



#B40S

</bitcoin for open source>

librería de Satoshi

Compra y vende BTC sin intermediarios

Clase 1



Introducción al P2P: Exchanges sin KYC

฿40S

Temas

- Qué es KYC y por qué implica riesgos para la privacidad
- Por qué comprar y vender Bitcoin sin intermediarios
- Qué son los exchanges P2P de Bitcoin
- Plataformas P2P sin KYC: HodlHodl, Bisq, Robosats, Peach, Lnp2pbot y Mostro
- Comparación entre plataformas P2P
- Buenas prácticas al usar exchanges P2P
- Uso de kycnot.me para encontrar exchanges sin KYC

Objetivos

- Entender qué es el KYC y los riesgos que implica para la privacidad.
- Comprender por qué comprar y vender Bitcoin sin intermediarios.
- Conocer qué son los exchanges P2P y cómo funcionan.
- Identificar plataformas P2P que no requieren KYC.
- Comparar diferentes plataformas P2P.
- Aprender buenas prácticas al usar exchanges P2P.
- Usar kycnot.me para encontrar exchanges sin KYC **₿40S**

¿Has comprado BTC alguna vez?



฿40S

KYC: "Know Your Customer"

Prevenir fraude, lavado de dinero y financiamiento del terrorismo

- Solo 0,34 % de las transacciones cripto en 2023 fueron ilícitas
- En 2024 la estimación cayó a 0,14 %
- La mayoría del crimen cripto ya no usa Bitcoin
- Entre 800 mil millones y 2 billones USD se lavan cada año en el sistema financiero tradicional
- Esto representa 2-5 % del PIB mundial

El crimen financiero ocurre principalmente en el sistema fiat, no en Bitcoin.

B40S

Peligros del KYC

- Exposición de datos
- Mal manejo de información
- Venta de datos
- Phishing
- Riesgos para usuarios
- Exclusión de usuarios

La filtración de información de acreedores de FTX provoca temores de estafa



CoinoMedia

13 ago 2025

...



- Los nombres y correos electrónicos de los acreedores de FTX fueron filtrados.
- El riesgo de phishing y estafas ha aumentado.

B40S

La filtración de información de usuarios de criptomonedas provoca temores de estafa



CoinoMedia

13 ago 2025



- Los nombres y correos electrónicos de los usuarios filtrados.
- El riesgo de phishing y estafas ha aumentado.

La dark web es inundada con datos de usuarios de criptomonedas: ¿Qué ha sucedido?

 Elígenos en Google



Escrito por
Nhat Hoang



Editado por
Luis Blanco

14 abril 2025
12:08 UTC

- Datos personales de usuarios de Ledger, Gemini y Robinhood se están vendiendo en la dark web, generando renovados temores de seguridad en el sector cripto.
- Filtraciones muestran que correos electrónicos, números de teléfono y direcciones de usuarios en Estados Unidos fueron comprometidos, probablemente a través de phishing, no por brechas en las plataformas.
- Con el aumento del fraude impulsado por IA, los expertos instan a los usuarios a

La filtración de información de ad... provoca temores de estafa



CoinoMedia

13 ago 2025



La dark web es inundada con datos de usuarios de criptomonedas: ¿Qué ha sucedido?

Elígenos en Google



La Dark Web se llena de listados de cuentas y carteras de criptodivisas hackeadas

Endpoint 15 SEP 2022

- Los nombres y correos electrónicos filtrados.
- El riesgo de phishing y estafas

Por poco más de mil euros se puede comprar suficiente información personal para robar la identidad de una persona. Los precios de las cuentas de redes sociales están bajando, mientras que algunas criptomonedas y cuentas de inversión cuestan más que algunas cuentas bancarias.

La filtración de información de usuarios de Ledger
provoca temores de estafa



CoinoMedia

13 ago 2025



- Los nombres y correos electrónicos de los usuarios de Ledger fueron filtrados.
- El riesgo de phishing y estafas se ha incrementado.

La dark web es inundada con datos de usuarios de criptomonedas: ¿Qué ha sucedido?

CRIPTONOTICIAS 10

Home > Seguridad

Ledger sufre una filtración: Hackers podrían saber si compraste una wallet

Datos personales de clientes de Ledger quedaron expuestos tras un fallo en Global-e, un procesador de pagos utilizado por la empresa.



