Billetera Virtual de Criptomonedas

Historial de cambios

Autor	Fecha	Versión	Descripción
Vanessa Aybar Rosales	12/08/2024	1.0	Documento inicial

Tabla de Contenido

1. Introducción

El presente documento tiene como objetivo detallar el análisis funcional para el desarrollo de una billetera virtual de criptomonedas. La solución propuesta busca proporcionar una plataforma segura y fácil de usar para gestionar activos digitales, realizar transacciones y acceder a diversas funcionalidades avanzadas. Esta billetera estará diseñada para satisfacer las necesidades tanto de usuarios novatos como experimentados en el ámbito de las criptomonedas.

2. Descripción General del Sistema

La billetera virtual será una aplicación que permitirá a los usuarios almacenar, enviar, recibir, comprar y vender diversas criptomonedas. El sistema garantizará la seguridad de los fondos mediante encriptación avanzada, autenticación de dos factores (2FA - Two Factor Authentication), y otras medidas de seguridad. Además, ofrecerá una interfaz intuitiva para que los usuarios puedan monitorear sus activos y realizar transacciones de manera sencilla.

Características principales

- Creación y gestión de cuentas de usuario con verificación de identidad.
- Soporte para múltiples criptomonedas (Bitcoin, Ethereum, Litecoin, entre otras).
- Funcionalidad para la compra y venta de criptomonedas utilizando monedas fiduciarias o de uso corriente (también conocido por su nombre en inglés “fiat”).
- Intercambio de criptomonedas dentro de la plataforma (swap).
- Envío y recepción de criptomonedas a través de direcciones públicas.
- Monitoreo de precios de criptomonedas en tiempo real.
- Generación de reportes financieros y fiscales.
- Historial completo de transacciones.
- Integración con métodos de pago tradicionales
- Servicio de soporte y asistencia al usuario disponible 24/7.

3. Funcionalidades del Sistema

3.1 Gestión de Cuentas de Usuario

Registro y autenticación: El sistema permitirá a los usuarios registrarse con sus datos básicos: nombres completos, apellidos, fecha de nacimiento, país donde desea operar, un e-mail y una contraseña segura. La autenticación de dos factores (2FA) será un requisito obligatorio, enviando un código al dispositivo móvil del usuario para acceder a la cuenta. En

principio el usuario podrá elegir como segundo factor de autenticación que se envíe un SMS a su número de teléfono móvil registrado ó a su casilla de e-mail.
Un requisito del área de Legales es que se registre además la aceptación de los términos y condiciones del uso de la billetera al momento de la registración.

Verificación de identidad: Para cumplir con las normativas de KYC (Know Your Customer), los usuarios deberán subir documentos de identidad oficiales y una fotografía reciente al momento de la registración. Solo los usuarios verificados podrán acceder a todas las funcionalidades de la billetera. Los documentos requeridos serán:

- una imagen de la cara anterior del DNI
- una imagen de la cara posterior del DNI
- una imagen del usuario sosteniendo el DNI

El sistema le ofrecerá al usuario la posibilidad de realizar este proceso luego de ingresar sus datos de registración básicos, ó de realizarlos posteriormente antes de poder realizar cualquier transacción en el sistema.

Configuración de seguridad: El sistema brindará a los usuarios la posibilidad de personalizar su experiencia de seguridad, incluyendo la opción de habilitar notificaciones de inicio de sesión que normalmente llegan a su casilla de e-mail y establecer 1 o más preguntas de seguridad adicionales.

Verificaciones adicionales: Periódicamente el sistema consulta a otro sistema externo (OFAC, Office of Foreign Assets Control), que verifica que el usuario de la billetera no se encuentre dentro de una lista de personas “inhabilitadas” por diversos motivos: ser PEP (persona políticamente expuesta) ó esté asociada a algún hecho ilícito, etc.

3.2 Gestión de Criptomonedas

Soporte para múltiples criptomonedas: Los usuarios podrán almacenar y gestionar diversas criptomonedas en sus cuentas. En todo momento el usuario podrá acceder al saldo asociado a cada criptomoneda, y al monto equivalente en moneda fiduciaria.

Visualización del saldo total (balance): El sistema proporcionará una vista consolidada del saldo de todas las criptomonedas en la cuenta del usuario, permitiendo visualizar el valor total en una moneda fiduciaria seleccionada por el usuario (si el usuario no especifica una moneda fiduciaria específica, se asume la moneda del país seleccionado al momento de la registración.

