Lighting Network (LN) - BITCOIN - Criptomonedas

La idea inicial es responder a estar preguntas:

1. Que es Nostr
2. Cómo crear un perfil en nostr
3. Cómo crear una wallet de lighting
4. Cómo vincular el perfil de nostr con una wallet
5. Como ingresar a fountain con el perfil de nostr, subir un post y personalizar el post para recibir donaciones por zaps de satoshis

Sin embargo creo que antes de llegar a esto, deberíamos tener muy claro las respuestas a estas preguntas.

1. Qué es bitcoin
2. Cómo funciona bitcoin
3. Qué son y cómo funcionan las Wallets
4. Qué son y como funcionan los mineros
5. Qué son los forks
6. Qué es la blockchain

Para luego entender un poco a grandes rasgos LN y todos los beneficios que trae para asi, posteriormente entrar a resolver las preguntas iniciales.

Qué es bitcoin

Para poder entender qué es bitcoin, primero necesitamos entender el sistema bancario tradicional.

Cómo funciona el sistema bancario tradicional

El sistema bancario tradicional tiene 3 pilares:

- **Los usuarios:** personas normalmente mayores de 18 años, que poseen una identificación de estado (cédula de ciudadanía), poseen ahorros y que pueden abrir una cuenta en un banco.
- **Los proveedores:** Normalmente es una institución reconocida, que tiene una credibilidad y que está regulada. Estas instituciones conocidas como bancos, ofrecen un SERVICIO de guardar los ahorros de los usuarios a cambio de un interés.
- **El regulador:** Emite las licencias que un banco adquiere y escribe las normativas a las cuales un banco se somete para poder operar sobre un país.

Hay un cuarto pilar que está omnipresente entre los pilares, y es **el estado**. Y es el estado porque el estado emite las cédulas de ciudadanía que usan los usuarios para crear una cuenta bancaria. Y a su vez están por encima del ente regulador, y esto es; porque da apoyo al ente regulador porque el estado es quien tiene el control del poder policial.

Acuérdate que las tres ramas del poder: El poder legal, el poder judicial y el poder económico dependen directamente del estado.

Usuarios: Normalmente el usuario usa su cédula de ciudadanía para verificar que con ella, el es, efectivamente; el dueño de los fondos de una cuenta x. Si se llegase a perder su tarjeta de banco, podría ir a una oficina bancaria y por medio de su cédula de ciudadanía el banco puede verificar que realmente es él quien es el dueño de esa cuenta y por consiguiente de los fondos que esta posea, donde podría el banco expedirle otra tarjeta bancaria y si se necesitase, el usuario podría retirar dinero en ese momento.

Bancos: Ofrecen a los usuarios guardar sus ahorros porque estarán más seguros que si estuvieran en su casa. Como normalmente están compitiendo entre sí, ofrecen un cierto **tipo de interés** por guardar su dinero con ellos. Luego lo que ocurre es que el banco presta dinero a otro usuario y en ese proceso el banco gana dinero por el interés que ese usuario paga por el dinero prestado del banco.

Cuando los ahorros de un usuario x son depositados en un banco x, el banco x lo que hace es que crea un registro en una base de datos, esa base de datos por decirlo de algún modo, es como la caja fuerte del banco, porque en esa base de datos es donde dice que el usuario x tiene x millones/plata. Finalmente los bancos adquieren las licencias de un regulador para poder operar sobre un país, a cambio estos se someten a las normativas que el regulador establece.

Conseguir/idearme imágenes para poder hacer un video explicando esto

Cómo funciona bitcoin

Al igual que el sistema bancario tradicional, podemos decir que el bitcoin también posee tres pilares:

- **Los usuarios:** Son las mismas personas que en el sistema bancario tradicional, solo que en el ecosistema de bitcoin para identificarse poseen un par de llaves/claves llamadas: llave/clave pública y llave/clave privada. Que se crean a partir de una wallet (billetera) pero no es necesario tenerla.
- **Blockchain/Mineros:** La blockchain es la única gran base de datos que controla las transacciones de los usuarios en la red bitcoin, sería como el proveedor/servicio en el sistema bancario tradicional. Los mineros son la gran red distribuida que valida las transacciones realizadas por los usuarios.
- **Los desarrolladores:** Comunidad de usuarios que escribe y mantiene el código de bitcoin, ademas de que son usuarios del mismo, y esto es así porque el código de bitcoin es opensource o código abierto.

Los usuarios en el sistema de bitcoin son los mismos, en lugar de ir a los proveedores con una identidad **(cédula de ciudadanía)**, se dirigen a una **wallet (billetera).**

Qué son y cómo funciona la wallet

Aunque este nombre suele ser muy ambiguo, porque más que una billetera lo que es en realidad es un **llavero**, porque es aquí donde se almacenan un par de claves: **clave pública y clave privada.**

En cuanto a las wallets, hoy en día existen muchas, pero básicamente se dividen en dos grupos:

- **Hot wallet:** monederos 100% online, que pueden ser aplicaciones o incluso se pueden instalar como extensiones al navegador.
- **Cold wallet:** monederos físicos (hardware) cuya premisa común es que funcionan sin conexión a internet y son dispositivos físicos, lo que les convierte en la opción más segura. La opción barata es una usb (Electrum + tails (Linux)) la opción cara es ledger y las otras. Hay otras incluso en papel. Paper wallet

Cuando se usa una app wallet, al momento de crear la billetera, se crean dos claves: **la clave privada y la clave pública.**

La **clave privada** no se comparte con nadie, es para uso personal y es la que **nos permite enviar/mover bitcoin a otro usuario u a otra wallet.**

La **clave pública** en realidad pueden ser muchas, para este caso imaginemos que solo es una. Y esta es la que se comparte con otro usuario para poder recibir bitcoin, pero además nos ofrece más posibilidades que las mencionare en unos instantes.

Voy a poner un ejemplo para que quede más claro.

La clave pública es similar a un número de cuenta bancaria, pongamos de ejemplo Bancolombia. Esta la podemos entregar a cualquier persona para que nos envíe dinero, sin el riesgo de que nos pueda extraer los fondos. En el ecosistema bitcoin: a través de la **clave pública** se generan direcciones para **recibir, consultar y ver el estado** de nuestros fondos.

La **clave privada** es el **número de 4 dígitos** que se usa por ejemplo para retirar dinero de un cajero o un pack en tiendas o establecimientos que ofrezcan el servicio. O la **clave dinámica** (normalmente una serie de números aleatorios que se generan en la app personas instalada en Android e Iphone) que se usa para transferir fondos a otro usuario o realizar compras digitales.

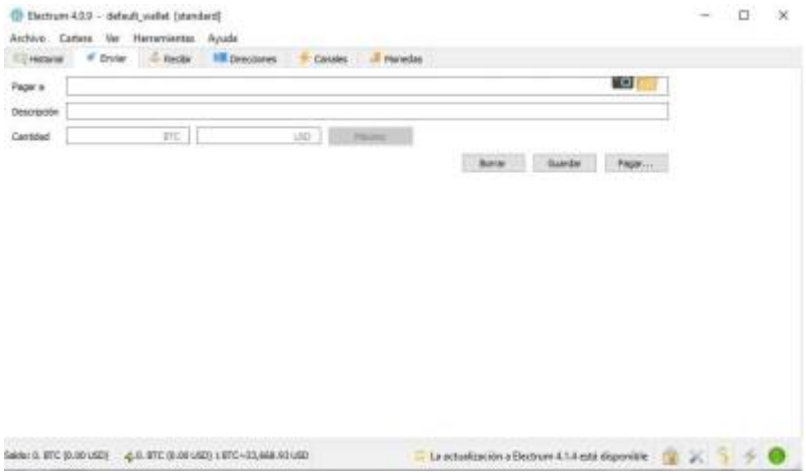
Hoy en día existe un gran gama de variantes de Wallets. Con la adopción de Bitcoin como moneda de curso legal en **El Salvador** y la **República Centroafricana**. Las opciones de uso de las wallets y la red Bitcoin se expandió, esto con la finalidad de mejorar la capacidad y la velocidad de las transacciones lo cual veremos en detalle mas adelante.

Conseguir/hacer imágenes para hacer un video de esto

Entonces cómo sería una transacción de bitcoin entre un usuario A y un usuario B ?.

El usuario A desea recibir del usuario B 5 bitcoins. Por lo tanto; el usuario A envía una clave pública al usuario B, el usuario B escanea un código Qr que contiene la **clave pública** del usuario A, o puede recibir directamente la **clave pública** enviada por el usuario A.

Cuando el usuario B recibe la clave/dirección, lo que hace es que en su wallet: (por ejemplo electrum) genera un nuevo pago en el cual hace una descripción del pago, ingresa la **dirección pública** recibida por el usuario A y finalmente escribe la cantidad de bitcoin a depositar. Cuando se hace el envío, la wallet aplica la **clave privada** a este recibo para que este nuevo evento sea validado por los **mineros** y luego **ejecutado en la blockchain.**



Si en el sistema tradicional los bancos son los que tienen las bases de datos que contienen la información de los usuarios con sus fondos. En el ecosistema bitcoin esto como es ?

