NOSTR

Notes, Relays, Portable Identities, and a touch of Lightning

Giovanni Moretti

November 8, 2023

Common Social Media sites - Your identity? Your data?

- Centralised Social media: Facebook, YouTube, Twitter, TikTok, Threads, WeChat
- Decentralised: Mastodon, Frendica, Diaspora, PeerTube

Site admins have a LOT of power

User's Banned for actual/perceived offences:

- broken T&C
- offending site owner
- "wrong" viewpoint
  - wrong political/gender/religious views
  - being for/against Masks/Vaccinations

If account closed, your data is gone: You can't your transfer Identity or Content

Nostr Overview

Nostr: “Notes and Other Stuff Transmitted by Relays”

- it’s a protocol, not a service or app
- based on simple & flexible Event objects (plain JSON)
- uses public-key cryptography for keys & signing messages

Resilient and verifiable

- users publish to one or more relays
- no home site makes content much harder to suppress
- messages are signed: can’t be forged

Nostr Protocol - the central ideas

User identified by a public/private keypair (not a name)

Clients access to Relay servers

- relays store user messages (typed)
- users can query relays for messages (all or a matching a query)
- anyone can post to an (unpaid) relay

Relays only have messages posted to that relay

- relays don't talk to each other
- users can post a message to multiple relays
- users can publicise which relays they post on

A sample Nostr note

```
{
    "id": "4376c65d2f232afbe9b882a35baa4f6fe8667c4e684749af565f981833ed6a65",
    "pubkey": "6e468422dfb74a5738702a8823b9b28168abab8655faacb6853cd0ee15deee93
    "created_at": 1673347337,
    "kind": 1,
    "tags": [
        ["e", "3da979448d9ba263864c4d6f14984c423a3838364ec255f03c7904b1ae77f206
        ["p", "bf2376e17ba4ec269d10fcc996a4746b451152be9031fa48e74553dde5526bce
    ],
    "content": "Walled gardens became prisons, and nostr is the first step
                towards tearing down the prison walls.",
    "sig": "908a15e46fb4d8675bab026fc230a0e3542bfade63da02d542fb78b2a8513fcd009
}
```

from `https://nostr.how/en/the-protocol`

Your identity isn't tied to a site or client

Your identity is a public-private key pair

- Secret: nsec10yalkuwf4xkdv8wyx48wjsu7gz0509nd0ea53cvafg2h04098qdqpyqeft
- Public: npub1yvs2quw0p6xq5m4susv8x4rfm08a42mzcucuzwya999gvwe0ssyq24f3g4

DON'T LOSE THESE & *Keep the nsec key secret*

Use any/multiple clients

- choose a client you like
- load key-pair
- post 'as you' from any client

Choosing a Nostr client

Amethyst for Android

- `https://github.com/vitorpamplona/amethyst`

For iPhones/iPads

- Damus - `https://apps.apple.com/us/app/damus/id1628663131`
- PlebStr - `https://apps.apple.com/us/app/plebstr-nostr-client/id166230916`

Web Clients for laptops and desktops

- Primal - `https://primal.net`
- Iris - `https://iris.to`

List of clients: `https://nostr.com/clients`

Finding people and content

Clients have a 'starter set' of relays preloaded
so your initial feed won't be empty

