NOSTR, "pštrosí" sociální síť

blog.root.cz/novacisko/nostr-pstrosi-socialni-sit

V článku proberu nově vznikající decentralizovanou síť NOSTR. Co to je, v čem stojí za pozornost, jakými bolestmi trpí, co se nepovedlo a zda to vůbec má smysl.

NOSTR je zkratka, která znamená `Notes and Other Stuff Transmitted by Relay`. Často jej snadno poznáte pomocí loga zobrazující pštrose – jako ostrich.

Jako NOSTR se označuje též protokol, který se používá při komunikaci po síti. NOSTR ale není žádný konkrétní program, ani server, ale jedná se jen o dokument, ve kterém je napsáno, jak spolu mají komunikovat jednotlivé prvky sítě. Za prvotní nápadem stál jakýsi „Fiatjaf“, což je jediná přezdívka, kterou se o autorovi dozvíte. Kromě toho se dozvíte, že vznik protokolu podpořil Jack Dorsey (bývalý CEO Twitteru) dotací ve výši 14 BTC v té době v hodnotě $250000.

Asi nikoho nepřekvapí, že NOSTR „vypadá“ v představě vývojářů jako náhrada Twitteru, alespoň z hlediska uživatelského zážitku.
I když je třeba říct, že to jsou zejména vývojáři klientů, kteří jej takto prezentují. Takže zde máte příspěvky, timeline, followery, soukromé zprávy (které jsou end-to-end šifrované), lajky, blokace (mute), tagy, atd … a také „zapy“, což jsou něco jako dýška posílané autorům populárních příspěvků jako odměna a finanční podpora, a které jsou realizovány pomocí bitcoinové sítě lightning. Asi je už jasné, že

narativy celého hnutí kolem NOSTR protokolu má takové kryptoměnové vibe, mluví se dokonce o logické evoluci v kryptosvětě.

Proč potřebujeme sociální síť?

Sociální sítě se zdají jako fenomén poslední doby, ale není to úplně pravda. Mezi lidmi se vždycky najde významná skupina lidí, kteří se rádi předvádí před ostatními a další skupinka lidí je nadšeně sleduje. A je jedno, o jaký obsah jde, zda jde o psaný nebo mediální obsah, zda jde o edukaci, politiku, společnost, nebo prostě zábavu. Jedna skupina vytváří obsah, druhá ho konzumuje.

Představa sociálního propojení byla nejprve přisuzována internetu jako takovému. Internet je skutečná síť která propojuje počítače. Každý máme počítač a na něm můžeme zveřejnit námi vytvořený obsah a ostatní počítače v síti si jej stáhnou a prezentují jej konzumentům. Dnes víme, že tahle obecná představa nejspíš selhala. V důsledku nedostatku IP adres je většina počítačů za nějakou formou NATu. Navíc ne každý má počítač připojený k internetu nepřetržitě a je dostatečně zabezpečený a připravený na „dravé“ internetové prostředí. Takže se většina zařízení připojená do internetu stala pasivními konzumenty.

Ale než přišly „velké“ sociální sítě, určité snahy o sebeprezentaci tu byly, a někteří si je dobře pamatují. Kolik geeků v počátcích internetu si vytvářela osobní stránky? (včetně mě). Kdo měl patřičné znalosti, nebo měl známého, který tomu rozuměl, „někde“ na internetu vystavil své osobní „webovku“ a tam se prezentoval. Kolik lidí dnes navštěvují osobní webovky? A kolik tvůrců raději vytvoří profil na Instagramu?