En la antigüedad cuando yo ponía dos lingotes de oro en un banco y luego 1 lingote de oro en otro banco, eran cajas fuertes distintas. Una innovación que hace bitcoin es que **solo hay una caja fuerte**. Es como si fuera un banco enorme lleno de puros lockers. Entonces esta gran caja fuerte sería **la base de datos**, esta gran única base de datos estaría llena de registros, serían como buzones cerrados que solo **llaves/claves privadas** pueden abrir.

Entonces mientras que en el **sistema tradicional** existen x cantidad de base de datos por banco, en el **ecosistema bitcoin** existe **una sola base de datos**, más conocida como ***blockchain.***

Regresando al ejemplo anterior, donde se responde a la pregunta de cómo sería una transacción de una usuario A a un usuario B teniendo en cuenta la **blockchain** sería lo siguiente.

El usuario A desea recibir del usuario B 5 bitcoins. Por lo tanto; el usuario A envía **una clave pública** al usuario B. Para poner una analogía sería que en la **blockchain**, el usuario B abre una caja con su **llave privada** donde en esa caja deposita 5 bitcoins y la vuelve a cerrar con la **llave pública** que recibe del usuario A a quien envía los 5 bitcoins.

Entonces en general **la wallet (que sería un llavero realmente)** es la pieza de software que me permite a mi transaccionar con bitcoin/satochis por medio de mis claves pública/privada sin entender cómo estos eventos de pagos y recibos se hacen en la blockchain.

Qué son y como funcionan los mineros

Si las bases de datos en el sistema tradicional están almacenadas en bancos, ¿dónde está la blockchain ?

En el sistema bancario tradicional cada banco tiene su propia base de datos de clientes. En el ecosistema bitcoin la base de **datos o blockchain** está en muchos lugares a la vez. Esto quiere decir que la **red bitcoin** está compuesta por una red de computadores llamados **mineros** que se comunican entre sí.

Cada **computador/nodo/minero** está conectado con todos los demás y a su vez **cada minero tiene una copia de la gran base de datos.**

La confianza que hay en bitcoin es que **no depende de una persona o institución** que maneje el dinero sino, en cambio; **es una red descentralizada de computadores**. En el sistema bancario tradicional solo poseo 10 o 15 entes bancarios donde guardar mi dinero y que además aquí en colombia, no ofrecen oportunidades como el **interés compuesto**...., en el ecosistema bitcoin tengo miles de mineros y podría hasta montar mi propio nodo para poder así, **tener el control total de mi dinero**, sería así pues, mi propio banco porque tendría mi propio **operador en la red.**

Volviendo al ejemplo donde un usuario A recibe dinero de un usuario B. Entonces cuando el usuario B configura su wallet para enviar bitcoin, **la wallet realmente lo que hace es hablar con un nodo/minero.**

Ahora, en el sistema bancario tradicional un usuario escoge uno u otro banco dependiendo del **nivel de popularidad o rentabilidad** que este le de. Pero en el sistema bitcoin esto cambia. Por qué la pregunta sería:

Qué es la blockchain

¿ Cómo hace una wallet para interactuar con todos estos mineros ?

La respuesta a esta pregunta realmente es más profunda porque ya entramos a detallar **cómo es que funciona realmente la blockchain**. Pero para entenderlo a grandes rasgos, lo dejaremos en un nivel alto para que se pueda entender.

Entonces la **blockchain** es una red que está **compuesta de computadoras** llamados **mineros**, donde cada minero ejecuta **el mismo software**. Cuando las transacciones que hacen los usuarios **llegan a 1000**, ocurre un trigger o **disparo en la red.**

Este pistoletazo hace que se les dé a todos los mineros que componen la red de bitcoin, un **problema matemático**, que surge de esas transacciones concretas. Es decir: si hubieron transacciones de A → B eso es un problema matemático. Y si hubieron transacciones de F → G → A → C es otro problema matemático. El **problema depende entonces de las transacciones que vengan en ese lote por decirlo así.**

Este p**roblema matemático tiene la particularidad de que no tiene solución**, es decir: no tiene una fórmula para llegar a la solución. Entonces, como no hay una fórmula para resolver el problema,

se llega a ella probando. Esto quiere decir: que se cambia un parámetro en la solución, el minero corre la solución para ver qué resultado da y si ese resultado es el esperado.

Entonces en resumen: cuando las transacciones que hacen los usuarios en la red bitcoin llegan a 1000, el software que corre en los mineros les dice a estos; es algo como una lotería: encuentra un valor aleatorio que haga que la solución a este problema matemático sea x. Entonces lo que hacen los mineros es empezar a poner valores aleatorios en este problema matemático usando algo que se llama la fuerza bruta.

Entendemos entonces que los **mineros al no necesitar intervención humana para operar**, salvo para mantenimiento del hardware y actualización del software. **No necesitan un ente regulador porque están automatizados** y funcionan como explique anteriormente, por medio de un sistema parecido a una lotería para dejarlo en analogía.

Ahora la pregunta que surge después de esto es...

¿ y las normativas... los reguladores, que papel toman en el ecosistema bitcoin si no existen ?

El código que corre en los mineros es **software libre**, open source, **aquí estamos hablando más del mundo linux.** Al ser software libre cualquier usuario puede acceder a él y modificarlo o cambiarlo. Entonces existe una comunidad de desarrolladores que hablan por reddit, por twitter, y que están desarrollando el código que luego los mineros van a ejecutar.

Entonces en el **sistema bancario tradicional** existe **un ente regulador** porque **es la única institución que tiene el poder que le ha otorgado el estado** para escribir normativas a las cuales los **bancos se someten les gusten o no.** Y son también los **entes reguladores** quienes **usan el poder** judicial, la policía y todos los mecanismos que tiene el estado **contra los usuarios.**

Porque por ejemplo si un usuario se somete a pagar a un banco cada mes una cuota de un préstamo y este no cumple. El banco va a ir al estado a decirle que el usuario x no ha cumplido lo que quedó en un contrato y es allí cuando se aplican los poderes del estado para que este usuario x cumpla o cumpla.

A lo que quiero llegar con todo esto es que en el **sistema bancario tradicional todo el poder recae en una sola voz...** que sería el ente regulador, o el banco central, etc... es decir, **una sola persona.**

En el **ecosistema bitcoin** en vez de un regulador, **lo que hay son usuarios como tú o como yo**, pero **son programadores o desarrolladores**. Y estos trabajan por consenso.

Por ejemplo, imagínate que la versión del software que corre en los mineros de repente ha quedado obsoleta o se quieren introducir nuevos cambios en este. Por ejemplo, si cada vez más gente adapta bitcoin en su día a día, más transacciones se van a realizar por segundo, lo que conlleva a que el sistema se vuelva lento y quizás se tengan que realizar mejoras en cómo funciona el sistema de lotería o entrar a analizar otros detalles.

Entonces aquí lo que ocurre son dos cosas: se llega al consenso, donde todos los programadores se ponen de acuerdo para escribir un solo código que ejecutan los mineros.

Y lo otro es lo contrario, que no haya consenso entonces ocurre una **separación (fork)**

Qué son los forks

Esta **bifurcación** de los **programadores** que sostienen el código de bitcoin, lo que significa es que: **donde antes había una pieza de software, ahora hay 2.**

Entonces lo que ocurre aquí es que antes del divorcio, existía solo una **única línea temporal**, después de la separación, se crean ahora dos caminos creando **ahora dos líneas temporales** en vez de una sola y original.

También puede ocurrir que las **discrepancias ocurran porque los mineros pueden variar en tamaño,** haciendo que se tomen decisiones sobre el código que corre en estas máquinas y estas actualizaciones pueden hacer que los equipos de desarrolladores **tomen diferentes caminos** para la **optimización** de los mismos. Es como si fuera una **competencia entre ellos,** y no solo eso, también el desacuerdo puede venir de los mismos usuarios ya que algunos claman que quieren que el bitcoin sea un reemplazo para el oro.

Resumen General Que es Bitcoin

Entonces resumiendo todo el esquema completo, desde el sistema bancario tradicional al ecosistema bitcoin atravesándolo por cada uno de los tres pilares que son los usuarios, los proveedores y la normativa. Notamos cambios importantes en cada uno de esos tres pilares:

- En el **pilar de los usuarios** pasamos de tener un sistema donde se usa una **cédula de ciudadanía**, a usar **claves criptográficas.**
- En el **pilar de los proveedores** pasamos de tener un **grupo reducido de bancos** a una s**ola base de datos con miles de computadoras**.
- Y en el **pilar de la normativa** pasamos de tener un **solo ente regulador que depende del estado,** a un sistema constituido por una **comunidad de programadores** donde **no hay una garantía de que siempre habrá consenso** por lo cual me expongo a los forks, pero lo más importante, **el estado no está presente en el ecosistema bitcoin.**

Y esto de verdad da para más escritura y quiero ser conciso y directo. Pero si se lo piensa, **esto tiene implicaciones que van más allá del dinero,** tiene implicaciones relacionadas con el **sistema político**. Ya que en el **sistema bancario tradicional es un sistema avalado por el estado**, y **si yo confío en el estado** (y yo no confío en el estado) eso es muy positivo, porque eso quiere decir que el estado de **mi país es honrado,** justo, **no se roba la plata,** la invierte bien en sus habitantes. Si mi estado por ejemplo es noruega, creo que no tendría que preocuparme mucho.