Customising your feed

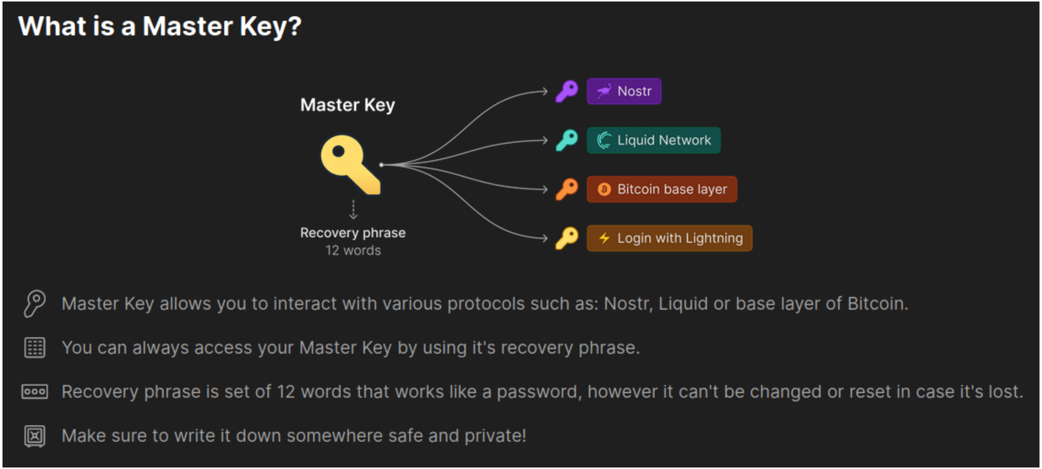
- **Finding content**: Hashtags work e.g. #gardening
- **Finding people**: `https://github.com/aitechguy/nostr-address-book`

See what relays others use

- `https://nostr.directory/p/npub1l2vyh47mk2p0qlsku7hg0vn29faehy9hy34ygaclpn66ukqp3afqutajft`

Manage keys with Alby Nostr/Lightning Wallet extension (Firefox/Chrome)

- https://getalby.com



What is a Master Key?

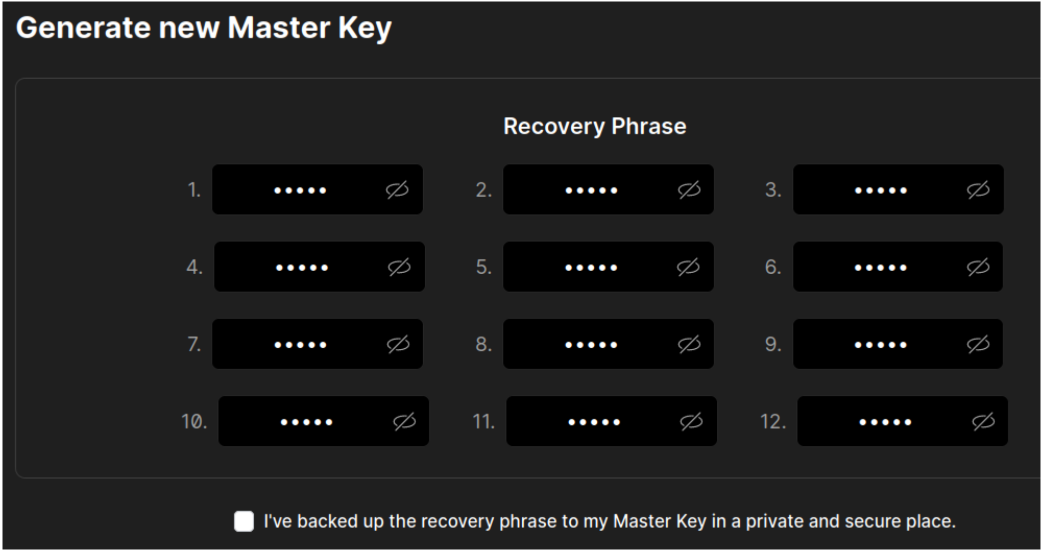
Master Key allows you to interact with various protocols such as: Nostr, Liquid or base layer of Bitcoin.

You can always access your Master Key by using it's recovery phrase.

Recovery phrase is set of 12 words that works like a password, however it can't be changed or reset in case it's lost.

Make sure to write it down somewhere safe and private!

Alby - Generate/Export new master key



Generate new Master Key

Recovery Phrase

1. •••••
2. •••••
3. •••••
4. •••••
5. •••••
6. •••••
7. •••••
8. •••••
9. •••••
10. •••••
11. •••••
12. •••••

□ I've backed up the recovery phrase to my Master Key in a private and secure place.

Bitcoin Lightning Network makes micropayments cheap and easy

One BitCoin ≈ NZ$50,000

This is too large to conveniently use or think about.