Další stránkou fenoménu je potřeba diskutovat, reagovat, vymezovat se, trolovat, obecně sdílet své názory. I takové možnosti existovaly v pravěkém internetu. Já ještě pamatuji Fidonet a BBS Bajt, kam jsem chodil diskutovat s ostatními anonymními uživateli

o nesmyslech. Kolik čtenářů si pamatuje, jak se přihlásit na Listserv? Kdo si vzpomněl na „newsy“, jak jinak se nazýval NNTP protokol. Dodám, že NOSTR je svým uspořádáním hodně podobný protokolu NNTP. S příchodem webu se rychle objevily služby jako Průvodce, Mageo, Lopuch, a v dnešním internetu stále přežívající Okoun. Samotnou kapitolou jsou diskuze pod novinovými články.

Těsně před vypuknutím boomu sociálních síti si pamatuju na stav českého internetu, kdy osobní stránky měly děti o svých domácích mazlíčcích, koní, nebo poníků z My Little Pony, teenagerky s fotkami, nebo oblíbené herce, osobnosti nebo seriály. Nezbytnou součástí byla i „návštěvní kniha“, kde bylo možné diskutovat se samotným majitelem stránek. Osobní stránky měli i Simpsonovi.

Velcí investoři si uvědomovali tuhle poptávku a převálcovali tehdejší osobní stránky a blogy svými centralizovanými sociálními sítěmi, ve kterých se kdokoliv může jednoduše prezentovat, diskutovat, lajkovat, lze sledovat každého účastníka, a je to za minimální náklady, platí se vlastně jen velice „málo“. Ztrátou soukromí, uživatel prodává osobní údaje, které lze výhodně zpeněžit na reklamním trhu. A nebo lze uživatele vhodně ovlivňovat ať už komerčně nebo politicky a tam právě přichází ty velké peníze. Pokud se někdo prezentuje mimo vymezený povolený rámec, je zablokován a profil mu je smazán. Taková jsou pravidla. A kupodivu to hodně lidí přijímá a rádi centralizované sociální sítě používají. Postupem času ale dochází k "utahování šroubů, cenzuře, a objevuje se nespokojenost.

NOSTR má být jedna z odpovědí na tuto nespokojenost. Jako by se NOSTR pokoušel sloučit to dobré z dob historického internetu, kdy si ti schopnější tvořili stránky nebo blogy, kde prezentovali sebe nebo svou tvorbu a zároveň poskytuje jednotné rozhraní pro konzumace obsahu, reakce a diskuze.

NOSTR ale není jediný pokus na světě, alternativních sociálních sítí vzniklo více, např: Mastodon nebo Diaspora. Otázkou teda je, proč by měl uspět zrovna NOSTR?

Organizace sítě NOSTR

Síť NOSTR staví na dvou základních prvcích. `Klienti` a `Relaye`. Klienta si asi dokáže představit každý, jedná se o webovou, desktopovou nebo mobilní aplikaci, která vizualizuje obsah sítě tak, aby se uživatel v obsahu vyznal, vyhledává a zobrazuje příspěvky lidí, které uživatel sleduje, umožňuje vkládat nové příspěvky, reakce, atd a platit nebo přijímat zapy. To vše zobrazuje v jednotném rozhraní a propojuje obsah s reakcemi na tento obsah.

Pod jménem `Relay` si musíte představit server, ke kterým se klienti připojují. V síti NOSTR to není jediný centrální server. V tuto chvíli už běží stovky těchto serverů. Vznikají z různých důvodů, mohou být tematicky zaměřené, různí uživatelé mohou postovat příspěvky na různé relay, které si vyberou. Někteří uživatelé mohou provozovat vlastní relay, protože chtějí mít svůj obsah pod kontrolou. Některé relay mohou mít exkluzivní obsah a mohou být i placené. Klientská aplikace by měla vynikat v rychlé a efektivní agregaci veškerého sledovaného obsahu z relayi, jejichž obsah uživatelé sledují – ovšem nesledují přímo relaye ale sledují zpravidla uživatele, kteří na ty relaye zasílají obsah a je úlohou klienta aby se připojoval na ty relay, kde se sledovaný publikuje.

