****

Integrantes:

Jazmín Chavira Ruiz

Naiby Adriana Villalobos Villarreal

Andrea García Espinoza

Alexander Romero Ramírez

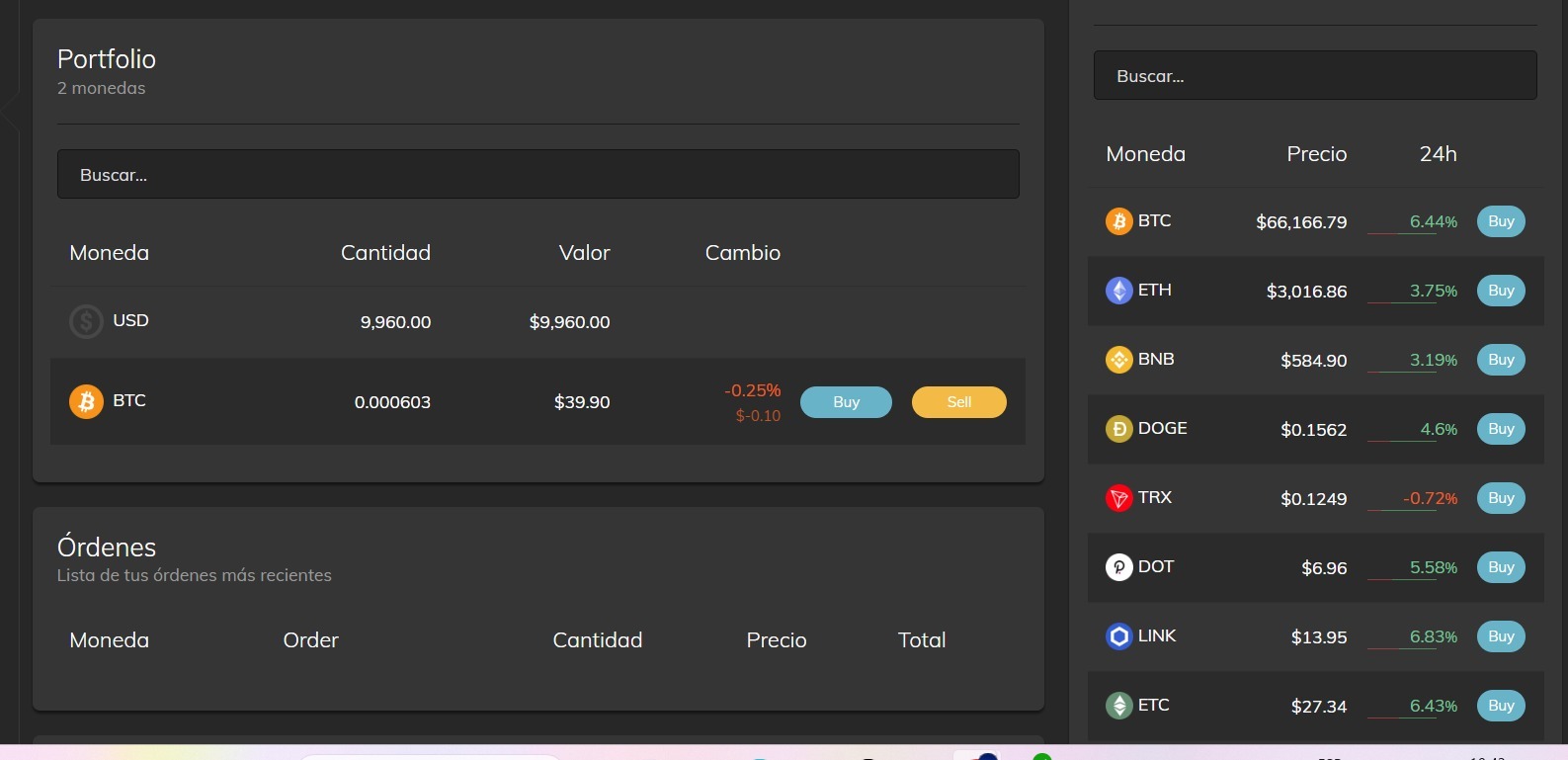
19/nov/2024

CRIPTOMONEDAS

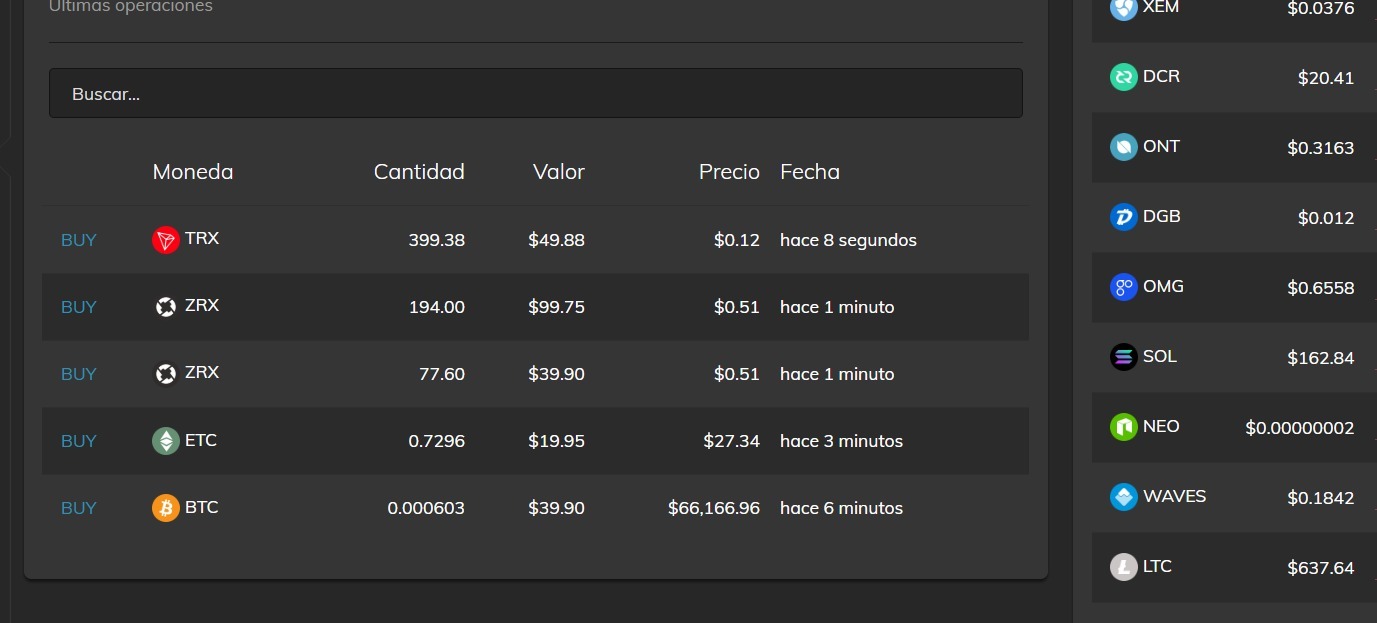
Práctica

**Simulación de Compra**

**Primero, entramos a la sección de compra de criptomonedas en la aplicación y seleccionamos Bitcoin. Después, escribimos cuánto queríamos comprar y elegimos el método de pago. Una vez que completamos la transacción, se revisó el portafolio:**



En este había $9,960 en USD y 0.000603 BTC, equivalente a $39.90, con una ligera baja del -0.25%. Se muestra una lista de criptomonedas disponibles, como Bitcoin, Ethereum y Dogecoin, con sus precios y cambios recientes.



En esta sección de la plataforma, se realizaron varias compras de criptomonedas.

