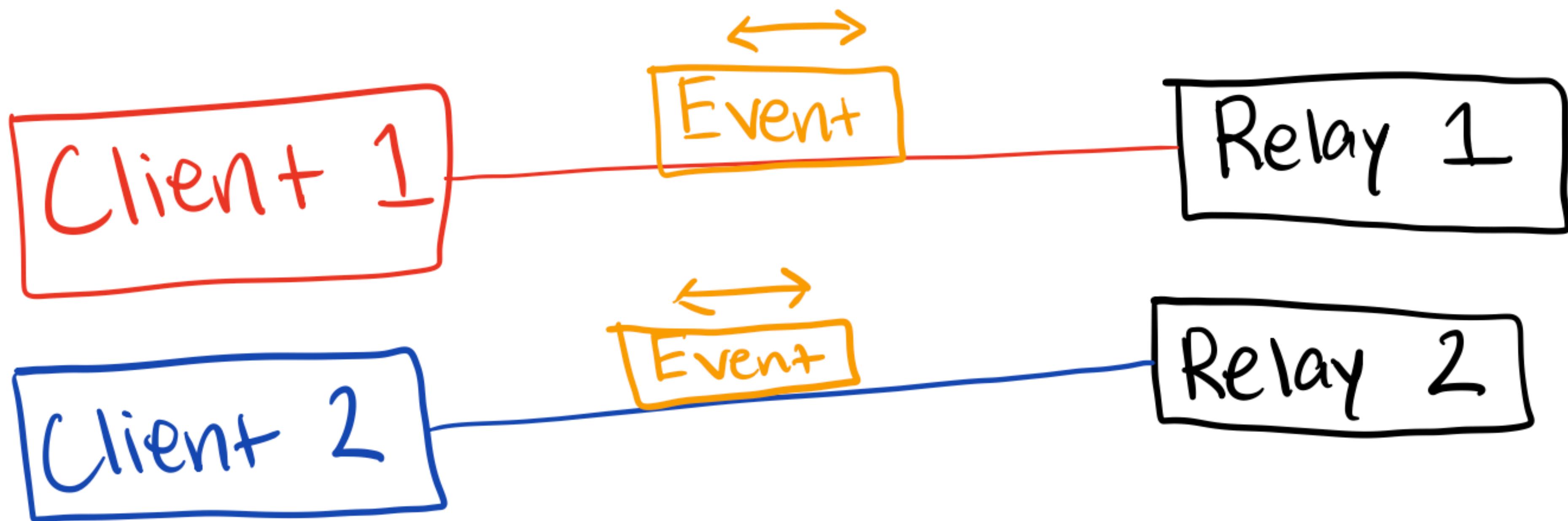












No Shared
relays
= No Shared
events

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

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.

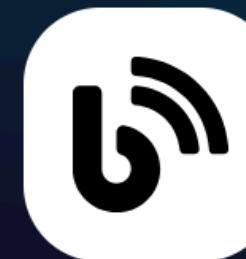


Writing



Habla

A long form content client for nostr notes.