Samotný protokol NOSTR je pak postaven nad protokolem WebSockets. Z něho používá textové rámce, kterými si klient a relay vyměňují informace ve formátu JSON. Komunikace je organizována v režimu request-response, kdy klient posílá požadavek a relay na něj odpovídá. Kromě toho se používá režim publisher-subscriber, kdy klient se přihlašuje k odběru novinek, které pak dostává asynchronně v reálném čase.

Jediným objektem, který se po síti přenáší je EVENT. Přesně definovaná JSON struktura:

```
{
   "id":"abc123...",
   "pubkey":"a1b2c3...",
   "content":"text příspěvku...",
   "created_at":1692441451,
   "kind": 1,
   "tags":[
        ["e","aabbcc11...",...],
        ["p","7a8b9f...",...],
        [...]
   ],
   "sig":"ab1c891e820..."
}
```

Každý event má **id** který je spočítán tak, že se obsah speciálním způsobem serializuje (content, kind, tags, created_at, pubkey), aplikuje se **SHA256** a výsledek se zapíše jako hex číslo. Toto **id** se zároveň podepíše soukromým klíčem uživatele a výsledný podpis se zapíše do **sig**. Tímto je autorství příspěvku nezpochybnitelné.

Důležitou roli hrají **kind** a **tags.** Pole kind představuje typ události. Ten říká klientovi, jak má událost interpretovat. Ve specifikaci je velké množství těchto typů, v příkladu nahoře představuje **kind=1** krátký příspěvek „twittrového typu“. V poli **content** najdete text příspěvku. Jiné „kindy“ mohou ale měnit význam pole **content.**

Tagy představují dodatečné informace o příspěvku. Tagů je také nepřeberné množství s různým významem a s různým počtem dodatečných parametrů. Tagy se mohou v příspěvku opakovat. Například pokud píšu reakci na jiný příspěvek, v tagu „e“ specifikuji ID příspěvku, na který reaguji, a v tagu „p“ specifikuji veřejný klíč uživatele, kterého chci zmínit. Přitom mohu samozřejmě zmínit více uživatelů, tak uvedu tag „p“ vícekrát pod sebe.

Některé tagy mají přesně danný globální význam (např „p“ , „e“), u jiných může být význam spjat s použitým **kindem**. Jednopísmenné tagy lze také nechat vyhledat na relay, nebo se přihlásit k odberu

nových příspěvku s daným tagem – takže lze třeba sledovat všechny reakce na můj post tím, že se přihlásím k odběru všech reakcí, které mají v „e“ vložený ID mého postu.

Nové eventy se posílají na relay pomocí zprávy `EVENT`, přičemž relay na to odpoví statusem „OK“ (což je název té zprávy). Relay může event i odmítnout – například kvůli spamu, nebo pokud je relay placená a uživatel nezaplatil.

Eventy lze pak vyhledávat pomocí zprávy `REQ` s definovaným filtrem. A na tu relay odpoví tolikrát zprávou `EVENT` kolik eventů je nalezeno a vyhovuje filtru, na konec odpoví zprávou `EOSE`, čímž oznamuje konec odpovědi a zároveň klienta přihlásí k odběru nových eventů v reálném čase. Pak může poslat další zprávy `EVENT` kdykoliv se takový event publikuje a vyhovuje filtru. Klient může nakonec odhlásit zprávou `CLOSE`

A to je v zásadě celé. Protokol není komplikovaný.

Kryptografie

Co je asi zajímavé na celém systému je použití kryptografie pro identifikaci uživatelů. Uživatelé se tedy nepřihlašují jménem a heslem, nebo telefonním číslem – to všechno by vyžadovalo nějakou centrální registraci a to jde proti duchu decentralizace – uživatel si prostě vygeneruje pár klíčů, kdy příspěvky publikuje pod veřejným klíčem a podepisuje soukromým klíčem. Tohle zpravidla zařizuje klient. Použití klíčů umožňuje uživateli v případě potřeby změnit klienta, nebo změnit relaye na které publikuje, aniž by ztratil svůj profil (obrovský problém, pokud máte účet na Mastodonu a pohádáte se se správcem toho uzlu).