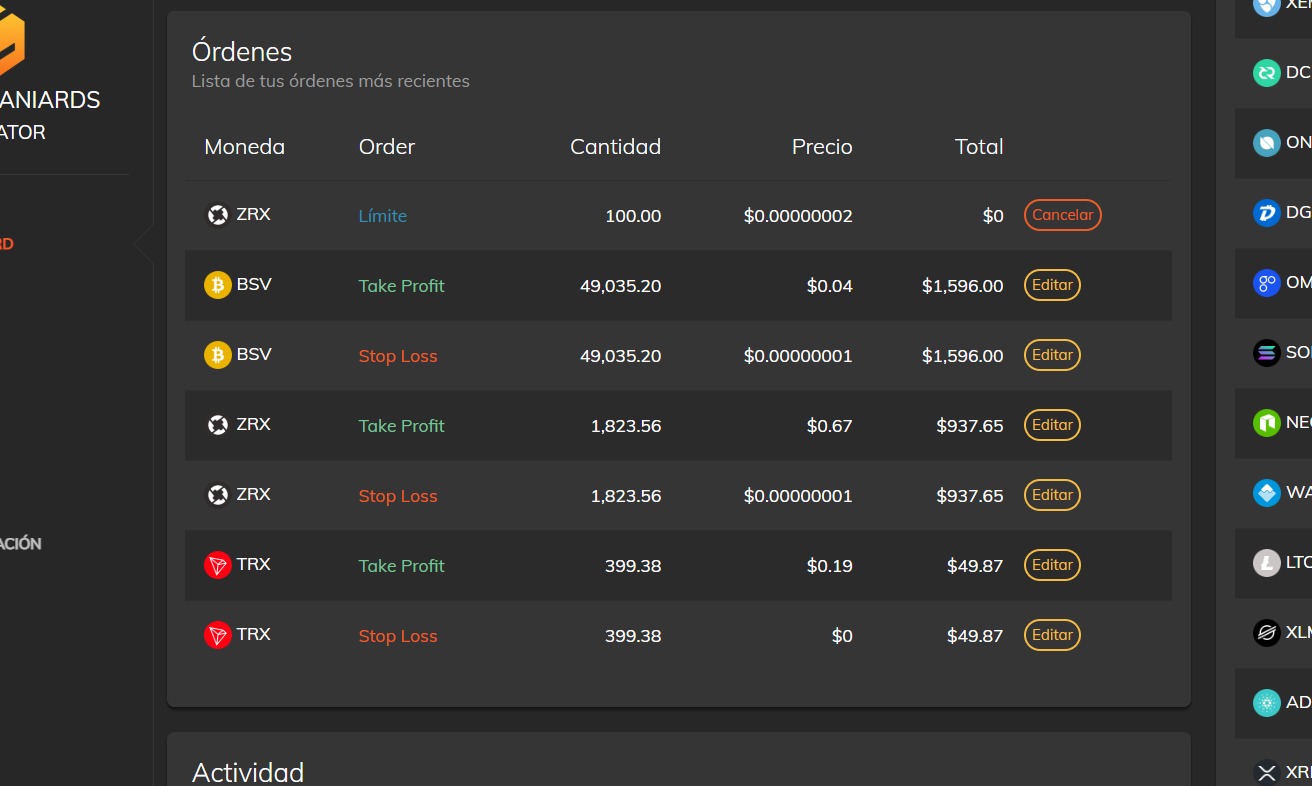
Seleccionamos las criptomonedas para comprar: Elegimos varias monedas, como TRX, ZRX, ETC y BTC.