Pero si mi estado es **Venezuela, Colombia o Argentina,** y **cuando hay gente en el poder usando el poder del estado de forma conflictiva y de una forma no idónea para sus habitantes,** pues el sistema bancario tradicional **es algo que sufre con esas decisiones.**

No hay nada que impida al estado a través del regulador decirle al banco que tiene una licencia que depende de esa normativa, que le dé el dinero de sus reservas, porque el estado lo necesita, haciendo que algún usuario del banco pierda su dinero así sea el poseedor de esa cuenta, y pueda demostrarlo con su cédula de ciudadanía… Y esto es un riesgo que podría pasar.

Bitcoin rompe con el omnipresente estado porque es **el usuario** que tiene sus claves pública y privada, haciendo que solo él **sea quien pues, el omnipresente de sus fondos,** solo el puede

gestionar sus fondos, además de que no existen cuotas de manejo o tasas de interés… lo único que hay son pagos que se hacen a la red por enviar o recibir dinero, o fee que llaman los usuarios de bitcoin.

Entonces no se si me explique, el estado a mi me podría quitar mi cédula, pero a mi en el ecosistema bitcoin nadie me puede quitar mis llaves, a menos que sea por la fuerza.

A lo que quiero llegar es que no quiero decir que bitcoin sea mejor o peor que el sistema bancario actual, el solo una alternativa para personas que no confiamos mucho en el estado y tengamos un lugar en el cual salvaguardar nuestro dinero y que no dependa de nadie.

Bitcoin Lightning Network - LN

Conceptos básicos de Bitcoin

Entonces para resumir lo anterior leído y mencionar otras cosas que no mencioné antes, necesarias para entender este apartado de **lightning network**. Pero antes de entrar a Lightning Network, es necesario tener algunos conceptos clave para poder adentrarnos en ello.

Bitcoin fue creado por **Satoshi Nakamoto**, una figura envuelta en misterio, ya que no se sabe si es una persona o un grupo. Desde su creación, **Bitcoin** se diseñó para ser un sistema de dinero electrónico **peer-to-peer (P2P)**, es decir, una forma de transferir dinero directamente entre dos personas, sin intermediarios como **bancos o empresas financieras**. Por ejemplo, sería como consignarle algo de dinero a un amigo pero en lugar de usar una aplicación de pagos que cobre comisiones o se demore en procesar la transacción.

Cuando hablamos de Bitcoin, hay que distinguir entre dos cosas:

- **Bitcoin:** (con “B” mayúscula) es el sistema o red que hace posible todo esto.
- **bitcoin** o **BTC:** Que es la moneda digital que circula en esa red, algo similar a lo que sería el COP (peso colombiano) o el USD (dólar estadounidense), pero en versión completamente digital.

Por ejemplo, si quieres pagar un almuerzo con BTC, sería como enviar pesos colombianos o dólares directamente desde tu celular al celular del restaurante (usando nequi o la app personas de Bancolombia), pero sin que un banco o intermediario procese el pago.

Sin embargo, la red Bitcoin tiene una limitación importante: no puede manejar tantas transacciones al mismo tiempo. Es como si un mercado muy popular tuviera solo una caja registradora, lo que hace que las filas crezcan y los tiempos de espera sean largos. Esto significa que, aunque BTC sea útil, la red no puede escalar lo suficiente como para que cada habitante del planeta tierra lo use como su método principal de pago, al menos con la tecnología actual.

El escalado, en términos simples, se refiere a qué tan rápido una red puede procesar transacciones. En el caso de Bitcoin, su red solo puede manejar alrededor de 7 transacciones por segundo (tps), lo cual es bastante limitado si lo comparamos con sistemas tradicionales como VISA. Por ejemplo, un día cualquiera, VISA procesa unas 1,700 tps, y si se requiere, puede llegar a manejar hasta 65,000 tps.

Por esto, el máximo de VISA (65,000 tps) se ha convertido en el estándar con el que se mide la velocidad ideal de las criptomonedas. Bitcoin, lamentablemente, todavía está muy lejos de alcanzar ese nivel. ¿Por qué? Esto se debe principalmente a dos factores técnicos:

- **El tamaño de los bloques**, que son como “paquetes” donde se agrupan las transacciones antes de ser procesadas. En Bitcoin, estos bloques son pequeños, lo que limita cuántas transacciones caben en cada uno.
- **El tiempo por bloque**, ya que cada bloque en la red Bitcoin tarda aproximadamente 10 minutos en confirmarse, lo que ralentiza aún más el proceso.

Bitcoin es, en esencia, una cadena de bloques, también conocida como blockchain. Esta blockchain es simplemente un registro compartido de transacciones que se almacena de forma distribuida en todos los computadores conectados a la red. En otras palabras, en lugar de que un banco mantenga la lista de todas las transferencias en una base de datos que solo ellos poseen, esta lista está copiada y sincronizada entre miles de computadores y dispositivos alrededor del mundo, asegurando transparencia y evitando manipulaciones.

Las transacciones en Bitcoin se agrupan en bloques, de ahí el término “cadena de bloques” o blockchain. Cada bloque en la red Bitcoin tiene un tamaño máximo de 1 megabyte (MB). Dado que cada transacción ocupa un espacio determinado, en promedio solo caben unas 2,700 transacciones por bloque.

Este espacio limitado genera competencia entre las transacciones. Para que una transacción sea incluida en el siguiente bloque, se debe pagar una comisión. Estas comisiones son un incentivo para los **mineros** (los computadores que validan y añaden bloques a la red) den prioridad a ciertas transacciones. Es como cuando compras algo en amazon y quieres que te llegue mas rapido, entonces pagas un poco más, para que tu producto sea despachado con más prioridad que los demás.

Además, crear un bloque en Bitcoin toma aproximadamente 10 minutos. Esto significa que la red procesa unas 7 transacciones por segundo en promedio, lo cual es bastante limitado en comparación con otros sistemas de pago tradicionales.

La Lightning Network se presenta como la solución para que Bitcoin pueda usarse como un medio de pago cotidiano. Actualmente, la red principal de Bitcoin enfrenta dos grandes problemas cuando se trata de realizar pagos:

- **Tiempos de confirmación de las transacciones:** Como mencionamos antes, validar una transacción en la red Bitcoin toma, en promedio, 10 minutos. Esto es demasiado lento para pagos rápidos, como comprar un café o pagar un servicio.
- **Costos de las transacciones:** Para montos pequeños, las comisiones que se deben pagar pueden ser un porcentaje significativo del valor de la transacción. Por ejemplo, si intentas enviar el equivalente a $1 USD en BTC y la comisión es de $0.50 USD, estarías gastando el 50% del monto solo en costos de transacción, lo que hace que este sistema no sea práctico para pagos pequeños.

La Lightning Network busca solucionar estos problemas para hacer que Bitcoin sea más eficiente y accesible para el día a día.

Analogía del ábaco para entender el funcionamiento de Lightning Network

Esta analogía, tomada de Roy Sheinfield, compara el funcionamiento de LN con un ábaco. Para quienes no estén familiarizados con el ábaco, es una herramienta utilizada para cálculos que tiene

líneas (o ejes), normalmente hechas de madera, con bolitas o cuentas que se pueden mover de un lado a otro.

En LN, los usuarios necesitan crear conexiones entre dos participantes o **nodos de la red**. Estas conexiones se llaman “canales de pago” o *payment channels*. Si hacemos la analogía con el ábaco, estos canales son como las líneas o ejes, y las bolitas representan los bitcoins que pueden moverse entre las dos personas que abrieron el canal.

Características comunes entre un ábaco y la Lightning Network

- **Son bidireccionales**: Las bolitas en el ábaco se pueden mover hacia la izquierda o hacia la derecha, y lo mismo sucede con los fondos en un canal de pago. Por ejemplo, si un amigo y tú abren un canal para pagar el almuerzo, el dinero puede ir de ti a él o viceversa, dependiendo de quién pague en cada transacción.
- **Son fijos**: La cantidad de bolitas en una línea del ábaco no cambia; simplemente se mueven de un lado a otro. Lo mismo ocurre en un canal de pago de la Lightning Network: la cantidad total de bitcoins que ambos deciden poner en el canal al inicio se mantiene fija. Si quieren agregar más bitcoins, deben cerrar el canal actual y abrir uno nuevo con una cantidad diferente.
- **Propiedad definida**: Cada bolita en el ábaco pertenece a uno de los lados: o es tuya, o de la otra persona. En la Lightning Network, lo mismo sucede con los bitcoins en el canal de pago. Cada bitcoin tiene un dueño claro, y no hay bitcoins “flotando” sin asignar.

Resumiendo el funcionamiento de la Lightning Network

Es una solución creada para que las transacciones de Bitcoin sean más rápidas y económicas. En lugar de procesar todas las transacciones directamente en la blockchain de Bitcoin (que es más lenta y costosa), la Lightning Network opera como una **segunda capa**. En esta capa, las transacciones entre usuarios se realizan de forma rápida y sin necesidad de registrar cada una en la blockchain principal.

Ejemplo práctico para entender

Imagina que tú y tu amigo Pedro acuerdan abrir un canal de pago en la Lightning Network para compartir gastos en un viaje. Los dos deciden “poner” un total de 0.1 BTC en el canal (como poner bolitas en la línea del ábaco).