Pokud posíláte soukromé zprávy (DMs), pak je obsah zprávy šifrován, tedy klienti předávají na relay zprávy již v šifrované formě – relay teoreticky nemůže číst obsah zprávy. V současné době se používá NIP-04, který k šifrování používá AES-CBC, kdy se sdílené heslo počítá pomocí Diffie–Hellman algoritmu přímo nad klíči

uživatelů. Celý NIP-04 ale není moc „bezpečný“, protože se šifruje jen zpráva, ale metadata zůstávají nešifrované, takže sice nelze zjistit, co je obsah zprávy, ale lze snadno dohledat, jaké strany spolu diskutují. Tyto problémy jsou adresovány v novém návrhu NIP-24.

Dobrý

NOSTR mě zaujal. Rozhodně si myslím, že je postaven na pěkné myšlence. Není to tedy tak, že bych objevil něco zcela nového. O decentralizované sociální síti jsem uvažoval už od roku 2015, hned po tom, co jsem objevil Bitcoin. Samozřejmě použití soukromých klíčů pro uživatele byla první myšlenka. V šuplíku bych našel několik návrhů protokolu, které jsem nakonec nerealizoval. NOSTR je pozitivní z několika úhlů pohledu: Předně se věnuju programování serverů a napsat ke každému serveru nějakou funkční klientskou část bývá pro mě utrpením. Naprogramovat klienta je často 4× víc práce, než naprogramovat server. A v tomto případě klienti už naprogramováni jsou, stačí tedy dodat vlastní server. Asi by nebylo těžké přijít s vlastním protokolem, ale já nejsem moc úspěšný v prodeji své práce, a je pro mne těžké přesvědčovat další vývojáře, aby použili nějaký můj (pro ně cizí) proprietální protokol.

A NOSTR protokol se stal známým, přestože se nejedná o geniální dílo (viz dále). Jeho autorovi se povedlo dát dokupy mnoho vývojářů, kteří skutečně nad tím něco postavili, a zajistil tak své sociální síti určitý sociální efekt.

Autor také vyvíjí protokol jako open source, k dispozici je github repozitář se specifikací, která je rozdělena na tzv NIPy (Nostr Implementation Possibilities) – je to samozřejmě inspirované BIPy a ty jsou inspirované RFC. Kdokoliv tak může napsat vlastní návrh, zveřejnit jej jako NIP a podrobit jej diskuzi v komunita. Dobré návrhy se nakonec dostanou do specifikace.

Celkově tedy beru NOSTR, jako zajímavý způsob jak se dostat k nějaké opravdu funkční myšlence na decentralizovanou a necenzurovatelnou sociální síť.

Špatný

NOSTR má spoustu negativ. Začnu pěti melouny ($250k) pro **Fiatjaf**ala. Vlastně by mě to mělo být jedno, kam posílá peníze kdejaký internetový milionář po tom, co donutil Elona Muska koupit předražený Twitter. Stalo se to v prosinci 2022, ale od té doby se vývoj moc nepohnul. Například dodnes nemá NOSTR vyřešené šíření médií (obrázky, video, hudba, atd). Pro tento účel se používají centrální servery třetích stran. Tolik k decentralizaci a k odolnosti proti cenzuře. Hlavně bych chtěl vidět, kde se tolik peněz na projektu projevilo. Založení github projektu a sepsání pár pravidel není tak drahé – nehledě na to, že ten už existoval. Takže možná reklama? zapojení více vývojářů? Na čem pracovali?