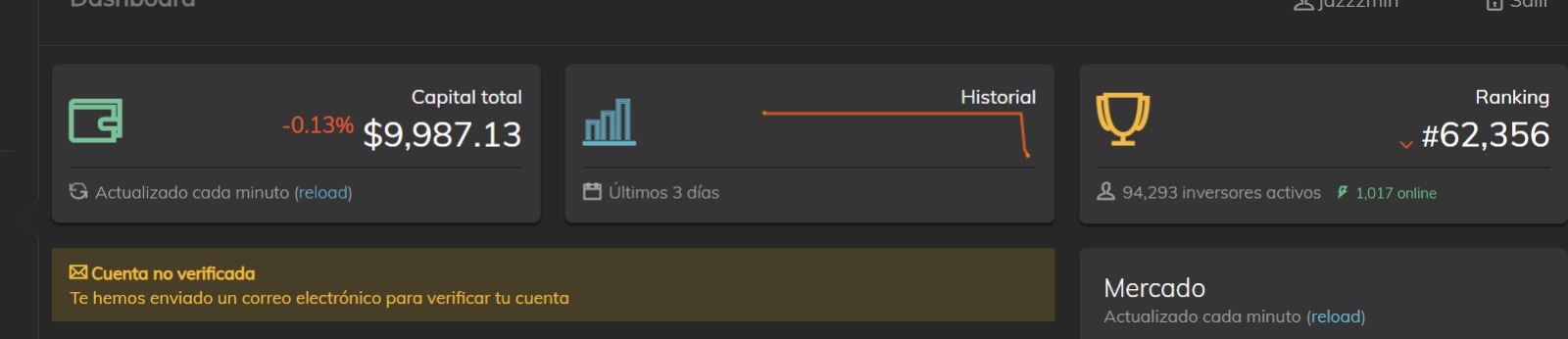
Determinamos la cantidad a comprar: Por ejemplo, compramos 399.38 TRX, 194 ZRX, 0.7296 ETC y 0.000603 BTC.

Revisamos los valores de las compras: Para cada moneda, vimos el valor total de la operación. Por ejemplo, TRX fue comprado por $49.88, ZRX por $99.75, y así sucesivamente.

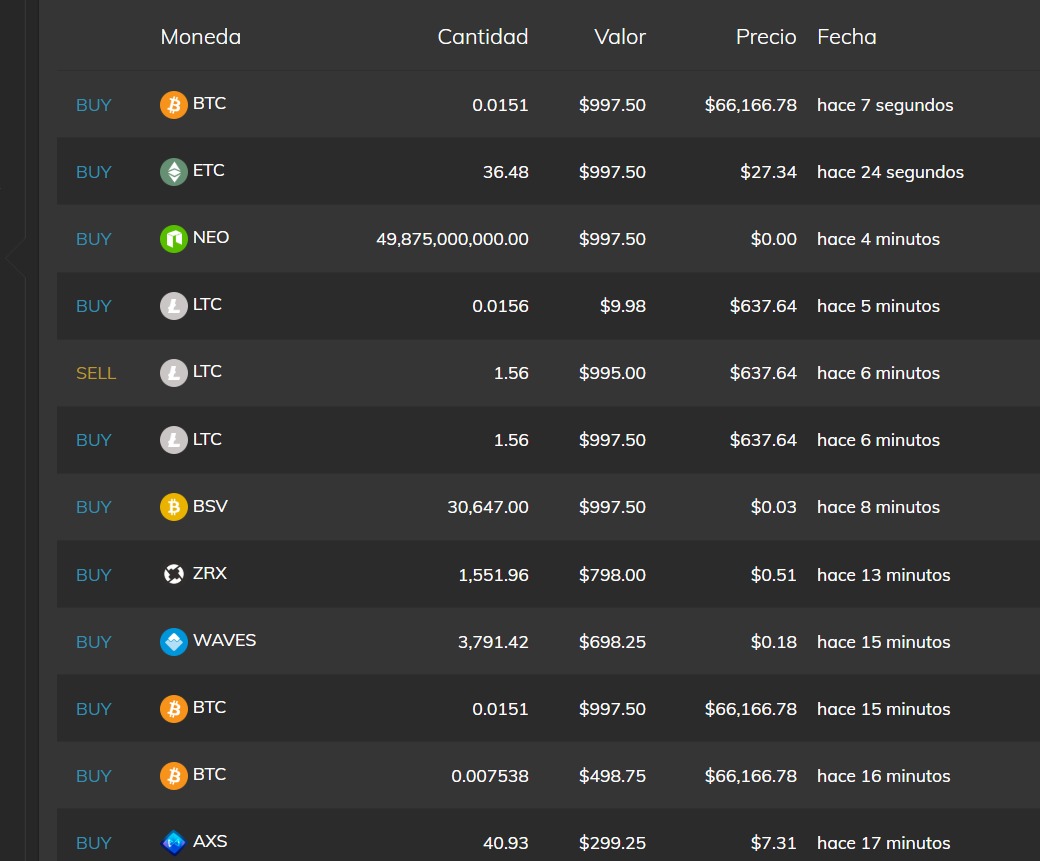
Completamos la compra: Las compras se realizaron con precios específicos por unidad de moneda, como $0.12 por TRX, $0.51 por ZRX, y $27.34 por ETC.