- Al inicio, tú tienes 0.05 BTC y Pedro tiene 0.05 BTC.
- Durante el viaje, tú pagas el almuerzo, así que 0.01 BTC se mueve de tus “bolitas” a las de Pedro. Ahora tú tienes 0.04 BTC y Pedro tiene 0.06 BTC.
- Más tarde, Pedro paga la gasolina y te transfiere 0.02 BTC en el canal. Ahora tú tienes 0.06 BTC y Pedro tiene 0.04 BTC.

Todo esto ocurre sin registrar cada transacción en la blockchain principal, lo que hace el proceso rápido y barato. Solo cuando ambos deciden cerrar el canal, se registra el saldo final en la blockchain.

¿Cómo funciona Lightning Network?

A diferencia de otras redes de **capa 2** para criptomonedas, **Lightning Network** no es una cadena de bloques en sí, sino una red de **canales de pago interconectados** que se crean entre dos partes en la red de Bitcoin. Esta definición puede sonar un poco técnica, así que vamos a desglosarla con un ejemplo sencillo.

Imagina que tienes una cuenta con el dueño de la tienda de tu barrio. Vas regularmente a comprar, pero en lugar de pagar cada vez que compras, tú y el dueño de la tienda acuerdan que solo pagues al final del mes por todas las compras realizadas. El dueño lleva un registro de cuánto le debes por las compras, y también puede restar las veces que te ha dado un descuento o algo gratis, como parte de tu trato. Al final del mes, ambos revisan el total y tú pagas.

Este sistema de pagos a crédito con un “registro” de lo que debes es muy similar al funcionamiento de los **canales de pago en Lightning Network**. Ahora, imagina que tú y el dueño de la tienda deciden usar **Lightning Network** para liquidar la cuenta mensual, y para hacerlo deben crear un **canal de pago** en la red de Bitcoin.

¿Qué es una wallet multifirma?

Para crear este canal de pago, necesitarán usar un **monedero o wallet multifirma**. Un monedero multifirma es un tipo especial de monedero en el que se necesita la firma de más de una persona para autorizar una transacción. En este caso, tanto tú como el dueño de la tienda son “firmantes” del monedero.

Primero, ambos depositan una cantidad de **BTC** en el monedero multifirma, cantidad que debe ser igual o superior para cubrir el total de las transacciones que esperan realizar durante el mes. Esta cantidad de BTC en el monedero es lo que se utiliza para el intercambio de pagos entre ustedes.

Cómo funciona el canal de pago

Una vez que el canal de pago está creado, las transacciones entre tú y el dueño de la tienda no requieren ser registradas en la blockchain de Bitcoin de inmediato. En lugar de eso, se actualiza un **registro digital** que refleja cuánto de esa cantidad de BTC le corresponde a cada uno. Es como un **recibo digital** que se actualiza cada vez que haces una compra. Esto te permite realizar transacciones rápidas y con comisiones casi nulas.

Imagina que compras algo en la tienda, pero en lugar de hacer una transacción en la blockchain cada vez que compras, lo que haces es actualizar ese recibo. La única limitación es el hardware de tu ordenador y la velocidad de internet. Esto hace que las transacciones en Lightning Network sean rápidas, casi instantáneas, y que puedan manejar miles de transacciones por segundo.

Cierre del canal de pago

Al final del mes, cuando ambos deciden liquidar la cuenta, se realiza una **transacción final** en la

blockchain de Bitcoin. En ese momento, el BTC de la wallet multifirma se distribuye entre las direcciones de los monederos de cada uno de ustedes, de acuerdo con el saldo final registrado en los recibos digitales. Entonces, es esta transacción final la que se registra en la blockchain y finalmente, cierra el canal.

Es importante saber que un **canal de pago** puede permanecer abierto indefinidamente y puede cerrarse en cualquier momento por decisión de una o ambas partes.

Ahora, imagina que, por alguna razón, no pagas todo lo que debías en la tienda. En este caso, el BTC que inicialmente depositaste en el monedero multifirma será enviado automáticamente al dueño de la tienda, asegurando que reciba el dinero que le corresponde. Por otro lado, si el dueño de la tienda intenta cobrarte de más, ocurrirá lo contrario: el sistema garantizará que tú recibas la cantidad correcta de BTC según los registros del canal de pago.

Este tipo de disputas es poco probable cuando existe confianza entre ambas partes. Sin embargo, en transacciones con personas que no conoces o que te generan desconfianza, esta confianza no siempre está garantizada. Por eso, ambas partes deben **prefinanciar el monedero multifirma con una garantía inicial**. Esto sirve como un incentivo para comportarse de manera honesta y evitar abusos.

Esto nos lleva a la parte clave de la **interconexión de los canales de pago**, lo que convierte a **Lightning Network** en una red global, no solo una conexión de dos direcciones entre dos personas. Así es cómo funciona:

Imagina que hay otro cliente habitual de la tienda, llamémoslo **Juan**. Juan tiene un canal de pago abierto con el dueño de la tienda, pero además, Juan tiene otro canal de pago abierto con el peluquero del barrio.

Entonces, si tú quieres pagar al peluquero en BTC pero no tienes un canal de pago directo con él, puedes utilizar los canales que se conectan a través del dueño de la tienda. El dueño de la tienda tiene un canal de pago con Juan, y Juan, a su vez, tiene un canal con el peluquero. Gracias a esto, **Lightning Network** puede redirigir tu pago a través de estos canales conectados, haciendo que el pago llegue al peluquero sin que tú tengas un canal directo con él.

Ahora bien, imagina que te haces amigo de Juan y abres un canal de pago con él. La próxima vez que vayas al peluquero y quieras pagarle en BTC, **Lightning Network** dirigirá automáticamente el pago a través del canal que tienes con Juan, evitando el recorrido que hacía antes con el canal del dueño de la tienda; porque: al igual que los rayos encuentran el camino de menor resistencia en la atmósfera para tocar la tierra, Lighting Network busca el camino más eficiente, minimizando la distancia que debe recorrer el pago.

Seguridad en los pagos con canales intermediarios

Puede que te preocupe que Juan, que quizás no conoces bien o no confías completamente, pueda robar el pago mientras se dirige al peluquero. Pero **Lightning Network** tiene una solución para esto: los pagos de BTC que se realizan a través de canales intermediarios están protegidos por una tecnología llamada **Hash Time-Locked Contracts (HTLC)**.

En términos simples, un **HTLC** es como un acuerdo digital en el que se intercambia un **código secreto** entre las partes antes de que se envíe cualquier BTC. Este código actúa como una garantía

de que el pago se llevará a cabo solo si el destinatario final lo confirma. Si algo va mal en el proceso, como que uno de los nodos (computadoras) involucrados queda fuera de línea, la transacción se cancela automáticamente y se “castiga” a la parte que haya intentado hacer algo malintencionado.

Cuantos más canales de pago haya conectados entre sí, la red **Lightning Network** se vuelve más rápida y tiene mayor alcance. Esta conectividad global significa que es posible que en el futuro todo los habitantes del planeta puedan usar **BTC** como dinero digital, tal como lo imaginó **Satoshi**.

Versiones personalizadas de Lightning Network

Para facilitar el uso de Lightning Network, se ha diseñado de manera que sea posible crear versiones personalizadas. Esto significa que cualquier persona o empresa puede crear su propia **versión the Lightning Network**. Para garantizar que todas estas versiones sean compatibles, se usa un protocolo llamado **BOLT (Basis of Lightning Technology)**. Gracias a BOLT, todas las versiones de Lightning Network son **interoperables**, lo que permite que diferentes implementaciones de la red trabajen juntas sin problemas.

Además, **Lightning Network** no está limitado solo a Bitcoin; puede utilizarse con cualquier criptomoneda que soporte **monederos multifirma** y **HTLC**, lo cual es común en la mayoría de las criptomonedas. Esto abre la puerta a una interoperabilidad entre cadenas de bloques, lo que significa que puedes realizar transacciones instantáneas y de bajo costo entre criptomonedas sin necesidad de pasar por un **exchange** tradicional.

Faltan muchos conceptos que analizar y términos que descubrir. Pero a medida que nos vayamos adentrando en el mundo de LN, descubriremos más beneficios de la tecnología.

Crecimiento explosivo de Lightning Network

Con todas estas características increíbles, no es sorprendente que **Lightning Network** haya crecido exponencialmente en el último año. En 2021, se registraron alrededor de **60,000 canales de pago** de Lightning Network en todo el mundo, con más de **100 millones de dólares** en BTC bloqueados en los monederos multifirma asociados.

Como hemos leído hasta ahora, **Bitcoin** nos da la posibilidad de tener un mundo nuevo en cuanto al manejo del dinero, porque evita un **ente regulador**, nos da la posibilidad de **tener anonimato**, nos protege de la **inflación**, que es otro tema importante pero no lo abordaremos ahora y finalmente, para el apartado que vamos a tocar en este momento; nos da la posibilidad de participar en la red de forma anónima y sin restricciones.

Una de las premisas de Bitcoin es que es una **red descentralizada** a diferencia por ejemplo de una **red centralizada**.

Te preguntaras un poco que esto de red centralizada y descentralizada y lo voy a explicar en un segundo:

Red centralizada

En una red centralizada, todo el control y procesamiento pasan por un único punto central, llamado **nodo central** o **servidor central**. Este servidor actúa como el corazón del sistema, gestionando todas las conexiones y decisiones.

- **Punto único de control**Todas las decisiones, datos y operaciones dependen de un único nodo o entidad.
- **Alta eficiencia inicial**Como todas las decisiones pasan por el nodo central, las operaciones suelen ser rápidas y directas.
- **Mayor vulnerabilidad**Si el servidor central falla o es atacado, toda la red se detiene o se compromete.