Las wallets de Ledger son unas de las más usadas por usuarios de criptomonedas. Fuente: Grok.

Publicado: 05 enero, 2026 02:01 pm GMT-0400

Actualizado: 05 enero, 2026 02:01 pm GMT-0400



Autor: **Franco Scandizzo**

Inió su recorrido en CriptoNoticias en mayo de 2024 y ha desempeñado su rol desde distintas secciones en la web, como Mercados, Comunidad y Estado. Su carrera comenzó en 2009 trabajando en diversos medios de comunicación, incluyendo crónicas radiales en medios locales, producción y coordinación de televisión en Canal 26.



Suscríbete a los boletines de CriptoNoticias

Mantente informado de los últimos

cuentas
as

ersonal para
s sociales están
uestan más

Cashea sufre filtración de datos tras incidente de seguridad

La empresa confirmó la filtración sin especificar qué tipo de información personal de sus clientes se encuentra comprometida.



Cashea se ha convertido en una alternativa de financiamiento en Venezuela. Fuente: Cashea.

Publicado: 22 febrero, 2026 02:12 pm GMT-0400

Actualizado: 25 febrero, 2026 02:17 pm GMT-0400



Autor: **Gabriela González**

Profesional venezolana orientada hacia las áreas de lingüística y literatura, así como también al análisis y a la investigación. Se ha desempeñado como redactora para medios digitales como Lifeder, Publisuites y Tintero Digital.

in X

Suscríbete a los boletines de CriptoNoticias

Mantente informado de los últimos acontecimientos del mundo de las criptomonedas.

SUSCRIBIRME

AA

🔗

X

✉

- Reportes externos mencionan hasta 46,5 GB de data filtrada.
- Los datos incluirían transacciones y registros vinculados a comercios aliados.

Los datos filtrados en la Cashea de Venezuela...

Cashea sufre filtración de datos por incidente de seguridad

La empresa confirmó la filtración sin especificar qué tipo de datos de sus clientes se encuentra comprometida.



Cashea se ha convertido en una alternativa de financiamiento en Venezuela. Fuente: Cashea.

AA

🔗

✂

✉

- Reportes externos mencionan hasta 46,5 GB de datos filtrados.
- Los datos incluirían transacciones y registros vinculados a comercios aliados.

Los datos filtrados incluyen los datos de los usuarios de Cashea.

La filtración de Ledger podría poner en riesgo la vida de las personas ¿por qué?

Al filtrarse las direcciones postales de los clientes, estos quedan expuestos a posibles ataques físicos o conocidos como 'wrench attacks'.



Los "wrench attacks" son ataques de violencia física donde un criminal amenaza a un propietario de activos digitales para robarle sus fondos. Fuente: Grok.

AA

🔗

✂

- En 2025, los ataques físicos aumentaron un 46% según TRM Labs.
- Latinoamérica es la región con mayor porcentaje de ataques físicos con desenlace fatal.

CRIPTONOTICIAS

Mantente informado de los últimos acontecimientos del mundo de las criptomonedas.

SUSCRIBIRME

Publicado: 06 enero, 2026 09:03 am GMT-0400

Actualizado: 06 enero, 2026 12:02 pm GMT-0400



Autor: **Franco Scandizzo**

Inicio su recorrido en CriptoNoticias en mayo de 2024 y ha desempeñado su rol desde distintas secciones en la web, como Mercados, Comunidad y Estado. Su carrera comenzó en 2009 trabajando en diversos medios de comunicación, incluyendo crónicas radiales en medios locales, producción y coordinación de televisión en Canal 26.

✂ ✉

Suscríbete a los boletines de CriptoNoticias

Mantente informado de los últimos acontecimientos del mundo de las criptomonedas.

B40S

Cashea sufre filtración de datos por incidente de seguridad

La empresa confirmó la filtración sin especificar qué tipo de datos de sus clientes se encuentra comprometida.



Usuarios de criptomonedas afectados por una masiva filtración de datos de infostealer

26 ene 2026, 09:03 GMT-6 · 3 minutos de lectura

Un investigador de ciberseguridad descubrió una base de datos masiva y de acceso público que contenía millones de credenciales de inicio de sesión robadas, recolectadas de dispositivos personales infectados con malware, incluyendo cuentas vinculadas a las principales plataformas de redes sociales y al exchange de criptomonedas, Binance.

La filtración de Ledger podría poner en riesgo la vida de las personas ¿por qué?