Verificamos el tiempo de las operaciones: Todas las transacciones fueron registradas, indicando el tiempo en que se completaron, como "hace 8 segundos", "hace 1 minuto", etc.



En este apartado se pueden ver la lista de las ordenes más recientes, muestra el tipo de moneda, tipo de orden, la cantidad, el precio y el total de cada una.

Aquí accedimos a la cartera en la cual aparece el total de las criptomonedas, bajó un 0.13%, pues al inicio contábamos con 10,000. También se puede observar el ranking y el historial de manera gráfica.



Hicimos más compras usando distintas monedas como BTC, ETC, NEO, LTC, BSV, ZRX, WAVES, y AXS. Y vendimos 1.56 criptomonedas de tipo LTC por un precio de $637.64.



Esta es la muestra de la billetera al final, el porcentaje de pérdidas es del 0.01%, pero comparándolo con el de antes, las perdidas han bajado.

## **Gestión de Criptomonedas**

### **2.1 Acceso a la Cartera**

Ingresamos a la sección de "Cartera" dentro de la aplicación para visualizar el saldo de criptomonedas.

**Detalles observados**:

* Saldo actual: [Cantidad de BTC u otra criptomoneda].
* Historial de transacciones: [Resumen del historial de depósitos y retiros].

### **2.2 Envío y Recepción de Criptomonedas**

* **Envío**:
  + Dirección utilizada: [Dirección de prueba].
  + Monto enviado: [Cantidad mínima permitida].
  + Confirmación: Recibimos notificación de envío exitoso.
* **Recepción**:
  + Compartimos nuestra dirección de billetera.
  + Verificamos la llegada de los fondos.

### **2.3 Conversión de Criptomonedas**

Exploramos la función de conversión para cambiar una criptomoneda por otra.

* **Criptomoneda inicial**: Bitcoin (BTC).
* **Criptomoneda de destino**: Ethereum (ETH).
* **Resultados**:
  + Tasa de conversión aplicada: [Tasa en el momento].
  + Monto convertido: [Cantidad recibida en ETH].

**Análisis de la Seguridad sobre las Criptomonedas**

La seguridad en el mundo de las criptomonedas es un tema de gran relevancia y complejidad. Si bien la tecnología blockchain, que sustenta a muchas criptomonedas, ofrece un alto nivel de seguridad y transparencia, existen diversos factores que pueden comprometer los activos digitales de los usuarios.

Las criptomonedas ciertamente tienen sus beneficios, pero muchos usuarios aún desconocen lo que son debido a las preocupaciones sobre la seguridad y sobre cómo funciona su tecnología. Es una industria emocionante en la que participar, pero se basa en la confianza. Por lo tanto, es muy importante que las empresas de criptomonedas hagan todo lo posible para proteger sus sistemas y minimizar las posibilidades de violaciones de seguridad que pueden ocasionar el robo de las criptomonedas de sus usuarios. Dado que las transacciones en redes blockchain públicas como Bitcoin y Ethereum se pueden rastrear debido a la estructura descentralizada de su cadena de bloques o blockchain, se determinará como las principales empresas que brindan servicios de intercambio de criptomonedas están trabajando con firmas de análisis para mantener una base de datos de transacciones y billeteras sospechosas.