Por ejemplo:

- **Bancos tradicionales:** Cuando haces una transferencia bancaria, el banco (servidor central) gestiona y valida la operación.
- **Redes sociales como Facebook:** Los servidores de la empresa almacenan todos los datos y controlan cómo funciona la plataforma.

Red descentralizada

En una red descentralizada, **no existe un punto central de control**. En su lugar, **hay múltiples nodos** (computadoras) que participan de manera independiente pero colaborativa, compartiendo datos y responsabilidades.

- **Sin punto único de fallo:** Si un nodo se desconecta o falla, la red sigue funcionando, ya que otros nodos pueden asumir el trabajo.
- **Mayor seguridad:** Es más difícil atacar o comprometer toda la red, ya que los datos y el control están distribuidos.
- **Escalabilidad compleja:** Aunque es robusta, coordinar muchos nodos puede ser más lento o complejo en comparación con una red centralizada.

Por ejemplo:

- **Bitcoin y blockchain:** La validación de transacciones no depende de un solo servidor, sino de miles de nodos distribuidos por todo el mundo.
- **Protocolos P2P (Peer-to-Peer) como BitTorrent:** Los archivos se comparten directamente entre usuarios sin necesidad de un servidor central.

Normalmente las redes sociales que usamos en el día a día: **facebook, youtube, instagram, twitter,** etc... Son redes centralizadas que censuran a sus usuarios y sus contenidos por ser sexistas, racistas o atacar a una población y esto está bien, porque lo que se está tratando de hacer es evitar el bullying o el abuso entre usuarios, todo esto por poner ejemplos. También puede pasar lo contrario, que un estado o nación prohíba el uso de ciertos contenidos o redes sociales (como pasa en venezuela en este 2024 con la prohibición del uso de whatsapp y Twitter por parte del presidente Nicolas Maduro)

Es aquí cuando llega **Nostr** la cual puede ser una opción para librarnos de un estado que nos impide acceso libre al internet, o por el contrario, nos censura por una hecho que queremos denunciar, darle

visibilidad y que puede ser contraproducente y no beneficia al estado ni a la nación.

Wallets más a fondo, LNURL y Lightning Address

Si todo lo tenemos claro hasta ahora, es necesario tener un canal abierto con alguien en la red de Lightning, ahora. Hoy en día para poder usar la red Lightning no es necesario tener un canal abierto porque las wallets disponibles en Android y Iphone se encargan de la apertura y cierre de los canales por nosotros, a cambio de una pequeña comisión fuera de los fees que se hacen en la red Lightning.

¿Qué es un nodo en Lightning Network?

Un nodo de **Lightning Network** es un software que gestiona los canales de pago, conecta con otros nodos y permite enrutar pagos. En términos simples, es como una pequeña "oficina bancaria" que:

- Abre y cierra canales de pago en la blockchain de Bitcoin.
- Mantiene registros de los balances entre los participantes.
- Facilita transacciones rápidas dentro de la red LN.

Mencionábamos antes que operar nuestro propio nodo nos da independencia total, pero puede ser complicado mantenerlo porque requiere conocimientos técnicos y recursos (configurar hardware, mantener conexiones, sincronizar con la blockchain, etc.).

Es entonces aquí cuando nos detenemos un poco y vamos a entrar a hablar de las **wallets con custodia (custodial)** y **sin custodia (Non-custodial)**

Wallets sin custodia (Non-custodial)

- **Tú controlas tus claves privadas.** Esto significa que eres el único responsable de tus fondos.
- Si pierdes tus claves privadas (o la frase de recuperación), nadie podrá ayudarte a recuperar tus bitcoins.
- Las transacciones las gestionas directamente en la red de Bitcoin o Lightning Network.
- Se considera la opción más segura desde una perspectiva de soberanía financiera.

Ventajas:

- Mayor seguridad y control sobre tus fondos.
- No dependes de terceros para mantener tus bitcoins.

Desventajas:

- Requiere mayor conocimiento técnico.
- La seguridad de los fondos depende completamente de ti.

Wallets con custodia (custodial)

- **Un tercero controla tus claves privadas.** Esto significa que delegas la seguridad y la gestión de tus fondos a la empresa o servicio que ofrece la wallet.
- Son más fáciles de usar porque la empresa gestiona todo, desde el acceso a las transacciones

hasta el almacenamiento.
- Sin embargo, si el servicio es hackeado o decide bloquear tus fondos, podrías perder acceso a ellos.

Ventajas:

- Fáciles de usar, ideales para principiantes.
- Soporte técnico en caso de problemas.

Desventajas:

- Dependencia de un tercero (menos soberanía).
- Mayor riesgo de hackeos o mal manejo por parte del proveedor.

Hemos entendido hasta ahora que existe la capa de red principal llamada cadena de bloques o blockchain y luego esta la capa dos o Lightning Network, hay billeteras con custodia y sin custodia que nos permite operar en ambas redes.

Lista de wallets sin custodia (Non-custodial)

Bitcoin + Lightning Network:

- **Phoenix:** Fácil de usar, sin custodia, gestiona canales automáticamente.
- **Breez:** Wallet Lightning sin custodia, con enfoque en simplicidad y comercio.
- **Muun:** Compatible con Bitcoin y Lightning, sin custodia, excelente para principiantes.
- **BlueWallet** (Modo sin custodia): Ofrece la opción de usar Lightning sin custodia si configuras tu propio nodo.
- **Zeus:** Diseñada para usuarios avanzados con su propio nodo Lightning.

Solo Bitcoin (On-chain), red principal

- **Electrum:** Wallet veterana, sin custodia, muy completa para usuarios avanzados.
- **Sparrow Wallet:** Sin custodia, ideal para transacciones seguras.
- **Wasabi:** Wallet sin custodia con enfoque en privacidad.
- **Samourai:** Centrada en privacidad, sin custodia, diseñada para transacciones seguras.

Lista de wallets con custodia (Custodial)

Bitcoin + Lightning Network:

- **BlueWallet (Modo custodial):** Si decides no gestionar tu nodo, Lightning funciona con un nodo externo de la empresa.
- **Wallet of Satoshi:** Súper sencilla, pero completamente custodial.
- **Strike:** Famosa por permitir pagos con BTC y fiat, pero depende de su infraestructura.
- **Zebedee:** Popular en juegos y micropagos, pero es custodial.

Solo Bitcoin (On-chain), red principal

- **Coinbase Wallet:** Aunque es una wallet de una exchange, tiene un diseño custodial.
- **Binance Wallet:** Similar a Coinbase, ofrece custodialidad con servicios adicionales.

- **Crypto.com Wallet:** Custodia tus BTC con servicios de staking y trading.

¿Cómo decidir cuál usar?

Todo depende del nivel de soberanía e independencia que quieras tener. Si eres principiante, si no te preocupa que un tercero maneje tus llaves y buscas mas comodidad por encima de control entonces **deberías usar una Wallet con custodia**. Si por el contrario lo que quieres es soberanía sobre tus fondos y entiendes como proteger tus claves entonces **usa una billetera sin custodia.**

¿Qué es una Lightning Address ?

Una **Lightning Address** es una forma simple y amigable de recibir pagos en la red Lightning. Esta tiene el formato de un correo electrónico, por ejemplo **alberguegolondras@dominio.com.**

Tener una Lightning Address es **muy útil para las personas que nos gustar crear contenido**. Porque convierte todas las piezas que producimos en internet, en una **bandeja de entrada de Bitcoin**. Con una Lightning Address será fácil para nuestra audiencia hacernos llegar el bitcoin que le he puesto a escuchar, leer o ver en un medio digital. Y esto puede ser para cualquier valor, desde 10 pesos hasta 10 millones.

Ademas, con la herramienta adecuada, no solo podremos recibir pagos en bitcoin sino que también **podremos leer los comentarios adjuntos que estos traen**, creando realmente **lazos auténticos** entre nuestros video/audio espectadores y nuestro contenido. Nuestro **trabajo solo es hacer visible esta dirección**, ya sea en cada subida que hacemos a una red social, en nuestro sitio web, en un video que subimos a youtube, la imaginación aquí se hace grande. Mas adelante aprenderemos a obtener una.

En general una **Lightning Address** facilitara a otras personas enviarnos fondos sin lidiar con las transacciones Lightning que hemos descrito atrás.

¿Para qué se usa una Lightning Address ?

- **Pagos instantáneos:** Recibir dinero de forma rápida y con bajas comisiones.
- **Donaciones:** Ideal para creadores de contenido, tiendas online, o proyectos abiertos a aportes.
- **Usabilidad:** Hace que la experiencia de usuario sea más intuitiva, especialmente para personas no técnicas.

¿Qué es LNURL?

LNURL es un protocolo que facilita las interacciones entre los usuarios y la red Lightning. Permite simplificar varias funciones relacionadas con pagos y retiros. En esencia, LNURL mejora la experiencia del usuario eliminando pasos técnicos.

Funciones principales de LNURL:

LNURL-Pay: Permite que las personas envíen pagos sin necesidad de una factura (invoice) específica. Esto es la base para Lightning Addresses.

LNURL-Withdraw: Facilita que retires fondos de plataformas o servicios de manera automática con un solo clic.

