

BILLETERAS CRYPTO:

TU LLAVE AL MUNDO DE LAS CRIPTOMONEDAS.

FOTO: WWW.FREEPICK.COM

>> POR:
CP. DR. MARTÍN
FEDERICI.



DIRECTOR DE KUABI. ESPECIALISTA EN GESTIÓN DE PATRIMONIOS E INVERSIONES.

La importancia de quién posee el control y custodia de las claves privadas se resume en el famoso dicho “no son tus llaves, no son tus monedas”.

Las criptomonedas han transformado el panorama económico, desde el emblemático Bitcoin hasta la creciente variedad de altcoins, ofreciendo emocionantes oportunidades tanto para inversores como para usuarios comunes. No obstante, lo que a menudo resulta intrigante y, en ocasiones, desconcertante, es la forma en que se almacenan y gestionan estos activos digitales, a través de la criptografía y la tecnología blockchain.

Esta última funciona como un libro de contabilidad público y transparente que registra de manera exhaustiva todas las transacciones de criptomonedas. Para acceder y administrar estos activos, necesitamos una billetera o monedero digital, también conocida como wallet. Esta herramienta puede ser tanto un dispositivo de hardware como una aplicación de software y nos otorga la capacidad de gestionar y controlar el acceso a nuestros activos digitales mediante un sistema doble de claves criptográficas: la clave pública y la clave privada. Aunque la billetera en sí no almacena las criptomonedas, genera y resguarda estas claves, lo que permite firmar, acceder y cifrar todas las transacciones que se realicen.

Por un lado, la clave privada representa la llave digital que otorga acceso y control sobre los fondos, es decir, sobre las criptomonedas, y permite la validación de las transacciones en la blockchain, similar a un PIN o contraseña que debemos mantener en secreto. Por otro lado, la clave pública es la dirección que podemos compartir con terceros para recibir esos activos, semejante a una cuenta bancaria.

Al comprender la importancia de estas claves y su relación con nuestros activos, estaremos preparados para sumergirnos en el apasio-

nante mundo de las criptomonedas y asegurar que los fondos estén bajo nuestro control y seguridad.

TIPOS DE BILLETERAS:

1- Billeteras calientes (Hot wallets)

Son ideales para las transacciones diarias por su conectividad constante a internet, lo que garantiza velocidad y accesibilidad. Por lo general, son gratuitas y recomendadas para inversores de corto plazo o “traders”, pero ofrecen un nivel de seguridad relativamente bajo.

1.1 Billeteras de software (Software wallets): Son aplicaciones o programas para dispositivos de escritorio o móviles, de fácil uso y muy populares entre los principiantes. Pueden dividirse en:

1.1.1. Billeteras de escritorio (Desktop wallets): Implica la descarga y ejecución local de un software, como Electrum o Exodus, a través de un archivo de datos de la billetera, brindando un control total de las claves, pero con el riesgo de daño físico o infección por virus.

1.1.2. Billeteras móviles (Mobile wallets): Son aplicaciones para smartphones, como Trust Wallet o Muun, que se descargan de las tiendas de Google o Apple y son útiles para servicios de pago, pero vulnerables al malware. Por eso, se recomienda siempre cifrar las contraseñas, además de realizar copias de seguridad de las claves privadas.

1.1.3. Billeteras en línea (Online wallets): Se ejecutan en servidores en línea y son accesibles desde cualquier navegador web, sin necesidad de descargar ni instalar nada. Algunas permiten un control total o compartido de las claves, utilizando multifirmas,

mientras que otras son custodiadas por terceros, como Binance o Coinbase, lo que conlleva ciertos riesgos de seguridad.