Al filtrarse las direcciones postales de los clientes, estos quedan expuestos a posibles ataques físicos o conocidos como 'wrench attacks'.



Publicado: 06 enero, 2026 09:03 am GMT-0400

Actualizado: 06 enero, 2026 12:02 pm GMT-0400



Autor: **Franco Scandizzo**

Inicio su recorrido en CriptoNoticias en mayo de 2024 y ha desempeñado su rol desde distintas secciones en la web, como Mercados, Comunidad y Estado. Su carrera comenzó en 2009 trabajando en diversos medios de comunicación, incluyendo crónicas radiales en medios locales, producción y coordinación de televisión en Canal 26.



Suscríbete a los boletines de CriptoNoticias

Mantente informado de los últimos acontecimientos del mundo de las criptomonedas.

Comparar gráficos



B40S

Cashea sufre filtración de datos por incidente de seguridad

La empresa confirmó la filtración sin especificar qué tipo de información de sus clientes se encuentra comprometida.



Usuarios de Cashea sufren filtración masiva de datos

26 ene 2026, 09:03 GMT-6 · 3 minutos de lectura

Un investigador de ciberseguridad publicó un informe público que contenía millones de datos personales recolectados de dispositivos personales de usuarios cuyas cuentas vinculadas a las principales criptomonedas, Binance.

La plataforma argentina Lemon Cash revela filtración de datos de usuarios

El equipo de Lemon confirmó que nombres y mails de usuarios quedaron expuestos tras un hackeo a su proveedor externo de analítica.



Lemon es una plataforma para almacenar y comprar y vender criptomonedas. Fuente: Grok.

AA

🔗

✕

- Desde Lemon aseguran que datos de fondos, claves privadas y frases de recuperación están a salvo.
- Mixpanel, el proveedor externo usado por OpenAI y Lemon, sufrió un hack que derivó en la filtración.

La filtración de Ledger podría poner en riesgo la vida de las personas ¿por qué?

Al filtrarse las direcciones postales de los clientes, estos quedan expuestos a posibles ataques físicos o conocidos como 'wrench attacks'.

Publicado: 06 enero, 2026 09:03 am GMT-0400
Actualizado: 06 enero, 2026 12:02 pm GMT-0400



Autor: **Franco Scandizzo**

Inicio su recorrido en CriptoNoticias en mayo de 2024 y ha desempeñado su rol desde distintas secciones en la web, como Mercados, Comunidad y Estado. Su carrera comenzó en 2009 trabajando en diversos medios de comunicación, incluyendo crónicas radiales en medios locales, producción y coordinación de televisión en Canal 26.

✕ ✉

Suscríbete a los boletines de CriptoNoticias

Mantente informado de los últimos acontecimientos del mundo de las criptomonedas.

Publicado: 04 diciembre, 2025 01:30 pm GMT-0400

Actualizado: 04 diciembre, 2025 03:24 pm GMT-0400



Autor: **Franco Scandizzo**

Inicio su recorrido en CriptoNoticias en mayo de 2024 y ha desempeñado su rol desde distintas secciones en la web, como Mercados, Comunidad y Estado. Su carrera comenzó en 2009 trabajando en diversos medios de comunicación, incluyendo crónicas radiales en medios locales, producción y coordinación de televisión en Canal 26.

✕ ✉

Suscríbete a los boletines de CriptoNoticias

Mantente informado de los últimos

NIKKEI

SP500

B40S

El peligro real es aplicar KYC

El filtrado de datos de Coinbase demuestra que el KYC actual aumenta los riesgos de crimen, en lugar de disminuirlo.



La vulneración de bases de datos de empresas de criptomonedas ha levantado olas de amenazas y violencia. Fuente: ChatGPT.

AA

🔗

✂

- El KYC vuelve a todos los negocios en agentes del Estado.
- Los ataques físicos a usuarios de criptomonedas crecen exponencialmente.

Publicado: 21 mayo, 2025 01:12 pm GMT-0400
Actualizado: 21 mayo, 2025 02:37 pm GMT-0400



Autor: **CriptoNoticias Editorial**

Editorial de CriptoNoticias. Publica artículos informativos y de opinión, así como mensajes institucionales sobre el medio, su gente y sus servicios.



Suscríbete a los boletines de CriptoNoticias

Mantente informado de los últimos acontecimientos del mundo de las criptomonedas.