LNURL-Auth: Sirve para autenticarse en aplicaciones o servicios usando tu monedero Lightning, sin necesidad de contraseñas.

LNURL y **Lightning Address** trabajan en conjunto para hacer que el uso de la red Lightning sea más accesible, rápida y cómoda tanto para pagos como para interacciones en la web.

Nostr - Publicaciones descentralizadas para la web

Nostr web

¿Qué es Nostr?

Nostr significa **Notas y otras cosas transmitidas por relés**. Al igual que HTTP o TCP-IP, Nostr *es un protocolo*; un estándar abierto sobre el cual cualquiera puede construir. Nostr en sí no es una aplicación o servicio en el cual nos registremos.

Nostr es un protocolo abierto y descentralizado lo que significa que **no está controlado por una sola entidad**. Nos empodera y nos da el control de nuestros propios datos lo que permite que nosotros mismos seamos nuestros propios curadores del contenido que subimos y mostramos.

En este **protocolo no existe la censura**, esto es positivo y negativo al mismo tiempo porque se permite el posteo de contenido obsceno y oscuro. Pero también tiene la flexibilidad de ser un medio tecnológico que nos permite **denunciar abusos y opresiones que las empresas centralizadas dueña de los medios comunes o el mismo estado no quiere que se difundan**. Además de ello, por ser un protocolo descentralizado, no necesitamos proporcionar nuestros datos personales para registrarnos y empezar a participar en la red. En cambio, podemos registrarnos con un seudónimo si queremos para mantener la privacidad y el anonimato.

¿Por qué necesitamos Nostr ?

¿Es necesario otro protocolo para publicar en internet? La respuesta es sí, porque la forma en que publicamos y compartimos información en la web está **manipulada y corrompida**. Lo que comenzó como un espacio libre y abierto, por allá hace varias décadas ya donde cualquiera podía crear y compartir contenido en sus blogs, ha sido **acaparado** por unas pocas corporaciones gigantes.

Como mencionaba antes en este texto, **estas empresas** no sólo deciden qué vemos y leemos, sino que también **logran manipular estos medios** para lograr dar difusión a solo las ideas o fines que ellos quieren. A través de la **actividad que realizamos en sus redes sociales**, los likes que damos, los comentarios que escribimos; en general toda la actividad que realizamos es **analizada por la IA que le ayuda a crear un perfil de nosotros**, que luego facilita a las empresas a

redireccionar campañas publicitarias, crear propaganda de manipulación y engaño para implantar miedo, difundir noticias falsas o implantar modas o comportamientos no adecuados para la salud y la convivencia con las personas.

Sus algoritmos, diseñados **para maximizar nuestro tiempo de conexión**, han tenido consecuencias devastadoras para nuestra sociedad: polarización, manipulación y la pérdida de autonomía sobre lo que consumimos en línea.

Es necesario que el cambio empiece ahora. Necesitamos recuperar esa esencia original de internet, donde las personas tengan el control, no las empresas. **Un lugar donde podamos decidir cómo interactuar con la información y construir comunidades auténticas**, libres de la influencia de intereses corporativos.

Nostr es una herramienta que permite que esto sea posible. Con su enfoque en la descentralización, nos da una oportunidad única para **reinventar la forma en que compartimos ideas y conectamos con otros en la web**. Es el momento de crear un internet que realmente funcione para todos.

¿Qué son los Zaps?

Qué son los Zaps, cómo funcionan, y qué necesita para usarlos en su cliente Nostr.

Los conceptos básicos

Para entender que son los **Zaps**, pensémoslos simplemente como **propinas**. Propinas que se transmiten a través de la Red Lightning a la velocidad del rayo, con prácticamente ninguna tarifa de transacción.

Desde que comenzó a usarse el protocolo Nostr, era habitual encontrarse con facturas de Lightning en las publicaciones. Sin embargo, con la llegada de NIP-57, apareció una forma mucho más práctica y directa de enviar valor: los Zaps. Ahora, **los Zaps se han convertido en la manera favorita de transmitir valor entre los usuarios de Nostr**. Vamos a explorar de manera sencilla qué trajo NIP-57 y cómo funcionan estos famosos Zaps.

NIP-57

El **NIP-57** es la guía que define cómo implementar los Zaps en el ecosistema Nostr. Este estándar introduce dos nuevos tipos de notas:

- **Tipo 9735:** Representa un Zap, o sea, un pago realizado.
- **Tipo 9734:** Es una solicitud de Zap, utilizada para pedir una factura de pago.

Gracias a estos dos tipos de notas, los clientes de Nostr pueden interactuar con servidores **LNURL** para generar y procesar facturas Lightning. Además, el NIP-57 especifica que las billeteras Lightning que reciben pagos mediante Zaps deben enviar notas correspondientes a los relés, asegurando la comunicación y transparencia dentro de la red.

¿Cómo funcionan los Zaps ?

Aquí no entraremos en detalles técnicos profundos, pero vamos a desglosar los conceptos básicos de cómo operan los Zaps.

1. **Inicia el proceso:** Cuando haces clic o tocas el ícono ⚡ en tu cliente favorito **(como Damus, Iris o Amethyst)**, tu cliente se conecta al servidor LNURL que gestiona la billetera Lightning del usuario que quieres zapear. Básicamente, el cliente dice: *"Hola, quiero enviarle algunos sats a unloquer."*

2. **Respuesta del servidor LNURL:** El servidor **verifica si la billetera de unloquer admite Zaps.** Si es compatible, confirma su clave pública y le dice al cliente que puede proceder.

3. **Creación de una solicitud de Zap:** El cliente genera una solicitud (una nota tipo 9734) que incluye:

- Información sobre el perfil o la publicación que deseas zapear.
- El monto en sats.
- Los relés donde se debe enviar la nota.
- Otros detalles técnicos necesarios. Esto es, en esencia, una petición de factura al servidor LNURL.

4. **Generación de la factura:** El servidor responde con la factura Lightning que el cliente necesita para completar el pago.

5. **Pago del usuario:** El cliente entrega la factura a tu billetera Lightning, como Alby (en el navegador) o cualquier otra, y procede al pago. Si tienes un presupuesto configurado, el proceso es casi instantáneo.

6. **Notificación del receptor:** Una vez que el pago se completa, la billetera del receptor (en este caso, unloquer) crea una nota tipo 9735. Esta nota se envía a los relés especificados en la solicitud de Zap.

7. **Visualización del Zap:** Los relés que reciben esta nota notifican a los clientes conectados, quienes mostrarán el Zap en sus interfaces. Así, tanto tú como unloquer pueden ver el resultado del pago.

Todo esto ocurre en cuestión de segundos y cuesta apenas una fracción de un centavo.

CLick para un esquema

¿Cómo envío y recibo Zaps?

Para Zapear a otras personas en Nostr, solo es necesario tener dos cosas:

1. Una billetera lightning compatible con Zap (como **Wallet of Satoshi, Muun, Zap, Zeus, Breez o alby**: esta última es una extensión en el navegador)

2. Un cliente que haya implementado Zaps (como **Damus, Amethyst, Iris o Snort**)

Para recibir Zaps en Nostr, solo necesitas asegurarte de que tu dirección Lightning esté configurada

correctamente en tu perfil. Esta dirección será el destino de los sats que otros usuarios te envíen.

Sin embargo, es importante saber que puedes pagar Zaps desde una billetera o dirección Lightning diferente a la que usas para recibirlos. Aquí tienes un ejemplo práctico:

1. Configuras en tu perfil de Nostr una dirección Lightning de Stacker News para recibir todos los Zaps.

2. En tu navegador, utilizas Iris como cliente y realizas pagos de Zaps desde la billetera Alby, usando su extensión para Chrome.

3. En tu móvil, usas Damus como cliente y pagas los Zaps con la aplicación Wallet of Satoshi.

El protocolo Nostr

El protocolo Nostr es una tecnología que permite a los usuarios compartir información y comunicarse sin depender de plataformas centralizadas. Explicare aquí de forma general sus componentes y como funciona.

¿Cómo funciona Nostr?

Nostr se basa en dos componentes principales: clientes y relés:

- **Clientes:** Son las herramientas que usas para enviar y recibir información, como una aplicación en tu teléfono o computadora. Por ejemplo, si piensas en una red social como Twitter, el cliente sería la aplicación que te permite leer y publicar tweets.
- **Relés:** Son como bases de datos donde se guarda toda la información. También permiten que los clientes envíen y obtengan datos.

Cada usuario tiene una **llave pública** que funciona como su identidad única. Cuando haces algo en la red, como enviar un mensaje o actualizar tu perfil, ese contenido (llamado evento) se firma digitalmente para asegurar que realmente fue hecho por ti. Los clientes verifican estas firmas para garantizar su autenticidad.

¿Cómo se conecta todo?

Los clientes y los relés no necesitan estar conectados entre sí todo el tiempo. Como usuario, decidimos a cuáles relés queremos conectarnos. Esto significa que tenemos el control sobre dónde se guardan y de dónde se obtienen los datos. Por ejemplo:

- Si queremos actualizar el perfil, el cliente que estemos usando envía un evento especial (tipo 0) a los relés que elijamos, y ellos lo guardan.
- Cuando abrimos un cliente, este consulta los relés que seleccionamos para mostrarnos la información más reciente.