2- Billeteras frías (Cold wallets)

Son adecuadas para inversores de largo plazo o "hodlers", ya que no están conectadas a internet. Ofrecen un alto nivel de seguridad y almacenan las claves fuera del entorno digital, es decir "en frío". Poseen una menor facilidad de uso y suelen ser más caras que el resto de las billeteras. Podemos dividir las en:

2.1 Billeteras de hardware (hardware wallets) Son dispositivos físicos similares a pendrives, como Ledger o Trezor, que se conectan por USB o Bluetooth. Almacenan las claves privadas de forma offline y validan las transacciones a través de una firma externa, lo que las hace inmune a los ataques en línea, incluso en dispositivos infectados.

2.2. Billeteras de papel (Paper wallets) Son una forma física de almacenar las claves privadas y direcciones públicas, en formato texto o QR, impresas en papel u otro material. Actualmente algunos las consideran obsoletas y poco confiables, ya que no son adecuadas para transacciones parciales.

3- Billeteras según tipo de custodia

La importancia de quién posee el control y custodia de las claves privadas se resume en el famoso dicho "no son tus llaves, no son tus monedas". En otras palabras, si no tenemos el control total de las claves, corremos el riesgo de perder nuestros activos digitales.

3.1 Billeteras de custodia propia (Self-Custody) En las Self-Custody, el usuario tiene un control total sobre sus claves privadas. No depende de terceros, lo que implica un mayor conocimiento y responsabilidad en la gestión de claves y copias de seguridad. Ejemplos: Desktop y hardware wallets.

3.1 Billeteras de custodia propia (Self-Custody) En las Self-Custody, el usuario tiene un control total sobre sus claves privadas. No depende de terceros, lo que implica un mayor conocimiento y responsabilidad en la gestión de claves y copias de seguridad. Ejemplos: Desktop y hardware wallets.

3.2 Billeteras custodiadas por terceros (Third-Party Custody) En este tipo de billeteras, se confían las claves privadas y activos digitales a terceros, como exchanges o servicios de billetera en línea. A menudo, se ofrece un servicio de recuperación de contraseña en caso de problemas de acceso. Sin embargo, esta elección conlleva un riesgo significativo de seguridad, como fraudes y hackeos en las plataformas, que pueden resultar en restricciones de acceso o robo de activos.

FACTORES A CONSIDERAR AL ELEGIR UNA BILLETERA:

Al seleccionar una billetera de criptomonedas, es esencial evaluar varios aspectos clave. Primero, debemos investigar el nivel de seguridad, incluyendo si utiliza almacenamiento en frío para las claves privadas y si ofrece autenticación de dos factores (2FA) para una capa adicional de protección. También, debemos considerar su compatibilidad con las criptomonedas específicas que planeamos almacenar o gestionar, así como su adecuación para el sistema operativo de nuestro dispositivo (Windows, macOS, Android o iOS).

La facilidad de uso es un factor importante, incluyendo la presencia de una interfaz intuitiva y una experiencia amigable. De igual modo, la capacidad de integración con aplicaciones externas para la compra y venta directa desde la billetera puede ser muy conveniente.

No debemos pasar por alto los costos y tarifas asociados, ya sea por transacciones o suscripciones. Además, es fundamental conocer la disponibilidad de soporte y atención al cliente en caso de problemas o preguntas.

La reputación y el historial de la billetera son indicadores valiosos, especialmente en términos de seguridad. Asimismo, la frecuencia de actualizaciones y el desarrollo continuo son señales de una billetera confiable y en mejora constante. Finalmente, debemos considerar si la billetera es custodiada por terceros o si tendremos el control total de nuestras claves.

CONCLUSIÓN: La evolución del ecosistema crypto ha mejorado nuestra percepción del valor de los activos digitales. Elegir la billetera adecuada se convierte en un paso fundamental en esta travesía. Comprender las diferencias entre billeteras calientes y frías, así como la importancia de la custodia propia frente a terceros, nos empodera para mantener nuestros activos seguros y bajo control. Factores como seguridad, facilidad de uso, compatibilidad y reputación deben orientar nuestra elección. Y aunque no existe una solución única, con la información y el conocimiento adecuados, podemos adentrarnos en el emocionante mundo de las criptomonedas con confianza y la certeza de que nuestras llaves representan nuestros activos. ■