To se dostávám k dalšímu problému. Jak jsem psal, vzniklo mnoho klientů, ale těch opravdu funkčních najdete pramálo. Klienti často nedodržují specifikaci, vymýšlí si vlastní pravidla, každý jiná a tak se stane, že příspěvek v jednom klientovi se zobrazí jinak v jiném klientovi, nebo se nezobrazí vůbec. Drtivá většina klientů vůbec nerespektuje původní myšlenku NOSTR sítě, kdy by klienti měli provádět chytrou agregaci příspěvků z relayí. To bohužel nefunguje, pokud se uživatel rozhodne publikovat na nějaké vlastní relay, dostane se do izolace a to i přesto, že rozdistribuuje informaci o své domovské relay na ostatní relay, mezi lidi co sleduje. Většina klientů vůbec neumí se připojit na jiné relay. Například Amethyst, který je docela populární. Nebo český pokus Plebstr, ten trpí stejným problémem, můj účet v jeho podání je prázdný, maximální vidím své příspěvky a žádné reakce.

Pokud bych mohl doporučit klienty, tak funguje mi Coracle, jen vám nesmí vadit, jak je neuvěřitelně pomalý. Na desktopu používám linuxový Gossip, ten funguje celkem pěkně, opravdu dokáže

dohledat příspěvky na jiných relay, pěkně řeší discovery, ale je děsivě uživatelsky nepřívětivý.

Na celém návrhu NOSTR protokolu je vidět, že to je psáno z perspektivy klienta. Veškerá „byznys“ logika sítě je řešena na klientské straně, relay je jen hloupá databáze. Perspektiva správce relay je ale jiné. To první, co člověka vyděsí je veřejně otevřená databáze! Zabezpečení nula. Co lze od toho očekávat? Hádáte správně – spam. Tuny spamu. Kdo by nepohrdnul místem zdarma?

Tuhle jsem vystavil nostr relay internetu a po dvou dnech jsem objevil, že ji někdo používá jako git repozitář. Neslyšeli jste o nástroji ngit? Bál jsem se zjišťovat, co se v tom repozitáři nachází, ale asi to nejsou úplně neškodné programy.

Spam se ale objevuje ve velkém i jako klasické příspěvky. Cokoliv člověk zveřejní, prakticky do několika sekund mu přistane reakce lákající čtenáře do nějakého kryptoscamu. Z principu fungování nemůžete zabránit, aby se tam taková reakce objevila. Můžete maximálně uživatele ztišit na své straně (mute). Jenže s tím, jak lehké je vyrobit nový profil má tahle funkce nulovou účinnost. A to jsme na začátku, zatím mi ještě nikdo nenabídl viagru. Zabezpečit relay tak aby zároveň byla použitelná s tou hromadou rozbitých klientů je tedy dost velká výzva.

Ošklivý

NOSTR rozhodně není geniálně navržený protokol. Naopak v něm najdete hrozně moc ošklivých věcí.

Chybějící počáteční handshake

Stalo se dobrým zvykem, že po navázání spojení se obě strany představí. Ten kdo tento protokol navrhoval dost jasně ukazuje, že té věci tak trochu nerozumí, protože tady žádné představování není.

Z perspektivy klienta je potřeba vědět, jaké služby relay nabízí, a tohle řeší NIP-11 pomocí externího dokumentu – tedy není to součástí protokolu, ale je to externí dokument, který si klient musí stáhnout a posoudit. A co víc, nějaký umělec tento dokument umístil na stejnou URI jako je websocketový endpoint a rozlišení funkce endpointu se řeší HTTP hlavičkou.

Bohužel relay je na tom ještě hůř, vůbec netuší, kdo je na druhé straně a co očekává, netuší v jaké verzi protokolu probíhá komunikace a jaké další funkce může klientovi nabízet.

Todle je neduh, který se už bude těžko řešit čistě. Na to měl pan autor myslet na začátku. Kdyby měl nějaké zkušenosti s návrhem protokolů, určitě by to neopomněl.

