Introducción a Nostr

@gzuuus

Que es nostr?

- Notes and Other Stuff Transmitted by Relays / Notas y otras cosas transmitidas por los relays
  - "Si una plataforma es un castillo(twitter, facebook, etc.), un protocolo es un río: nadie es su dueño, y todo el mundo es libre de nadar". Edward Snowden
  - Nostr hace posibles redes sociales globales, descentralizadas abiertas y resistentes a la censura. Es nuevo y puede resultar confuso al inicio, pero también es genial.
- Nostr no es una plataforma, no es una empresa, no tiene un servidor central.
  - A diferencia de Twitter o Facebook, Nostr es descentralizado. No hay servidores centrales ni empresas que controlen lo que puedes publicar y lo que otros pueden ver, no hay ninguna entidad central. Nostr es resistente a la censura y de código abierto. La licencia de Nostr es simplemente "Dominio Público".

    - https://github.com/nostr-protocol/nostr
- Piensa en Nostr como una red social, que puede funcionar de forma similar a Twitter, en la que puedes crear publicaciones o "notas" (como un tweet), dar "me gusta" a publicaciones, seguir a personas, repostear publicaciones (como un retweet), intercambiar mensajes directos, e incluso hacer tips a través de lightning network⚡.
- El diseño de nostr esta basado en tres componentes esenciales, **clientes, relays y eventos o notas**. Cada usuario usa un cliente y estos se conectan a relays para recibir y enviar eventos.
    - Los relays son servidores que solo guardan y reciben peticiones para servir eventos. Cualquier persona puede correr su relay o usar uno publico.
    - Los clientes o apps son interfaces para conectarse a relays e interactuar con la red de nostr. Hay muchos casos de uso para los clientes. Social, mensajería, juegos, etc.
    - Los clientes o apps son interfaces para conectarse a relays e interactuar con la red de nostr. Hay muchos casos de uso para los clientes. Social, mensajería, juegos, etc.
    - La identidad en nostr o los perfiles, están basados en pares de llaves (publica y privada), como bitcoin, si tienes el control de tu llave privada puedes enviar mensajes o eventos e interactuar. La gente puede encontrarte e interactuar contigo a través de tu llave publica
- El protocolo define un conjunto de reglas que relays y clientes utilizan para comunicarse (como Bitcoin, el correo electrónico o Bittorrent). Nostr no es una aplicación ni una "plataforma", pero muchas aplicaciones o clientes pueden construirse sobre Nostr.

Como funciona?

Identidad o perfiles en nostr

- La identidad en nostr esta basada en pares de llaves, una privada y una publica, como en Bitcoin o PGP/GPG. Un par de llaves conforman una identidad o perfil con la que se podría empezar a publicar o interactuar en nostr.
    - Puedes obtener o generar tantos pares de llaves como quieras, son ‘infinitas’ y no tienes que pasar ningún tipo de proceso kyc para generar nuevos pares de llaves.
    - No hace falta estar conectado a internet para generar nuevas claves, puedes generarlas offline.
    - No necesitas permiso de nadie para generar u obtener tus llaves
    - Existen diferentes métodos para generar nuevas claves
        - Con un gestor de llaves como alby o nos2x (recomendado)
        - Con openssl `openssl rand -hex 32`
        - Startr para generar tu par de llaves y almacenarlas en un archivo encriptado y portable
        - Con rana o nostril para ‘minar’ llaves. (Ej. npub1gzuushllat7pet0ccv9yuhygvc8ldeyhrgxuwg744dn5khnpk3gs3ea5ds)
- Una vez generadas tus nuevas llaves podrás utilizar cualquier cliente y empezar a agregar metadatos que quedaran asociados a tu llave publica. Ej. Foto de perfil, handle, nombre, nip05, LN address, etc. De esta forma cuando alguien busque tu clave publica en algún

cliente también vera los metadatos asociados a ella
    - Los metadatos asociados a tu llave púbica también conforman un evento, en este caso kind 0 para metadata y kind 3 para tu lista de contactos o follows
    - Toda interacción representa un evento que envías o recibes de relays, seguir a una persona, escribir una nota, darle ‘me gusta’ a una nota, enviar un mensaje directo.