SUSCRIBIRME

El peligro El caso Coinbase pone en evidencia el lado oscuro del KYC

El filtrado de datos de crimen, en lugar de



La vulneración de bases de datos de

AA

🔗

✂

- El KYC vuelve Estado.
- Los ataques exponencial



Imagen destacada por momius / stock.adobe.com

AA

🔗

✂

- Coinbase aseguró que reembolsará el dinero a gente que pagó el “rescate” de sus datos.
- Si no dinero, estos usuarios todavía perderán tranquilidad, reputación y privacidad.

Si la filtración de datos de usuarios no les provocó pérdidas económicas a algunos, todavía podrán ser acosados y manipulados en el futuro.

Publicado: 16 mayo, 2025 12:10 pm GMT-0400

Actualizado: 16 mayo, 2025 06:43 pm GMT-0400



Autor: **Paulo Márquez**

Paulo Márquez es el Jefe de Redacción en CriptoNoticias. Ha cubierto eventos en Estados Unidos, Andorra y Colombia. Anteriormente, fue responsable de la sección Tecnología y también de Afiliados, además escribió múltiples reseñas y tutoriales de productos con criptomonedas, desde exchanges hasta monederos.



Suscríbete a los boletines de CriptoNoticias

Mantente informado de los últimos

B40S

El peligro El caso Coinlado oscuro

El filtrado de datos de crimen, en lugar de



La vulneración de bases de datos de

AA

🔗

✕

- El KYC vuelve Estado.
- Los ataques exponencial

Si la filtración de datos de u todavía podrán ser acosado



AA

🔗

✕

- Coinbase aseguró que que pagó el “rescate” de sus datos.
- Si no dinero, estos usuarios todavía perderán tranquilidad, reputación y privacidad.

KYC no es efectivo para detener criminales, pero les facilita robar datos de sus víctimas

Los especialistas en privacidad y Bitcoin, Janine Römer y Matt Odell, intercambiaron ideas en el marco del evento Keys Fest 2022, organizado por Casa.



Janine Römer y Matt Odell, investigadores de Bitcoin y la privacidad dijeron en la conferencia Key Fest 2022 que la conciencia individual sobre la importancia de proteger la privacidad aún no se ha generalizado entre los usuarios de Bitcoin. Composición por CriptoNoticias, putlov_denis/ stock.adobe.com; Bits and Splits/ stock.adobe.com

AA

🔗

✕

- Especialistas creen que actualmente los jóvenes no están conscientes de cuánto exponen su privacidad
- Señalan que los datos KYC en poder de custodios de bitcoin serían más valiosos que el bitcoin en sí.

Suscríbete a los boletines de CriptoNoticias

Mantente informado de los últimos

Publicado: 09 enero, 2022 12:33 pm GMT-0400
Actualizado: 09 enero, 2022 12:33 pm GMT-0400



Autor: **Genny Díaz**

Comunicadora Social. Adepta a la libertad. Curiosa de las nuevas tecnologías. Firme creyente en que los valores y principios sostienen las grandes sociedades.

✕ ✉

Suscríbete a los boletines de CriptoNoticias

Mantente informado de los últimos acontecimientos del mundo de las criptomonedas.

SUSCRIBIRME

B40S

Comprar Bitcoin directamente entre personas

P2P = peer to peer

Ventajas:

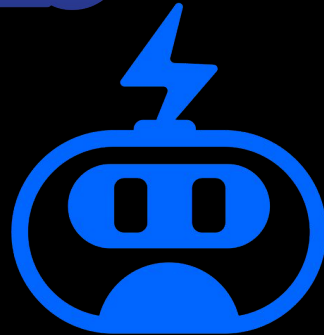
- Más privacidad
- Menos intermediarios
- Más control propio

Exchange P2P

Plataforma que:

- Conecta compradores y vendedores
- Usa escrow
- Permite distintos métodos de pago