3.3 Compra y Venta de Criptomonedas

Compra de criptomonedas: Los usuarios podrán comprar criptomonedas utilizando su saldo en moneda fiduciaria. El sistema mostrará las tasas de cambio en tiempo real, las comisiones aplicables, y el monto total antes de que el usuario confirme la compra.

Venta de criptomonedas: Esta funcionalidad permitirá a los usuarios vender sus criptomonedas y recibir el valor equivalente en moneda fiduciaria, que luego podrá ser transferido a una cuenta bancaria o retenido en la billetera para futuras transacciones.

3.4 Intercambio entre Criptomonedas

Exchange interno (swap): Los usuarios podrán intercambiar diferentes criptomonedas dentro de la misma plataforma utilizando tasas de mercado actuales. A modo de ejemplo, un usuario que posee Litecoin podría cambiar al equivalente pero en Dogecoin. El sistema le mostrará el detalle de esta transacción, incluyendo las comisiones asociadas.

3.5 Envío y Recepción de Criptomonedas

Envío de criptomonedas: Los usuarios podrán transferir criptomonedas a otras direcciones de billeteras externas, simplemente necesita especificar la dirección del destinatario. Esta transacción podría o no ejecutarse de manera inmediata, depende de la blockchain que se use para registrar la transacción. Y la transacción generalmente tiene un costo de comisión que también depende de la blockchain. El usuario de la billetera generalmente no necesita saber toda esta información, simplemente cuando quiera enviar cripto se le ofrecerán las opciones de demora en envío con su costo y podrá elegir entre esas opciones.
Nuestra billetera consultará servicios externos para saber la información de demora y costos, pero deberá registrar la operación realizada con todo el detalle asociado.

Recepción de criptomonedas: Los usuarios recibirán criptomonedas en su dirección pública única generada por el sistema. El sistema notificará al usuario cuando se reciban fondos.

Por cada moneda cripto que el usuario posea, el sistema generará una dirección la cual quedará asociada a esa moneda para ese usuario. Es importante que el usuario indique con exactitud esta dirección cuando quiera recibir cripto.

3.6 DeFi (Decentralized Finance)

En el mundo cripto también existe algo parecido a los plazos fijos del mundo bancario tradicional, aunque con mayor volatilidad en cuanto a los intereses que pueden generarse, y de disponibilidad inmediata. En el mundo cripto estas opciones de DeFi se conocen como “protocolos”, entre los más conocidos se encuentran AAVE, Yearn, Compound, etc. Nuestra billetera consultará periódicamente los valores de intereses de cada protocolo para ofrecerlas a los usuarios. Una vez que un usuario coloca una cantidad determinada de sus cripto en un protocolo, ya no dispone de esa cripto para realizar otras operaciones, debiendo retirarla de DeFi para tenerla a disposición nuevamente.
Nuestra billetera virtual cobrará intereses por la colocación de nuestra cripto en DeFi así como por el retiro de los mismos.

3.7 Monitoreo de Precios en Tiempo Real

Integración con APIs de mercado: El sistema se integrará con APIs que proporcionan datos de precios en tiempo real. Los usuarios podrán configurar alertas de precios para ser notificados cuando una criptomoneda alcance un valor específico.

3.8 Generación de Reportes Financieros

Historial de transacciones: El sistema almacenará un historial detallado de todas las transacciones realizadas por el usuario, incluyendo compra, venta, intercambio, envío y recepción de criptomonedas.

Reportes fiscales: El sistema generará reportes de ganancias y pérdidas, incluyendo el costo base de adquisición, el valor de venta y cualquier ganancia o pérdida registrada, que podrán ser exportados en formatos como PDF o CSV.

3.9 Soporte y Asistencia al Usuario

Centro de ayuda: El sistema incluirá un centro de ayuda con respuestas a preguntas frecuentes, guías y tutoriales.

Asistencia 24/7: El soporte técnico estará disponible a través de chat en vivo, correo electrónico o llamada telefónica para resolver cualquier problema.

3.10 Tarjetas

Nuestra billetera virtual brinda la posibilidad de obtener una tarjeta de débito VISA, la cual estará asociada a una de nuestras criptomonedas, de modo que las transacciones que se realicen con la tarjeta en moneda fiduciaria, en realidad se realizarán en cripto y al monto equivalente de conversión al momento de la transacción.
Cuando un usuario quiere que se le otorgue una tarjeta de débito, debe aceptar términos y condiciones. Por cuestiones legales, esa aceptación debe quedar registrada.
Un usuario puede hacer uso de la tarjeta de débito siempre que tenga saldo en la tarjeta de débito elegida.