Llave publica

- Piensa en la clave pública como tu nombre de usuario (como tu @handle en Twitter) o un identificador único
- Aspecto de una llave publica:
    - Diferentes formatos, misma llave
        - Bech32: npub1gzuushllat7pet0ccv9yuhygvc8ldeyhrgxuwg744dn5khnpk3gs3ea5ds
        - HEX (antiguo): 40b9c85fffeafc1cadf8c30a4e5c88660ff6e4971a0dc723d5ab674b5e61b451
    - Se puede hacer la conversion entre un formato y otro con algunas herramientas como damus.io/key/ , nostrcheck.me/converter/ , o Startr.
- Para encontrar a otro usuario de Nostr, sólo tienes que buscarlo en el cliente de tu elección utilizando su clave pública. Una vez encontrado podrás seguirlo/interactuar
- También existen directorios que facilitan encontrar a personas:
    - ~~https://bitcoinnostr.com~~
    - ~~https://nostr.directory~~
    - ~~https://nostrplebs.com/directory~~

Llave privada

Piensa en tu clave privada como tu contraseña o tu llave privada de bitcoin; NO LA COMPARTAS CON NADIE. Con ella podrás firmar los mensajes o notas e interactuar con el resto de la web

- Aspecto de una llave privada:
    - Diferentes formatos
        - Bech32: nsec1g56vl9475frrxtycwc8vkvnkvpxjv9k5q97t2eyfdesw93amkx4s6sqwls
        - HEX(antiguo): 4534cf96bea246332c98760ecb3276604d2616d4017cb564896e60e2c7bbb1ab
        - BIP39, mnemonic: early please toss later caught book raven attract attract flower outside scene sponsor arena exotic convince rely cattle fortune scrub cluster tape shop horror
- Tu llave privada es algo sensible y debe de tratarse con las consideraciones necesarias. Usa un gestor de contraseñas para guardarla de forma segura o alguna otra alternativa como Startr para almacenarla de manera apropiada.
- Tu llave privada te dará acceso y privilegios para interactuar con tu perfil en nostr y los diferentes clientes. Sin embargo, si se trata de un cliente web es extremadamente

recomendable (se podría decir obligatorio) usar un gestor de llaves como puede ser alby o nos2x. Estas son extensiones que instalas en tu navegador, con ellas tu llave privada estará segura y podrás usar cualquier cliente web de manera segura.
- Si no usas estos gestores de llaves en clientes web tu llave privada podría quedar comprometida.

Arquitectura

Que es un cliente de nostr?

- **Clientes**
  - Para utilizar Nostr, debes usar un cliente. Hoy en día hay muchos y esto es solo el principio.
  - Un cliente es una aplicación diseñada para interactuar con el protocolo de nostr, es simplemente una interfaz con la que puedes conectar con relays de tu elección, recibir actualizaciones de las cuentas que sigues (consultar tu feed), enviar notas, e interactuar. Hay clientes web, móvil, clientes nativos de escritorio, etc.
  - Los clientes son como la aplicación de telegram o twitter por ejemplo.
  - Para publicar algo en Nostr, escribes una nota en tu cliente favorito, lo firmas con tu llave privada y esta se enviará a tus relays configurados
  - Nostr es un protocolo abierto y, por lo tanto, los clientes son inter-operables, esto quiere decir que puedes utilizar cualquier cliente para interactuar con la red, mientras estés conectado a los mismos relays siempre obtendrás la misma información (tu perfil, follows, followers, etc) independientemente del cliente que uses.
  - El protocolo de nostr permite crear clientes para diferentes casos de uso. Por ejemplo para redes sociales como twitter, para comunicación o chat como telegram, para fotos y social como instagram por ejemplo, lector de rss, etc.
  - Nostr tiene el potencial de sustituirlos a todos
- **Clientes recomendados:**
  - **Web:**
    - **snort.social**
    - **ris.to**
  - **Android:**
    - **Amethyst**
    - **Nostros**
  - **Ios**
    - **Damus**
  - **Escritorio (avanzado):**
    - **Bija**
    - **Nostr_console (CLI)**
    - **Gossip**

Notas, eventos o mensajes

- Se denominan notas, eventos o mensajes a todas las publicaciones o interacciones que suceden en nostr.
- Toda interacción en nostr representa un nuevo evento.
- Toda interacción representa un evento que envías o recibes de relays, seguir a una persona, escribir una nota, darle ‘me gusta’ a una nota, enviar un mensaje directo.
- Los eventos a nivel de protocolo están construidos en formato JSON, un lenguaje ampliamente utilizado en el mundo de la programación y comunicación en protocolos web como las APIs.
- El formato JSON esta basado en una estructura {Clave:Valor} y puede almacenar diferentes campos dentro de un mismo registro
- Los eventos de nostr tienen diferentes campos que conforman su estructura y determinan de que tipo de evento se trata (nota, ‘me gusta’, follow, etc.)
- El tipo de evento se especifica en el campo “kind”

Que es un relay?