Don't have to buy/sell whole bitcoins - fractions are fine

The minimal amount is the Satoshi

The Lightning Network payments are in Satoshis

$$One\ Satoshi = \frac{Bitcoin}{100,000,000}$$

Lightning Network Payments use Satoshis (sats)

Easier to think of Sats in multiples

1 sats	=	0.05c NZ
20 sats	=	1c NZ
100 sats	=	5c NZ
1000 sats	=	50c NZ
10000 sats	=	$5 NZ

Lightning Network Overlay Network

- very fast
- fees are very low
- payments of 20-100 sats are fine

Enable new options - *Value-for-Value* Micropayments

Payments for 'Likes'

Know the npub - Know the creator: Send Sats (called *Zaps* in Nostr)

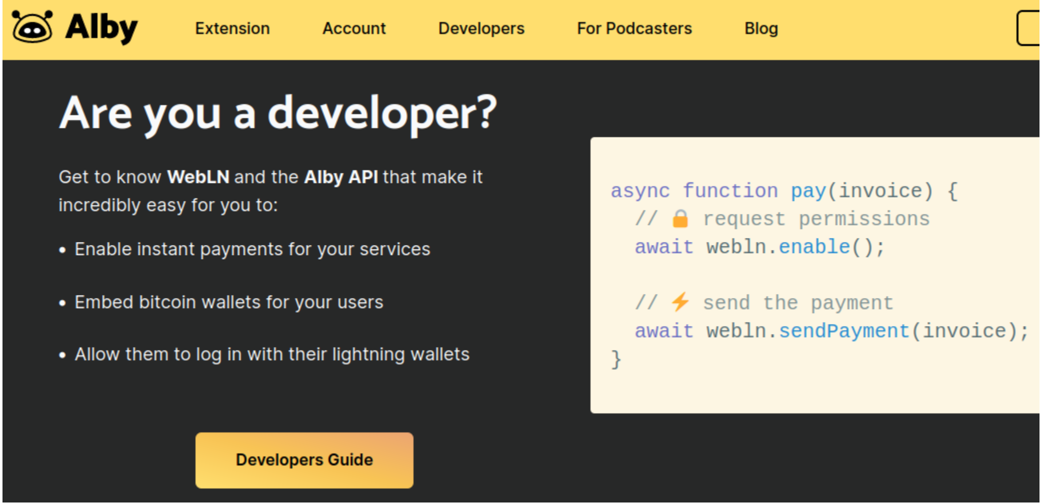
Pay Creators Directly

- no middleman taking a cut
- pay WordPress Authors
- pay podcast creators
  - pay per segment (e.g. 100 Sats every 5 minutes)

Support worthy causes

- `https://nodeless.io/donate/oral-surgery`

Alby - enabling payment to your site



Are you a developer?

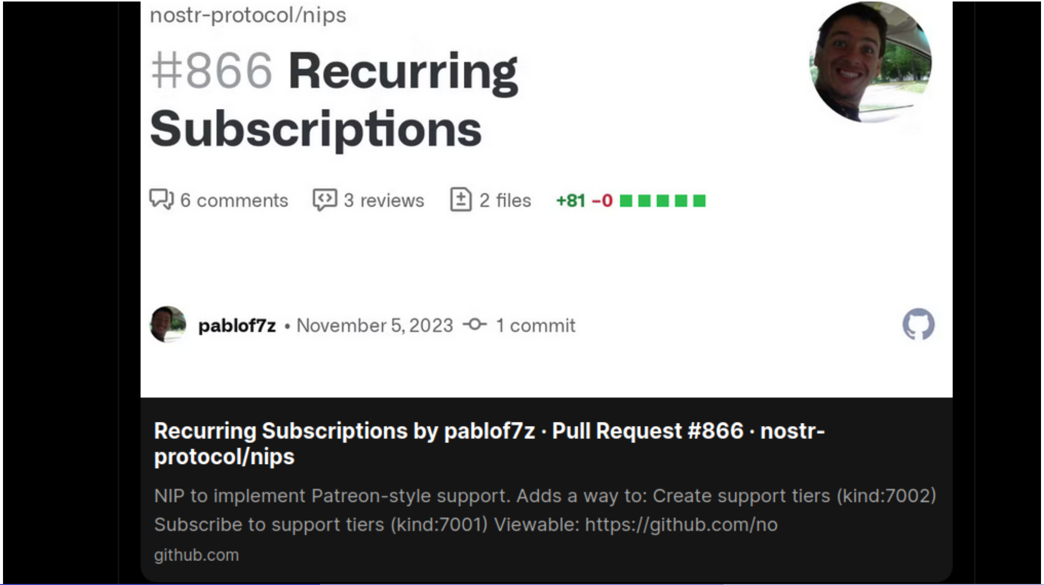
Get to know **WebLN** and the **Alby API** that make it incredibly easy for you to:

- Enable instant payments for your services
- Embed bitcoin wallets for your users
- Allow them to log in with their lightning wallets

```
async function pay(invoice) {
  // 🔒 request permissions
  await webln.enable();

  // ⚡ send the payment
  await webln.sendPayment(invoice);
}
```

NIPs - Nostr Improvement Possibilities



nostr-protocol/nips

#866 **Recurring Subscriptions**

6 comments 3 reviews 2 files +81 −0 🟩🟩🟩🟩🟩

pablof7z • November 5, 2023 1 commit

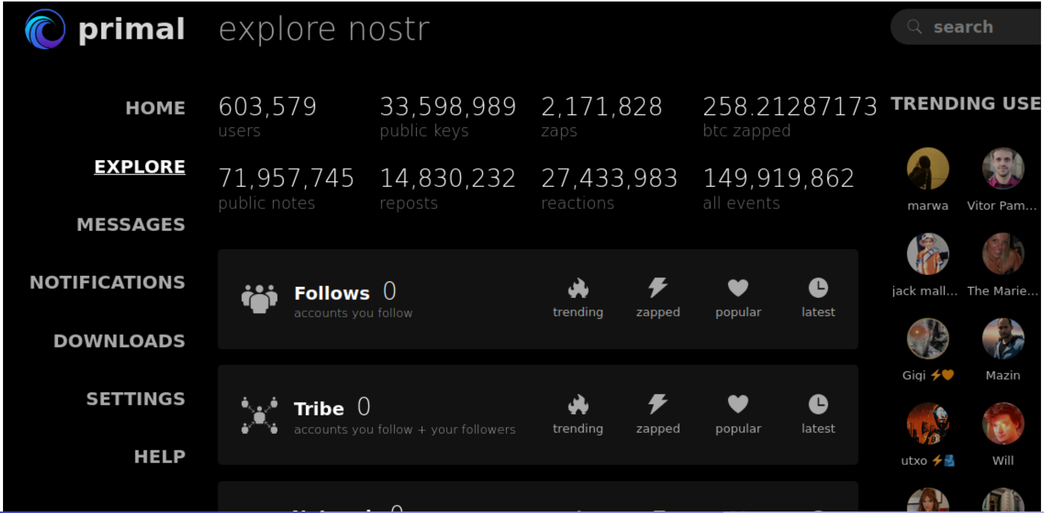
Recurring Subscriptions by pablof7z · Pull Request #866 · nostr-protocol/nips

NIP to implement Patreon-style support. Adds a way to: Create support tiers (kind:7002) Subscribe to support tiers (kind:7001) Viewable: https://github.com/no

github.com

Nostr Stats (Nov 7,2023)

From `https://primal.net/explore`



explore nostr

603,579 users

33,598,989 public keys

2,171,828 zaps

258.21287173 btc zapped

71,957,745 public notes

14,830,232 reposts

27,433,983 reactions

149,919,862 all events

Follows 0 accounts you follow

Tribe 0 accounts you follow + your followers

Getting started

Just looking

- https://www.iris.to OR
- https://www.primal.net

Posting with a permanent ID

- install Alby: https://getalby.com
- Create a new Master Key AND SAVE THE RECOVERY WORDS
- use Primal web client

For detailed instructions, see https://nostr.how

Lots more

- Nostr Home: https://nostr.com
- Extensive list of everything Nostr including Podcasts, Telegram groups ...
  - https://www.nostr.net