Exchanges P2P

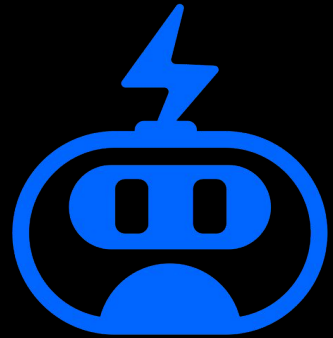


Lnp2pBot



B40S

- **Tipo:** Bot de Telegram para intercambios P2P de Bitcoin
- **Capa:** Lightning Network
- **Escrow:** Hold invoice (Lightning)
- **Cliente:** Telegram
- **Registro:** No requiere registro, solo cuenta de Telegram
- **Open Source:** Sí
- **Liquidez:** Fuerte en LATAM
- **Reputación:** Sistema de reputación entre usuarios
- **Comisiones:** ~0.6% para vendedores, 0% para compradores
- **Ventajas:** Muy fácil de usar, rápido gracias a Lightning
- **Limitaciones:** Depende de Telegram, no soporta transacciones on-chain



Lnp2pBot

<https://lnp2pbot.com/>

B40S

- **Tipo:** Exchange P2P basado en web
- **Capa:** Bitcoin On-chain
- **Escrow:** Contrato multifirma (multisig)
- **Cliente:** Web
- **Registro:** Registro con email, sin KYC
- **Open Source (No):** Backend de la plataforma, motor del marketplace, infraestructura del servidor y lógica de trading
- **Open Source (Sí):** Librerías y herramientas relacionadas con multisig y algunos componentes auxiliares publicados en GitHub
- **Liquidez:** Principalmente EUR y USD
- **Reputación:** Sistema de reputación de usuarios
- **Comisiones:** Aproximadamente 0.5%–0.6%
- **Ventajas:** Escrow multisig robusto, plataforma estable con varios años de operación
- **Limitaciones:** No soporta Lightning, experiencia de usuario menos moderna



HODLHODL

<https://hodlhodl.com/>

Bitcoin
B40S

- **Tipo:** Exchange descentralizado P2P
- **Capa:** Bitcoin On-chain y Lightning
- **Escrow:** Multisig
- **Cliente:** Aplicación Desktop y app
- **Registro:** No requiere registro ni cuenta
- **Open Source:** Sí
- **Liquidez:** Variable según región
- **Reputación:** Sistema descentralizado con depósitos de seguridad
- **Comisiones:** Aproximadamente 1.15% Taker / 0.15% Maker
- **Ventajas:** Muy descentralizado, alto nivel de privacidad
- **Limitaciones:** Interfaz más compleja para usuarios nuevos



<https://bisq.network/>

- **Tipo:** Exchange P2P enfocado en privacidad
- **Capa:** Lightning Network y Bitcoin On-chain
- **Escrow:** Hold invoice + Fidelity Bond
- **Cliente:** Web sobre Tor y aplicación móvil
- **Registro:** No requiere registro
- **Open Source:** Sí
- **Liquidez:** Principalmente EUR, USD y BRL
- **Reputación:** Identidades temporales (robots)
- **Comisiones:** Aproximadamente 0.175% Taker / 0.025% Maker
- **Ventajas:** Alta privacidad, uso sencillo sin cuentas
- **Limitaciones:** Liquidez variable según región, Tor es muy lento, Bond



<https://learn.robosats.org/>

B40S

- **Tipo:** Aplicación móvil P2P
- **Capa:** Bitcoin On-chain
- **Escrow:** Multisig
- **Cliente:** Aplicación móvil
- **Registro:** No requiere KYC
- **Open Source (No):** Backend completo del marketplace, infraestructura del servidor y lógica de coordinación de intercambios
- **Open Source (Sí):** Parte del código de la aplicación (frontend), API pública y algunas herramientas para desarrolladores
- **Liquidez:** Principalmente en Europa
- **Reputación:** Sistema de reputación de usuarios
- **Comisiones:** Aproximadamente 2% para compradores
- **Ventajas:** Experiencia de usuario simple
- **Limitaciones:** Muy poca liquidez fuera de Europa



<https://peachbitcoin.com/>

₿40S

- **Tipo:** Exchange P2P construido sobre Nostr
- **Capa:** Lightning Network
- **Escrow:** Hold invoice
- **Cliente:** App Android, clientes TUI y CLI
- **Registro:** No requiere registro
- **Open Source:** Sí
- **Liquidez:** En crecimiento, depende de cada Nodo
- **Reputación:** Sistema de reputación basado en Nostr
- **Comisiones:** Aproximadamente 0.3% Maker / 0.3% Taker
- **Ventajas:** Arquitectura descentralizada basada en Nostr, fácil de usar
- **Limitaciones:** Hay que buscar la pubkey del Nodo al que unirse