Nevyřešené sdílení binárního obsahu

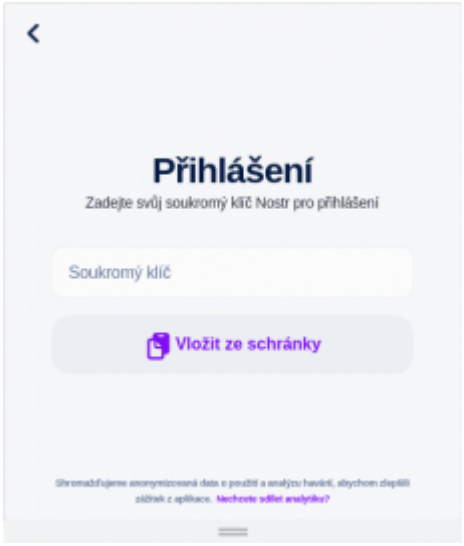
Je až trapné, že tuhle základní funkci NOSTR nemá a komunita není schopná se na tom dohodnout. Koho chce NOSTR oslovit? Jestli chce být konkurencí Twitteru, to je málo, a mladí lidi půjdou radší na Instagram, Tiktok, nebo Onlyfans. Argumentem proti je masivní nárust spamu, nebo šíření dětské pornografie. Nesmysl, protože banujeme technologii kvůli možnosti nevhodného použití. Zakážeme nože, protože se s tím dají zabíjet lidi?

Zde jsem se do diskuze zapojil i já svým návrhem NIP-97.

Uživatelsky nepřívětivé přihlašování.

Přesvědčte uživatele, aby si někam zapsal soukromý klíč? Je to asi problém, usoudila komunita a navrhla zápis soukromého klíče pomocí dvanácti slov, jako to mají Bitcoin peněženky. Z louže pod okap.

Divná je i praktika „zadání soukromého klíče“ do formuláře klientské aplikace. Jakou mám jistotu, že mi ten klíč někdo neukradne?



Trochu se to snaží řešit „signer“, který zpravidla běží jako externí aplikace nebo doplněk, který drží tento klíč a podepisuje eventy. Ale – i tak si myslím že pro uživatele je jednodušší si vytvořit účet na Instagramu, než tohle řešit. Je to prostě ošklivé.

Řešení? Pár bych jich měl, ale to je na delší článek. A samozřejmě, vidle do toho hází rozbité klientské aplikace a obecná neochota podporovat nové NIPy

Nenalezeno

NOSTR velice špatně řeší discovery. Příslušné NIPy se ve specifikaci objevily relativně nedávno, a zřejmě kvůli rozbitým klientům. Původní myšlenka je hezká – zveřejňovat obsah na nějaké relay a všem ostatním poslat informaci, na které relay je ten obsah k nalezení. Bohužel málokterý klient tyto informace umí používat. V důsledku toho že se lidé na siti nebyli schopni navzájem vidět – což je dost zásadní chyba sociální sítě – stalo se zvykem, že většina klientů si oblíbila několik velkých veřejných relayí, kam onboardují nové uživatele a ve výsledku se tedy veškerý obsah posílá „na všechny strany“ do všech těchto relayí. Proč by se někdo měl zabývat nějakou discovery, je chyba uživatele, že nepublikuje na veřejně známou relay – a pak si něco povíme o decentralizaci.

Nevyřešené otázky bezpečnosti

A teď chvíli budu ignorovat společenské otázky bezpečnosti jako šíření fakenews, dětské pornografie, terorismu, nebo nezákoného obsahu, který hrozí na každé síti. Jde mi o otázky zdrojů, zejména na relay. Jak už jsem napsal, otevřenou veřejnou databázi není zrovna jednoduché zabezpečit a nikomu se nechce poskytovat úložiště zdarma. Je nutné počítat s tím, že pokud se síť rozšíří, bude dobře zabezpečená relay cenným zbožím. Nemusí jít jen o místo a boj se spamem. O ngitu jsem už hovořil, ale co třeba decentralizované ulož.to – i kdyby NOSTR nepodporoval binární přenosy, co brání nějakému klientovi ukládat obsah zakódovaný jako text. NOSTR protokol ale umí víc, díky tzv. ephemeral eventům, u kterých relay slouží jako prostředník komunikace mezi dvěma klienty by nemělo být těžké realizovat třeba VPN síť přes NOSTR, za plného zneužití všech současných relay. Je možné, že všechny mé obavy jsou liché. I Bitcoin síť lze zneužít k jiným účelům, například Bitcoin `ordinals` umožňuje uložit do blockchainu libovolný soubor – takže i soubor odporující zákonům – přesto to (zatím) nepředstavuje problém a Bitcoin síť to ustála.