Existen planes a futuro de brindar la opción de tarjetas de crédito. En este caso, cuando se implemente, la billetera virtual será la que, en base a la calificación del usuario decida si puede o no operar con tarjeta de crédito o incluso inhabilitar luego de haber otorgado la tarjeta. También establecerá los límites máximos de crédito por usuario. Si bien esta opción no se encontrará disponible en el lanzamiento de la billetera, el sistema debe ser escalable para luego ser incorporado.

4. Casos de Uso

4.1 Registro de Nuevo Usuario

- Actor: Usuario
- Descripción: Un nuevo usuario desea registrarse en la billetera virtual.
- Flujo principal:
    1. El usuario accede a la pantalla de registro.
    2. Completa los campos obligatorios (correo electrónico, contraseña, etc.).
    3. El sistema envía un código de verificación al correo electrónico del usuario.
    4. El usuario ingresa el código para confirmar su cuenta.
    5. El sistema solicita al usuario completar su perfil y verificar su identidad.
    6. El usuario carga los documentos necesarios.
    7. El sistema verifica la identidad del usuario y habilita su cuenta.

4.2 Compra de Criptomonedas

- Actor: Usuario
- Descripción: Un usuario desea comprar criptomonedas utilizando una tarjeta de crédito.
- Flujo principal:
    1. El usuario selecciona la opción de compra de criptomonedas.
    2. Escoge la criptomoneda y el monto deseado.
    3. Selecciona la tarjeta de crédito como método de pago.
    4. El sistema muestra la tasa de cambio, la comisión y el monto final.
    5. El usuario confirma la compra.
    6. El sistema procesa la transacción y acredita la criptomoneda en la billetera del usuario.

4.3 Intercambio de Criptomonedas

- **Actor:** Usuario
- **Descripción:** Un usuario desea intercambiar una criptomoneda por otra dentro de la billetera virtual.
- **Flujo principal:**
    1. El usuario inicia sesión en su cuenta.
    2. Selecciona la opción de "Intercambio" en el menú principal.
    3. Escoge la criptomoneda que desea intercambiar y la criptomoneda que desea recibir.
    4. El sistema muestra la tasa de intercambio actual y la comisión aplicable.
    5. El usuario confirma la transacción.
    6. El sistema procesa el intercambio, deduce la cantidad especificada de la criptomoneda original y acredita la criptomoneda seleccionada en la cuenta del usuario.
    7. El sistema envía una notificación al usuario con los detalles de la transacción completada.

4.4 Retiro de Fondos a Cuenta Bancaria

- **Actor:** Usuario
- **Descripción:** Un usuario desea retirar fondos de su cuenta en la billetera virtual a su cuenta bancaria.
- **Flujo principal:**
    1. El usuario inicia sesión y accede a la sección de "Retiros".
    2. Selecciona la opción de "Retiro a cuenta bancaria".
    3. Elige la moneda fiduciaria y la cantidad que desea retirar.
    4. Selecciona la cuenta bancaria a la cual desea enviar los fondos (previamente vinculada).
    5. El sistema muestra las comisiones aplicables y el tiempo estimado para completar la transacción.
    6. El usuario confirma el retiro.
    7. El sistema procesa la transacción y notifica al usuario cuando los fondos han sido transferidos exitosamente.
    8. El usuario recibe una confirmación por correo electrónico con los detalles de la transacción.

5. Glosario de términos

1. Autenticación de Dos Factores (2FA): Una medida de seguridad adicional que requiere dos formas de verificación de identidad antes de conceder acceso a una cuenta. Normalmente, combina algo que el usuario conoce (como una contraseña) con algo que el usuario posee (como un código enviado a su dispositivo móvil).

2. Billetera Virtual: Aplicación o software que permite almacenar, enviar, recibir y gestionar criptomonedas. Funciona de manera similar a una billetera física, pero para activos digitales.

3. Criptomoneda: Activo digital diseñado para funcionar como un medio de intercambio, utilizando criptografía para asegurar las transacciones, controlar la creación de nuevas unidades y verificar la transferencia de activos. Una criptomoneda tiene un nombre asociado y además una sigla que lo identifica: Bitcoin -> BTC, Ethereum -> ETH, Dogecoin -> DOGE.

4. Clave Privada: Código criptográfico que permite al usuario acceder y gestionar sus criptomonedas. Es esencial mantenerla segura, ya que quien la posee tiene control total sobre los fondos asociados.

5. Clave Pública: Código criptográfico que se comparte públicamente y se utiliza para recibir criptomonedas. Es la dirección a la cual otros pueden enviar criptomonedas.