Los eventos en Nostr pueden contener diferentes tipos de información, desde mensajes hasta listas de contactos o actualizaciones de perfil. Para que todo funcione de manera ordenada, existen

estándares llamados NIPs (Posibilidades de Implementación de Nostr, Nostr Implementation Possibilities), que definen cómo deben manejarse estos eventos. Esto asegura que todos los clientes y relés trabajen de manera compatible.

Diagrama de la red de Nostr

En el diagrama vemos tres relés (las bases de datos) y tres usuarios, cada uno usando una aplicación diferente para conectarse a la red Nostr. **Bob** usa damus en Iphone. **Alice** usa Amethyst en Android y finalmente **Mary** usa Iris que es un cliente en un navegador web como crhome o safari o firefox.

De acuerdo con lo que se ve en las flechas de lectura y escritura en la imagen podemos decir lo siguiente:

- **Bob** puede leer todos los mensajes de **Alice**, pero no sabe nada sobre **Mary**, ya que no está conectado a los relés que ella usa.
- **Alice** puede leer todos los mensajes de **Bob**, pero notiene acceso a lo que publica **Mary**.
- **Mary**, en cambio, puede leer los mensajes de **Bob** y **Alice** porque, aunque escribe en el Relé 3, también lee desde el Relé 2, donde **Bob y Alice** guardan sus mensajes.

Aunque esta es una situación sencilla, muestra algo importante: el relay al que decidamos conectarnos influye directamente en las personas y mensajes que podemos ver.

Eventos en Nostr

En la red Nostr, todo gira en torno a los **eventos**, que son el único tipo de objeto que existe. Cada evento tiene un **tipo**, que define qué acción representa o qué clase de mensaje puede enviarse o recibirse.

Por ejemplo, un evento de **tipo 1** corresponde a una nota de texto breve, algo similar a un tweet en Twitter. Este tipo de evento es ideal para compartir mensajes cortos con otros usuarios. Mas información sobre los eventos aquí

```
  "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":
```

```
"908a15e46fb4d8675bab026fc230a0e3542bfade63da02d542fb78b2a8513fcd0092619a2c8
c1221e581946e0191f2af505dfdf8657a414dbca329186f009262"
```

¿Qué son los clientes de Nostr?

Un **cliente** en Nostr es simplemente la aplicación que se usa para conectarse e interactuar con la red. Es como la app de Twitter que se utiliza para publicar y leer tweets, pero en este caso, sirve para acceder al protocolo Nostr.

¿Cómo funcionan los clientes?

Dado que Nostr es muy flexible y sencillo, los clientes pueden enfocarse en distintas características. Por ejemplo:

- Algunos priorizan una interfaz fácil y atractiva.
- Otros se especializan en habilitar pagos con Bitcoin a través de Lightning Network.
- También hay clientes diseñados para usos creativos, como jugar ajedrez directamente en Nostr.

La mayoría de los clientes actuales están pensados para redes sociales, pero cada vez surgen opciones más variadas y sorprendentes.

Ejemplos de clientes en Nostr

- Jester: Para jugar ajedrez en Nostr.
- Habla: Publicación de contenido en formato largo, como Medium.
- Nostrgram: Un cliente especializado en contenido multimedia.

¿Es posible usar más de un cliente?

Sí, se puede cambiar de cliente o usar varios a la vez. Mientras todos los clientes consulten los mismos relés (las bases de datos de Nostr), se tendrá acceso a los mismos mensajes y datos, sin importar qué aplicación utilices. Y destacando además, que **la clave privada servirá para ingresar a todas las aplicaciones**

Sobre tu clave privada

Tu clave privada es tu identidad en Nostr. Es lo que te permite acceder a tu cuenta, tus mensajes y tu lista de seguidores. Sin embargo, es importante protegerla bien:

- **Evita ingresar tu clave privada en cualquier cliente**, si es posible. Aunque muchos clientes se esfuerzan por proteger tus datos, siempre existe el riesgo de fallas de seguridad o errores que puedan comprometerla.
- Si tu clave privada se ve expuesta, perderás acceso a tu cuenta y todos tus datos asociados. Tendrías que empezar desde cero reconstruyendo tu identidad y tu lista de seguidores.

Algunos clientes

Web

- Iris – Recomendamos este para nuevos usuarios
- Snort
- Coracle
- nostrudel
- primal

PC

- Gossip: es un cliente de escritorio diseñado para usuarios que tienen un poco más de experiencia técnica. Aunque su uso puede requerir algo más de conocimiento, la ventaja es que ofrece un mayor control sobre cómo se interactúa con la red Nostr.

iOS

- Damus– Este es el primer y más exitoso cliente de Nostr para iOS hasta ahora.
- Nos
- Nostur
- primal

Android

- Amethyst – Un excelente cliente para Android
- primal
- Fountain

¿Qué son los Relés en Nostr?

Los relés (o Relays en Inglés) son una parte esencial de la red Nostr. Funcionan como servidores que permiten a los clientes enviarles mensajes. Estos mensajes pueden ser almacenados y compartidos con otros clientes conectados al mismo relé, dependiendo de cómo esté configurado.

Importancia de los relés

Actualmente, muchos relés son gratuitos, pero operar un relé implica costos de computación, almacenamiento y ancho de banda. Por esta razón, se espera que los relés de pago se vuelvan más comunes en el futuro.

Una cualidad importante a la hora de utilizar relés de pago es que suelen tener una mejor calidad de contenido y de usuarios. La *prueba de trabajo* de pagar por el acceso al rele actúa como un filtro que reduce a evitar las cuentas spam.

Lista de todos los réles

¿Qué sucede si los relés dejan de funcionar?

Si todos los relés utilizados dejan de operar, las publicaciones realizadas a través de ellos serán irrecuperables. Para mitigar este riesgo, se recomienda conectarse a varios relés. También es posible operar un relé personal para asegurar que las publicaciones y datos estén siempre disponibles.

¿Es recomendable ejecutar un relé propio?

Para la mayoría, no es necesario. Sin embargo, para quienes tienen conocimientos técnicos y buscan máxima resistencia a la censura o desean un relé privado para un grupo reducido, puede ser una buena opción. Operar un relé personal asegura que todas las publicaciones y datos permanezcan accesibles.

Para quienes deseen configurar su propio relé, existe una guía detallada escrita por Andre Neves que explica el proceso paso a paso.

- Implementaciones de Relés
- Proyectos Nostr

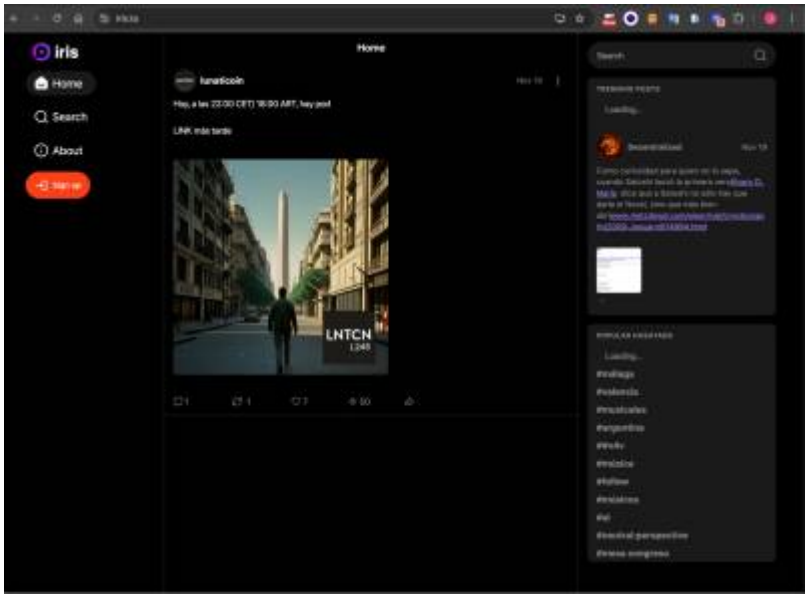
Guía como empezar en Nostr

Cómo crear una cuenta

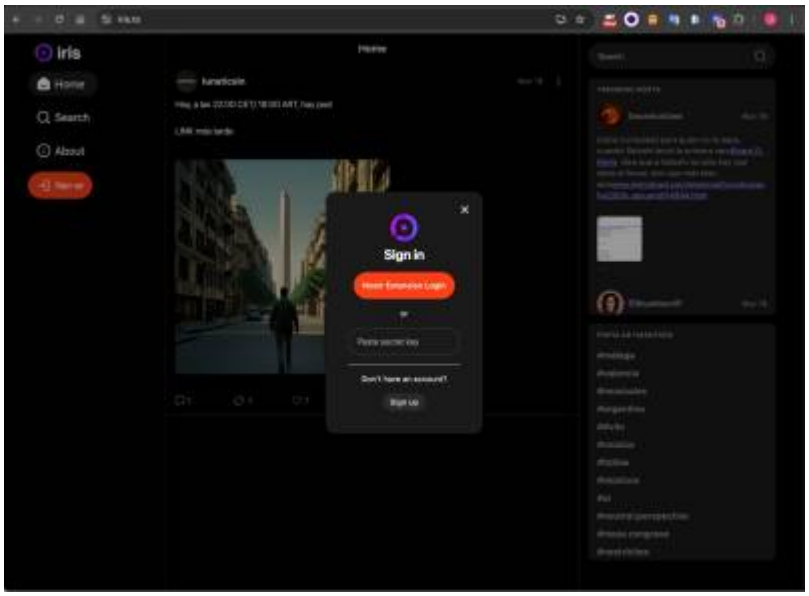
Realmente podemos utilizar cualquier cliente para poder obtener las claves pública/privada necesarias para poder utilizar los diferentes clientes que hay disponibles hasta el momento.