### Vulnerabilidades y Riesgos

* **Hacking de intercambios:** Los intercambios de criptomonedas son objetivos frecuentes para los ciberdelincuentes, quienes buscan robar grandes cantidades de monedas. Los hackeos a plataformas como Mt. Gox y Coincheck han demostrado la gravedad de estas amenazas.
* **Phishing y estafas:** Los ataques de phishing son comunes en el mundo de las criptomonedas. Los delincuentes utilizan correos electrónicos falsos, mensajes de texto o sitios web clonados para engañar a los usuarios y obtener sus credenciales de acceso.
* **Pérdida de claves privadas:** Las claves privadas son fundamentales para acceder a las criptomonedas. Si se pierden o son robadas, es prácticamente imposible recuperar los fondos.
* **Vulnerabilidades en las carteras:** Las carteras de criptomonedas, tanto las de software como las de hardware, pueden presentar vulnerabilidades que pueden ser explotadas por los atacantes.
* **Ataques de 51%:** En algunas criptomonedas, un atacante podría controlar más del 51% de la potencia de cálculo de la red, lo que le permitiría revertir transacciones y generar nuevas monedas falsas.
* **Regulaciones y cumplimiento:** La falta de regulaciones claras en algunos países puede dificultar la protección de los consumidores y crear un entorno propicio para actividades ilícitas.
* **Hackeos de computación:** Es muy normal encontrar ataques a activos o páginas de internet, donde el hacker introduce código de minado, para secuestrar recursos de computación remoto, que añaden a un pool, para obtener más capacidad y redito económico en las operaciones de minado. Aquí son susceptibles todos los activos que tengamos publicados en Internet.

A medida que las criptomonedas ganan popularidad, también aumenta la cantidad de ataques a las plataformas de intercambio de criptomonedas. Los mayores ataques, como el ataque a FTX, provocaron el robo de millones de dólares, el cierre de las plataformas en cuestión y, en algunos casos, incluso consecuencias legales para los propietarios de las plataformas.

En el caso de algunas plataformas de trading y monederos, como Stormgain, los ataques aún no se convirtieron en un problema grave, aunque quizá solo sea cuestión de tiempo. Estos son los ataques a las plataformas de intercambio de criptomonedas más conocidos.

### 1. Ronin Network

* En marzo de 2022, en el mayor ataque en el mundo de las criptomonedas hasta la fecha, un grupo de ciberdelincuentes —que se cree que es un grupo de hackers norcoreanos— [irrumpió en la plataforma de intercambio Ronin Network, especializada en videojuegos, y robó unos $615 millones](https://es.cointelegraph.com/news/the-aftermath-of-axie-infinity-s-650m-ronin-bridge-hack) en las criptomonedas estables Ethereum y USDC.
* Los hackers llevaron a cabo el ataque a través de claves privadas robadas a los propietarios para retirar las monedas, lo que constituye un [ejemplo paradigmático de piratería informática](https://latam.kaspersky.com/resource-center/definitions/what-is-hacking) efectuada mediante el robo de claves.

### 2. Poly Network

* En otro gran ataque a una plataforma de intercambio de criptomonedas, ocurrido en agosto de 2021, los atacantes aprovecharon una vulnerabilidad en el [software de Poly Network para robar criptomonedas por un valor de $611 millones](https://www.lavanguardia.com/tecnologia/20210811/7656867/poly-network-mayor-robo-criptomonedas-historia-pmv.html). Sin embargo, el hacker había llevado a cabo el ataque solo para ver si era posible. Eventualmente, devolvió todos los fondos robados.

### 3. FTX

* Llevado a cabo en noviembre de 2022, el [ataque a FTX](https://es.beincrypto.com/aprende/quiebra-ftx-sam-bankman-fried/) es quizás uno de los más notorios. En ese momento, FTX era una de las plataformas de intercambio más poderosas de la industria de las criptomonedas, pero el día en que se declaró en quiebra, robaron más de $600 millones de sus monederos. Este fue el primero de dos ataques a la plataforma de intercambio FTX. En enero de 2023, otro ataque informático le costó $15 millones en monedas robadas.