6. Clave Virtual Uniforme (CVU): Es un identificador único asignado a cada cuenta dentro del sistema de la billetera virtual. Similar al CBU (Clave Bancaria Uniforme) en el sistema bancario tradicional, el CVU permite a los usuarios realizar transferencias de dinero en moneda fiduciaria de forma rápida y segura dentro de la plataforma.

7. Fiat: Moneda fiduciaria emitida por un gobierno, como el dólar estadounidense, el euro o el peso argentino.

8. Know Your Customer (KYC): Proceso mediante el cual una empresa verifica la identidad de sus clientes para cumplir con regulaciones legales y prevenir actividades ilícitas como el lavado de dinero. Incluye la verificación de documentos de identidad y la recopilación de datos personales.

9. API: Es el acrónimo de "interfaz de programación de aplicaciones" (Application Programming Interface). Se trata de un conjunto de reglas, protocolos y herramientas que permiten a diferentes programas de software comunicarse entre sí. Las API pueden considerarse como un contrato de servicio entre dos aplicaciones.

10. Transacción: Proceso mediante el cual se realiza un intercambio de criptomonedas entre usuarios o dentro de la billetera virtual. Cada transacción tiene un identificador único y se registra en el historial del usuario. Una transacción tiene un estado, que puede ser: Completada, pendiente, fallida.

11. Volatilidad: Medida de la fluctuación de los precios de un activo, en este caso, de las criptomonedas. La volatilidad indica el grado de variación en el precio de una criptomoneda a lo largo del tiempo, lo cual puede implicar un riesgo mayor para los inversores.

12. Blockchain:
Tecnología subyacente en la que se basan la mayoría de las criptomonedas. Haciendo una analogía con términos contables, es un libro mayor distribuido y descentralizado que registra todas las transacciones de manera segura y transparente.

6. Código de Ética Académica

Todos los estudiantes deben comprometerse a actuar con integridad y honestidad en todas las etapas del trabajo. Esto incluye, pero no se limita a:

- **Autoría Original:** Todos los diagramas UML, códigos, y cualquier otra producción académica presentada debe ser el resultado del esfuerzo individual o grupal, sin recurrir a fuentes no autorizadas.
- **Prohibición de Plagio:** Está estrictamente prohibido copiar, reproducir, o utilizar trabajos de otros sin el debido reconocimiento. Esto incluye copiar código de otras fuentes sin citar, o presentar el trabajo de otro estudiante como propio.
- **Colaboración Transparente:** Se entiende que cada miembro del equipo colabora y participa en el diseño de esta entrega, y por tanto puede responder por cualquier sección dentro de la misma.

7. Contenido de la entrega

La entrega incluye un archivo ZIP que contiene lo siguiente:

1. Diagrama de clases en UML (en formato imagen o PDF).

   Analice el enunciado propuesto y determine las clases que participan en la implementación de esta billetera virtual de criptomonedas.
   Para realizar el diagrama utilice alguna de las herramientas disponibles. Se sugiere https://app.diagrams.net/ (draw.io) aunque puede usar cualquier otra herramienta con la que se sienta cómodo.
   El diagrama debe indicar las clases con sus atributos y los métodos que hacen a la solución del problema. Su solución debería permitir luego realizar las operaciones indicadas en la especificación.

2. Diagrama de secuencia (en formato imagen o PDF), imagine una situación donde las clases propuestas colaboran para resolver un problema y realice el diagrama. No pueden aparecer menos de 3 clases participantes.
   a. adjuntar una breve descripción -no más de 2 líneas- de lo que se busca reflejar en el diagrama.
   b. adjuntar un pseudocódigo (no se está pidiendo código que compile, la intención es verificar a quien se está delegando y que información eventualmente enviarán para poder resolver el problema).

3. Un proyecto en eclipse que contenga al menos 4 clases de todas las propuestas en el diagrama, relacionadas entre sí, con sus métodos getters y setters, nada más. Todos deben estar ubicados en un paquete java. Considerando que algunas clases no serán entregadas, simplemente en caso de requerirse deje comentado la línea donde se encuentre asociada/referenciada.

4. Documentación HTML de las clases entregadas en el proyecto eclipse, usando javadoc. Debe usar no menos de 4 etiquetas javadoc.

Nota

1. En el caso del diagrama UML y el diagrama de secuencia, si se le dificulta el acceso a una herramienta de software, puede hacerlo en papel siempre y cuando se respete la notación requerida.
2. No será válido generar el UML a partir de clases Java vía un generador de diagramas.