Para esta vez, utilizaremos Iris para crearnos una cuenta. Entonces lo primero será ir a la página.

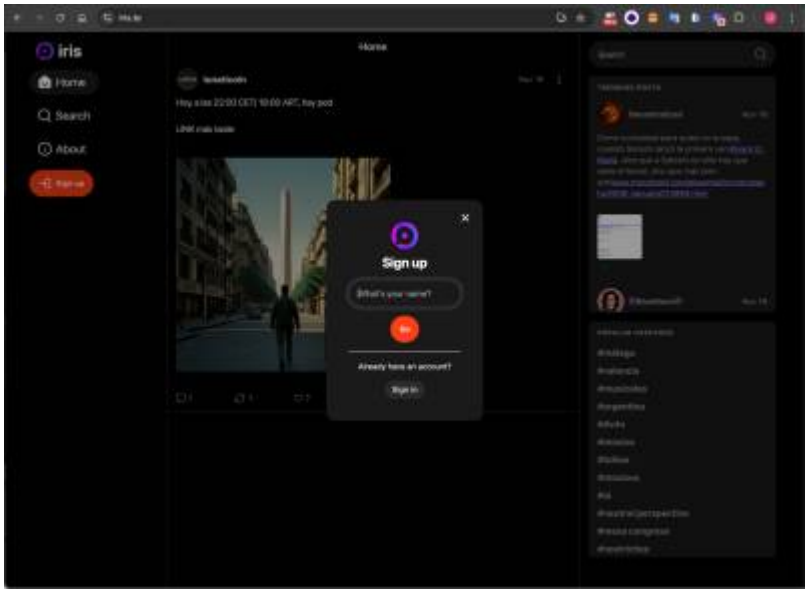
La primera vez que entramos al sitio, veremos una vista similar a la siguiente imagen, entonces hacemos click en el botón rojo que dice **Sign Up**



Después de hacer click, sale una ventana nueva sobre el feet, el cual nos pregunta si tenemos una cuenta “**Don’t have an account**”. Como vamos a crear una cuenta nueva, entonces hacemos click en ese texto.

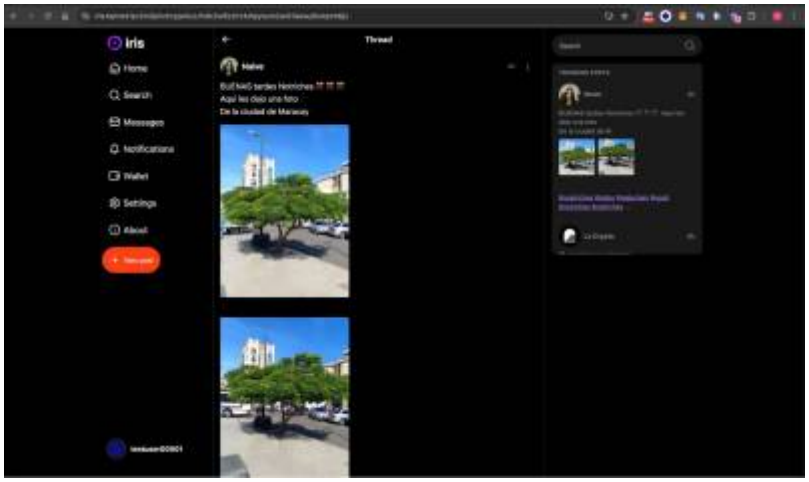


Después de que hacemos click en ese texto, el campo de la ventana cambiará y nos preguntará “cual es nuestro nombre” “**what’s your name** ?



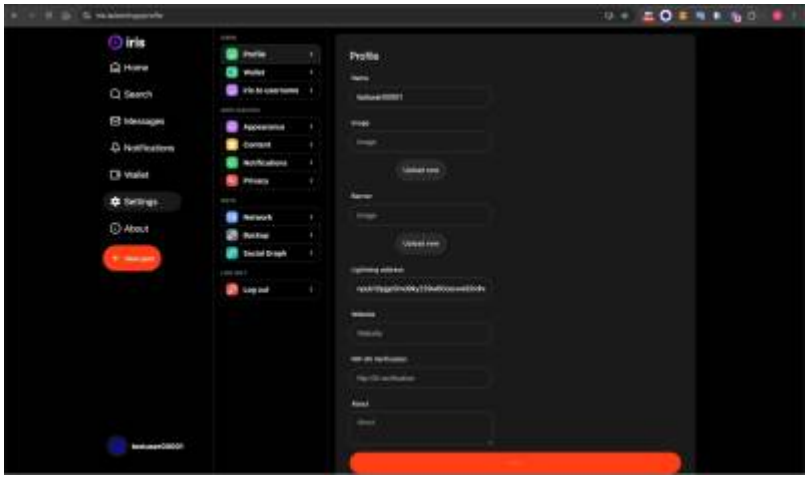
Esto es importante porque este nombre será único y será nuestro nombre de usuario en las diferentes redes.

Una vez que hayamos escrito un nombre y hagamos click en el botón “Go” ya estamos logueados en la aplicación web Iris; y nos daremos cuenta de ello, porque el nombre que ingresamos en el campo anterior, ahora aparece en la parte inferior de la pantalla.



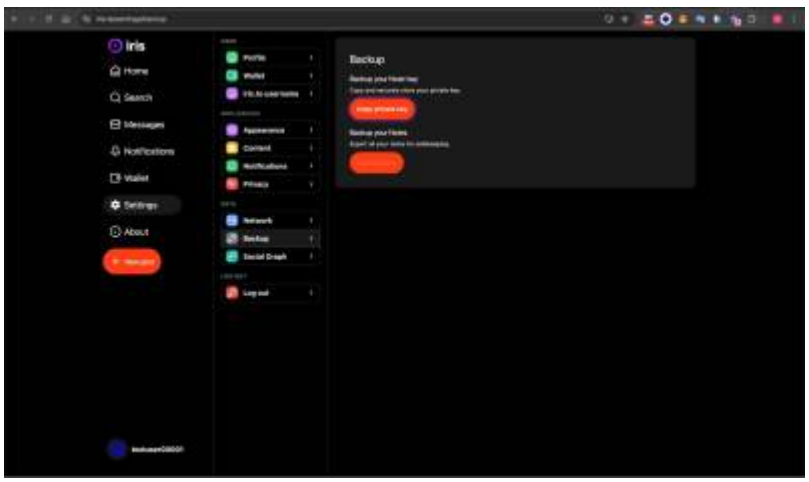
Para obtener nuestras claves pública/privada debemos hacer click en el botón "**settings**" ubicado a la izquierda. Una vez allí en la **opción profile**, donde dice "*Lightning address*", tendremos acceso a nuestra **clave pública o npub**.

Tendrá el siguiente formato:
npub10pjgd3md9ky239w10cecws92rdheel58ah74qc4q6n8743jxqdsqpwahr4@npub.cash



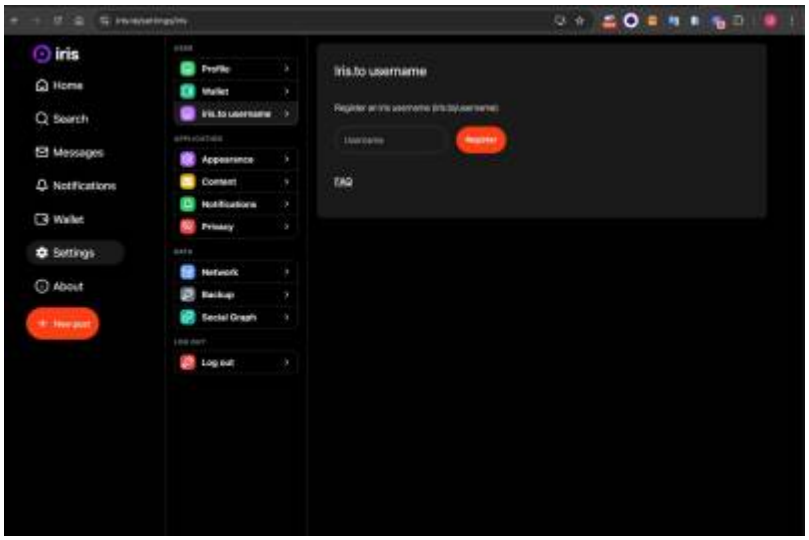
Luego hacemos click en la opción backup y allí hacemos click en el botón "**copy private key**"

La llave privada tendrá el siguiente formato:
nsec1qn3k92f44b5dwg9030980upvf339qc3gxezhcag6y0dymxagz77qzjzqrf



Finalmente para crear un alias a la cuenta y poder tener una dirección Nostr nos dirigimos a la

pestaña **iris.to username**. Allí nos aparecerá un campo que nos pide registrar un nombre de usuario. Normalmente ese nombre de usuario debería ser el nombre que ingresamos inicialmente cuando ingresamos a Nostr.



Una vez con estos datos, ya tenemos acceso a la web de iris y publicar y hacer nuestros primeros post en este cliente.

Cómo entrar a un cliente si ya tengo mi clave privada (nsec)