Blogstack

Decentralized blogs over relay using nostr w/ ⚡ lightning tips

Music & Podcasting



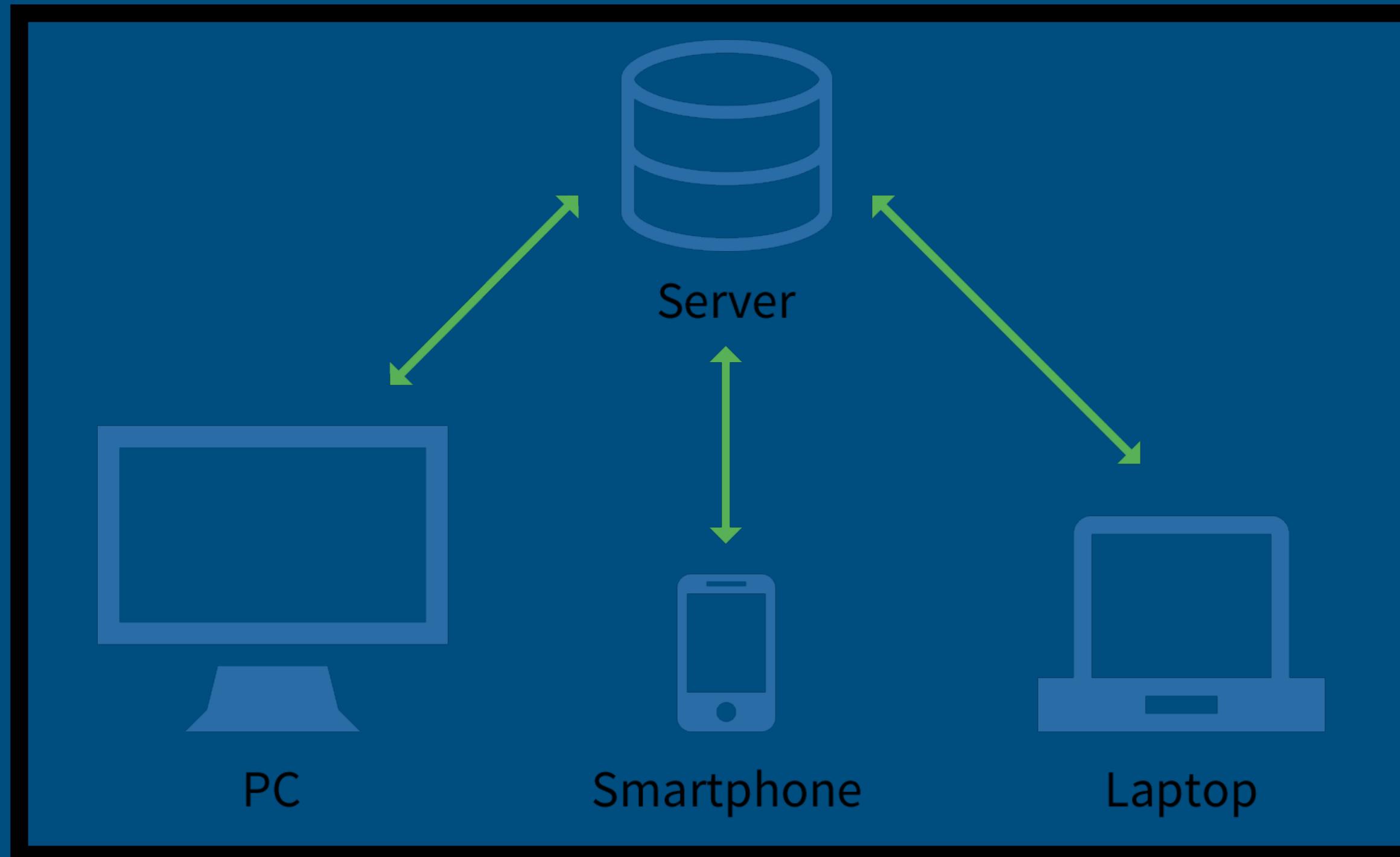
Fountain

The podcast app that pays.