Podivně vedený projekt

Musel jsem si nastudovat několik desítek stránek textu, prostudovat skoro všechny NIPy, abych mohl naprogramovat relay. To bylo konečně mým cílem. Zároveň hledat cesty, jak protokol a celý systém vylepšit, ať už pro mne samotného, nebo pro mou sociální bublinu a ideálně pro celou komunitu. Ale zjistil jsem, že je sice hezké mít něco napsané, když to nedodržuje ani sám organizátor repozitáře. Například jedna z podmínek pro přijetí nového NIPu je referenční implementace na jedné relay a dvou klientech (myšleno třeba na dvě platformy). Přesto v seznamu NIPů najdete takové, které neimplementuje nikdo, což je hloupé v případně, že pro svou stranu kódu hledáte protistranu. Případně zjistíte, že příslušné NIPy se na žádném klientovi neimplementují správně. A opět to spíš ukazuje, že organizátor repozitáře nebude žádný odborník a spíš jen se snaží napodobovat to, co viděl u podobných projektů.

Neexistence oficiální referenční implementace je významnou překážkou v dalším vývoji. Fiatjaf sice má repozitář se svou implementaci v jazyce Go, ale to nedává jistotu, že jde o úplnou referenční implementaci. Když sáhnu po podobném projektu – Bitcoin – tak tam vznikal protokol současně s jeho referenční implementaci která se dnes nazývá Bitcoin-Core. Pokud tedy nějaký BIP není jasné, stačí si otevřít zdrojáky Bitcoin-Core a podívat se, jak je ten BIP implementován.

Závěr

NOSTR je určitě zajímavý počin, který může mít slibnou budoucnost, zároveň je ale před ním dlouhá cesta, kde nebudou jen programátorské překážky. Já jsem si chtěl NOSTR vyzkoušet. Během toho jsem napsal vlastní implementaci relay, kterou najdete na mém githubu. Jen pozor, je to silně experimentální projekt, který je stále ve vývoji, i když už se dá nasadit jako 100% relay. Jen musíte počítat s tím, že nové verze nemusí být kompatibilní se starými, nedávno jsem měnil formát dat a bylo nutné celou databázi smazat. Motivací bylo nad NOSTR postavit osobní blog, tedy provoz vlastní relay mi dává v tomto ohledu smysl. Ale zda se tak daleko dostanu ještě nevím. Mám nutkání si naprogramovat svého klienta, protože z toho, co je k dispozici se mi dělá nevolno. (je pravdou, že se mi dělá nevolno i z předpokládaného objemu práce).

Pokud mne budete hledat na NOSTRu, mám NIP-05 identifikátor ondra@nostr.novacisko.cz (ano, tamtéž běží i má relay)

Přidat názor

- **Dnes 5:22**

  alex6bbc

  mi se libi projekt upspin.io, je za nim treba rob pike.
  jak decentralizovane nabizet sve soubory.
  to by byla zajimava myslenka jak to zkombinovat pro nanizeni binarnich dat.

- **Dnes 5:29**

  alex6bbc

  a nebo by relaye drzely treba jen nekolikadenni databazi a tim setrily svuj prostor a klient by si musel u sebe ukladat historii pokud by chtel. tim by se vyresilo i pravo na zapomenuti :-)

Přidat názor