## **Cómo se protegen las criptomonedas**

### 1. Plataformas de criptomonedas confiables

Buscar plataformas de criptomonedas **confiables y reconocidas es una medida clave**. Investigar y elegir intercambios que tengan un historial de seguridad sólido y una buena reputación en la comunidad de criptomonedas es indispensable para la seguridad.

### 2. Autenticación de dos factores (2FA)

Habilitar la**autenticación de dos factores (2FA)**en todas las cuentas relacionadas con criptomonedas, carteras y plataformas de intercambio es otra medida de seguridad indispensable.

La 2FA agrega**protección adicional**al requerir un segundo factor para el ingreso. Generalmente, se trata de un código generado en tu dispositivo móvil, además de tu contraseña.

* **Métodos comunes de 2FA:**
  + Códigos de autenticación**:** Enviados a tu teléfono móvil.
  + Aplicaciones de autenticación**:** Como Google Authenticator o Authy.
  + Llaveros de seguridad: Dispositivos físicos que generan códigos únicos.

### 3. Actualización de software

Mantener actualizado el software y sistemas operativos es crucial para evitar posibles amenazas. Las**actualizaciones incluyen parches de seguridad**que protegen tu dispositivo contra vulnerabilidades conocidas.

### 4. Respaldo de clave privada

Es importante**guardar copias de tu clave privada en lugares seguros y fuera de línea**. La clave privada es esencial para acceder y controlar tus criptomonedas. Nunca se debe compartir con nadie.

### 5. Protección contra el phishing

Ser **cautelosos al abrir correos electrónicos y al hacer clic en enlaces** es una medida de seguridad indispensable. Los estafadores envían correos electrónicos de phishing que buscan engañar para que sus víctimas revelen los datos de inicio de sesión.

### 6-Wallets Frías: Tu Fortaleza Digital

Una wallet fría es un dispositivo de almacenamiento de criptomonedas que no está conectado a Internet. Esto significa que tus claves privadas, que son esenciales para acceder a tus fondos, están completamente aisladas de posibles ataques cibernéticos.

* **Tipos de Wallets Frías:**
  + Hardware wallets**:** Dispositivos físicos como el Ledger Nano S o Trezor, que ofrecen un alto nivel de seguridad.
  + Paper wallets: Impresiones físicas de tus claves públicas y privadas. Aunque son económicas, requieren un manejo cuidadoso para evitar daños.

|  |  |  |  |
| --- | --- | --- | --- |
| **Característica** | Plataforma con Verificación | |  | | --- | | Plataforma sin Verificación | |
| Ventajas |  |  |
| Rapidez | El proceso puede ser rápido una vez completada la verificación inicial. | Permite un acceso inmediato sin necesidad de validación. |
| Burocracia | Requiere cumplir con ciertos procedimientos administrativos. | Simplificada: no se requiere documentación adicional. |
| Anonimato | El anonimato es limitado, ya que solicita datos personales. | Mayor nivel de anonimato para los usuarios. |
| Seguridad | Alta: protege la información y las transacciones. | Baja: mayor probabilidad de usuarios malintencionados. |
| Soporte Técnico | Ofrece soporte técnico especializado. | Limitado o inexistente. |
| Cumplimiento de Regulaciones | Asegura el cumplimiento de normas legales y regulatorias | Puede operar al margen de regulaciones. |
| Desventajas |  |  |
| Riesgo de Fraude | Bajo: procesos de verificación reducen estas posibilidades | Alto: mayor exposición a estafas y actividades fraudulentas. |
| Garantías | Ofrece mayor garantía en servicios y transacciones. | Limitadas o nulas para los usuarios. |
| Tiempo y Esfuerzo | Requiere más tiempo para completar procesos de validación. | Baja inversión de tiempo y esfuerzo para registrarse. |
| Privacidad | Menor privacidad por la necesidad de compartir datos personales. | Mayor privacidad al no compartir datos sensibles. |