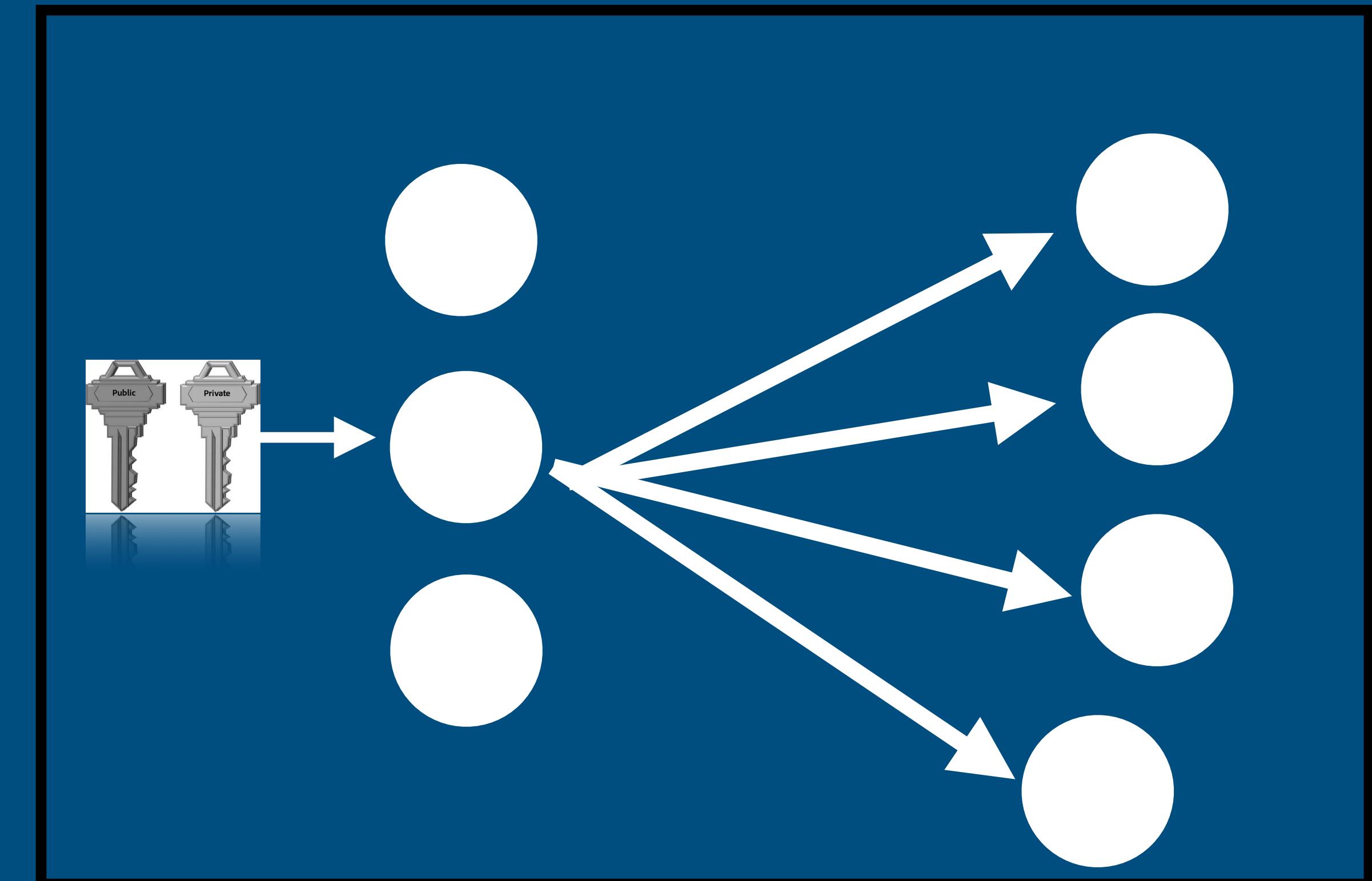


Decoupling Identity, Frontend, Backend

Client-Server

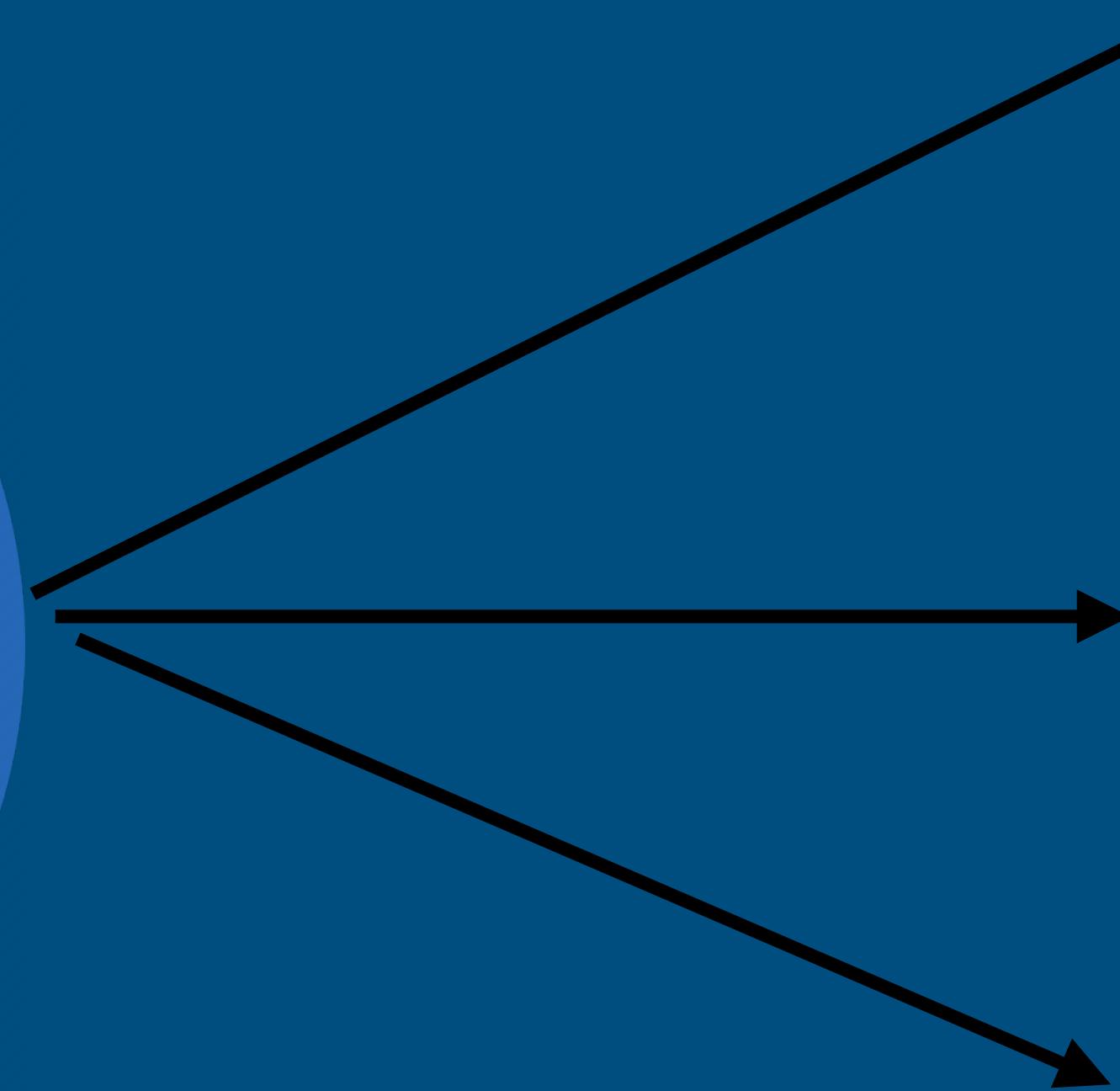