Relays

- Un relay es un servidor alojado por ti o por otra persona; cualquiera puede montar y gestionar un relay.
- Los relays funcionan como bases de datos que **guardan notas de personas y las reenvían a otras**. Ej. Dame todas las notas de esta llave pública entre este rango de fechas
- Un relay es ‘tonto’. Tanto la firma como la presentación de las notas sucede de lado del cliente.
- Para obtener actualizaciones de otras personas, se pregunta a varios relays si saben algo de esas otras personas.
- Hay relays públicos y de pago
- La url de un relay tiene este aspecto: **wss://eden.nostr.land**
- Los relays usan el protocolo websocket (wss://…) para conectar con los clientes. Websocket es un protocolo web moderno que permite la comunicación asíncrona y canales de comunicación bidireccionales que se mantienen abiertos. Esto es ideal para recibir actualizaciones en tu feed sin tener que actualizar la pagina web.
- Un relay propio o auto hospedado se podría ver como una forma de hacer backup de tu actividad en nostr, si tienes tu propio relay para tus notas/eventos nadie podrá borrarlos nunca. Si usas un relay publico o de pago y este desaparece, también lo harán tus notas o eventos que tengas alojados en ellos.
- Poco a poco se hará **más fácil** tener un relay propio e incluso que este retransmita o haga mirroring(reenvíe) a otros con más ‘visibilidad’ para que tus notas sean visibles a la red.
- Hay diferentes implementaciones de relays. Las diferencias son los lenguajes de programación en las que están escritos y diferentes características o funcionalidades.

- Se están desarrollando nuevas implementaciones de relays llamados ‘proxys’ que tienen la función de retransmitir tus eventos a una serie de relays públicos, de esta forma tu solo te conectas a un relay proxy y este se encarga de conectarse a otros relays para retransmitir tus eventos CC.

Relays públicos

- Los relays públicos son abiertos y puedes usarlos para mandar y recibir notas.
- Puedes encontrar una lista de relays públicos con información y estadísticas sobre ellos en https://nostr.watch/

Relays de pago

- Los relays de pago tienen **restringida la escritura** para los usuarios no registrados, pero **cualquier usuario podría leer.**
- Un relay de pago tiene la ventaja de filtrar spam y de ser mas estable/confiable.
- Por supuesto el pago es con bitcoin.
- Pues encontrar una lista en https://relay.exchange/

Como usar nostr

Todo el mundo usa un cliente. Puede ser un cliente de escritorio, web, móvil, etc. Para publicar algo, escribes un post, lo firmas con tu clave y lo envías a múltiples relays. Para obtener actualizaciones de otras personas, preguntas a varios relays si saben algo de esas otras personas. No hace falta “confiar” en los relays. Las firmas se verifican en el lado del cliente.

Configuraciones para usar nostr

Como ya habrás percibido la experiencia de usuario de nostr es modular, osea tienes diferentes clientes con los que puedes interactuar en la red, tienes una serie de relays publicos y privados. No hay una unica manera de usar nostr y esto es bastante llamativo y se aleja del modelo convencional de redes sociales a las que estamos acostumbrados donde entras y la experiencia de usuario esta bien definida y acotada. En nostr cada uno diseña su experiencia de usuario, elige sus clientes favoritos y los relays a los que se conecta.

Como selecciono los relays a los que me conecto y a cuantos?

- La selección de relays y el numero de ellos a los que te conectas realmente variara en función del caso de uso. Pero en general conviene conectarse a algún relay ampliamente

usado (puedes ver una lista en https://nashboard.space/ en la sección “MOST CROWDED RELAYS”) y sobre todos a los relays que usen las personas que sigas para estar seguro de que recibes actualizaciones con sus nuevos eventos. Normalmente en los clientes encontraras la información de que relays usan las personas a las que sigues.
- También conviene entender que mientras a mas relays estés conectado mas conexiones abiertas tienes y mas consumo de datos y batería tendrás. Esto es importante sobre todo si usas nostr en el móvil.
- Una cantidad optima de relays no hay, pero digamos que con un numero entre 5 y 10 relays bien seleccionados tienes mas que suficiente.

Bitcoin y nostr

- Nostr fue creada por un bitcoiner y desarrollador de lightning bien conocido (fiatjaf) Por lo tanto bitcoin y ln están bastante presentes en el diseño de nostr. Hoy en día el protocolo ofrece un nivel sin precedentes de integración con LN en comparación con cualquier otra plataforma o medio de comunicación social.
  - De forma nativa puedes establecer una ln address como un metadato mas en tu perfil para recibir pagos o tips.
    - Esto significa también poder pagar o tipear fácilmente a cualquier usuario de la red.
  - Muchos clientes hoy en día tienen un botón para dar tips o “zaps”.
  - Zaps (NIP-57) esta es una nueva forma de tipear que tiene asociados unos metadatos para hacer la función de tips mas social e interactiva con nostr. Adios like, hola Zap!
- Otros proyectos interesantes relacionados con bitcoin y nostr:
  - Joinstr, implementación de coinjoin sobre nostr
  - Mostro, intercambio p2p sobre nostr

Consejos de seguridad y privacidad al usar nostr:

Llaves privadas

- Gestión de tu llave privada
- Tu llave privada te da acceso a gestionar tu perfil, publicar, reaccionar. Guárdala debidamente en tu gestor de contraseñas (bitwarden, lastpass, no bloc de notas) o en un archivo de Startr
- En clientes web es prácticamente obligatorio usar extensiones como alby o nos2x

Cross Site Scripting (XSS)

Si no usas una extension para el navegador como alby o nos2x puede haber filtrado de llaves privadas al copiar/pegar directamente en clientes web. Solución: nos2x and Alby

Protección de tu dirección IP

Los operadores de relays pueden conocer tu ip pública cuando te conectas a su relay. (Realmente como cualquier página web en internet). Solución:

- Usa una VPN o TOR
- Usa relay conocidos y de confianza
- No hagas click en enlaces extraños
- Usar tu propio relay junto con un VPS y reverse proxy para que este se encargue de retransmitir a otros relays públicos (avanzado y en desarrollo)

Suplantación de identidad

Cualquiera puede crear un nuevo par de llaves y usar la foto/datos de una persona conocida. Por eso debes verificar los perfiles antes de interactuar con ellos. No te fíes de DMs aleatorios o de “envíame un bitcoin y te devuelvo dos”. Solución:

- WoT (web of trust) es un concepto con bastante historia utilizado en PGP, GnuPG y otros sistemas criptográficos basados en pares de llaves para establecer la autenticidad del enlace entre una clave pública y su propietario.
- Metadata asociada al perfil, mientras mas datos relacionados con el propietario mas verificable es.
- Verificación NIP05, es una especificación nativa de nostr, relacionado con WoT. Si un perfil tiene una dirección nip05 con un dominio de internet bien conocido es una buena forma de verificar la autenticidad del perfil

Mensajes privados

Los mensajes privados en nostr son eventos iguales que las notas publicas pero encriptados, por lo que solo son legibles por el receptor y poseedor de la llave privada asociada a la llave publica. Aun que nadie puede leer el contenido, cualquiera podría ver que ha habido una interacción entre dos llaves publicas (ojo). La manera mas segura y privada para intercambiar mensajes privados con otra persona seria usar un relay propio o uno “desechable”.

Borrar

En nostr si quieres borrar una nota tienes que hacer una petición a los relays a los que hallas enviado la nota para borrarla.

Bloquear y mutear

En nostr puedes bloquear y mutear usuarios. El bloqueo es una opción que ofrecen algunos clientes (Ej. snort.social). El muteo es una especificación nativa de nostr y es simplemente otro tipo

de evento. Ojo, tu lista de muteados es publica.

En que momento se encuentra nostr?

- Nostr se creó en 2020 y está en continuo desarrollo
- Es el inicio, a penas se esta viendo todo el potencial que tiene este protocolo.
- Cada vez están llegando mas personalidades reconocibles a nostr como Jack dorsey, Edward Snowden, Anita posch, etc.
- El desarrollo está siendo **frenético y excitante.** Cada día salen nuevos clientes o actualizaciones. (Puedes encontrar una lista curada de proyectos en nostr en **nostr.net)**
- Tu también puedes crear o desarrollar sobre nostr, es muy divertido y agradecido. Cada vez existen mas librerías para diferentes lenguajes de programación. Usa tu lenguaje favorito, no necesitas aprender uno nuevo.
- El crecimiento de la red se esta acelerando.
- Estadísticas: https://nostr.band/stats.html

Por que nostr es importante?

- Es un protocolo abierto y de dominio público. Los protocolos abiertos son nuestra mejor baza para un futuro libre.
- Ante la creciente restricción de la libertad de expresión y el control de los contenidos en plataformas centralizadas, Nostr supone un cambio trascendental como herramienta para la libertad de expresión.
- No hay ningún algoritmo entre bastidores que decida lo que ves y lo que permanece oculto o que fomente tendencias, publicidad o propaganda; ves lo que quieres ver. No echo chambers.
- Además, Nostr es simplemente divertido. La gente experimenta, se ayuda mutuamente y trabaja unida por un futuro menos sombrío.
- Nostr en su diseño es similar a bitcoin en algunos aspectos y puede conformar una capa de comunicación social muy interesante que integre Bitcoin de forma nativa.

Gracias!

@gzuuus
npub1gzuushllat7pet0ccv9yuhygvc8ldeyhrgxuwg744dn5khnpk3gs3ea5ds

Canal de nostr_es en telegram : https://t.me/nostr_es
Presentacion: Introduction to Nostr (English) :
https://www.canva.com/design/DAFcs32eM7k/1twoK_IqInXQm5txlZBLCg/view

Revision #7
Created 27 November 2024 23:46:13 by meowtoshi
Updated 28 November 2024 00:14:04 by meowtoshi