<https://mostro.network/>

B40S

		Lightning	Onchain	Fees	Cliente	Escrow	Open Source
Lnp2pbot		✓	✗	0.6% Vendedor 0% Comprador	Telegram	Hold Invoice	✓
HodlHodl		✗	✓	0.3% Taker 0.3% Maker	Web	Multisig	✗
Bisq		✓	✓	1.15% Taker 0.15% Maker	Desktop	Multisig	✓
Robosats		✓	✓	0.175% Taker 0.025% Maker	Web(Tor) y App	Hold Invoice	✓
Peach		✗	✓	2% Comprador 0% Vendedor	App	Multisig	✗
Mostro		✓	✗	0.3% Taker 0.3% Maker	Cientes Nostr	Hold Invoice	✓

Riesgos del P2P

- Triangulaciones
- Comprobantes falsos
- Pagos revertidos
- Contrapartes maliciosas

Buenas prácticas

- Informarse antes de usar el sistema
- Revisar reputación de la contraparte
- Si es un sistema multi-instancias, revisar su reputación
- No operar fuera del sistema
- No acceder a cambiar el método de pago a última hora
- No dar más información personal de la necesaria a tu contraparte
- Usar métodos de pago del fiat irreversibles
- Nunca liberar los sats si el fiat aun no te llega
- Reportar comportamientos sospechosos
- Abrir disputas a tiempo
- Verificar el “soporte de la plataforma”
- Reportar errores

FILTERS

Sort By

Score (High → Low) ▾

⌂ Ties randomly sorted

Name

Search...

Type

- ☐ ↔ Exchange 148
- ☐ ⌘ Aggregator 51
- ☐ ☁ Hosting 42
- ☐ ✂ Tool 42
- ☐ 🛒 Shopping 31
- ☐ 🖥 VPS 29
- ☐ 🛡 VPN 26
- ☐ 💬 SMS 19

+ Show more

Approved and Verified services

80 results

🔍 Include +281 community contributed

+ Add service

**RoboSats** ✓

↔ Exchange

P2P exchange bitcoin for national currencies. Robosats simplifies the peer-to-peer user experience.

10



KYC 0

**Bisq** ✓

↔ Exchange

Buy and sell bitcoin for fiat (or other cryptocurrencies) privately and securely using Bisq's peer-to-peer network and open-source desktop software. No registration required.

10



KYC 0

**eigenwallet**

↔ Exchange

Bitcoin -> Monero atomic swaps, securely and in a decentralized manner using a state-of-the-art cryptographic protocol and open-source desktop software. Formerly...

9



KYC 1

**XmrBazaar**

🛒 Marketplace 🛒 Shopping

Peer-to-peer Monero marketplace. Buy and sell products, services and rentals for Monero.

9



KYC 0



- ☐ Clearnet
- ☐ Onion
- ☐ I2P

Currencies

OR AND

- ☐ Monero
- ☒ **Bitcoin**
- ☒ **Lightning**
- ☒ **Fiat**
- ☐ Cash

KYC Level

- ☒ **Guaranteed no KYC** lvl. 0
- ☒ **No KYC mention** lvl. 1
- ☒ **KYC on authorities request** lvl. 2
- ☒ **Shotgun KYC** lvl. 3
- ☒ **Mandatory KYC** lvl. 4

User Rating (min)



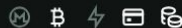
9 KYC 1

**Peach Bitcoin**

Exchange

Peach is a mobile application that connects Bitcoin Buyers & Sellers together. Buy or sell bitcoin peer-to-peer, anywhere, at anytime, with the payment method of your choice.

8 KYC 0

**Inp2pBot**

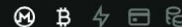
Exchange

A Telegram bot for buying and selling bitcoin on the Lightning Network, in a peer-to-peer manner, using your local currency without requiring KYC or providing personal data.

8 KYC 0



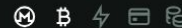
9 KYC 1

**WizardSwap**

Exchange

WizardSwap is an instant swap exchange run by LocalParticl.com - Supports many privacy coins.

8 KYC 1

**Boltz**

Exchange

Non-custodial Bitcoin bridge to swap between the Liquid and Lightning Network. Boltz Users can always rest assured to be in full control of their bitcoin throughout the entire flow of a...

8 KYC 1



Próxima Sesión:

Práctica con LNP2PBot y Mostro

B4OS

Gracias!

bitcoin4opensource.com