Clients-Relays



Social Media

Vendor Lock In

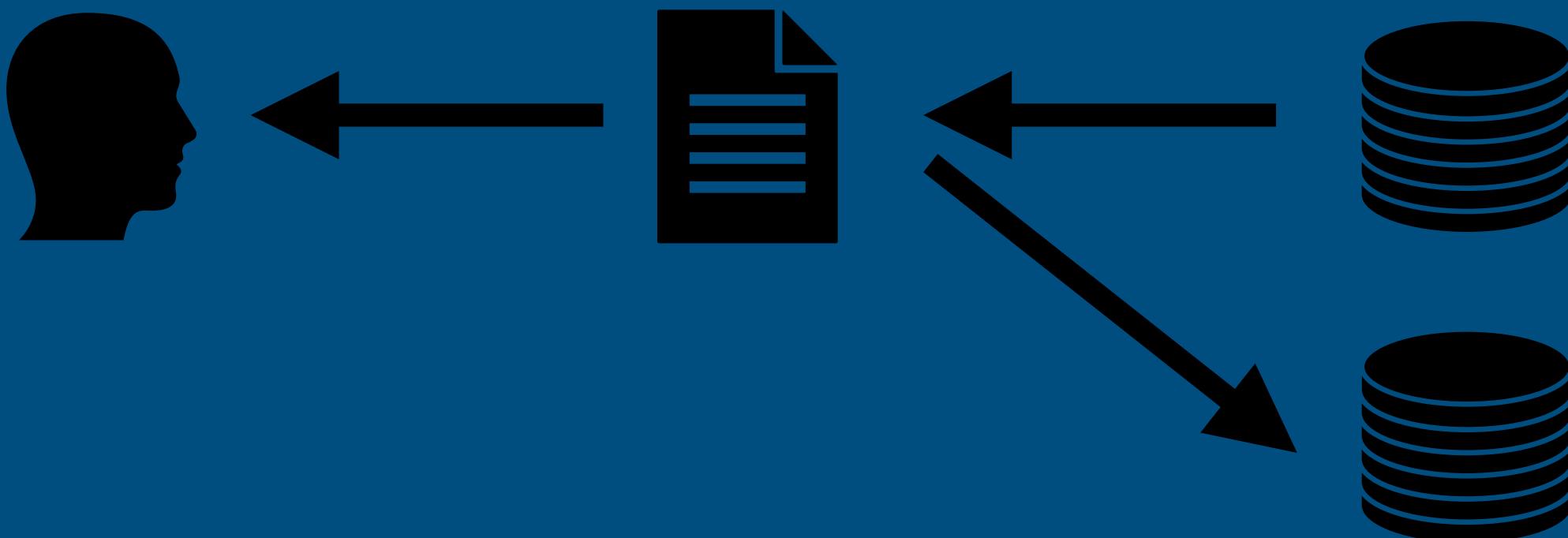


Music

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

