

Revisión Técnica Formal (RTF)

Compra y venta de criptomonedas – Auto vinculación digital



Equipo de Trabajo

Berserkers

Docente

Robinson Coronado Garcia

Responsables

Alejandro Mesa Gómez

Jhon Janer Torres Restrepo

Hernán Javier Aguilar Cruz

Cristhian Javier González Rodríguez

Arquitectura de Software

Universidad de Antioquia

Medellín

2020

Tabla de Contenido

1. Generalidades	3
1.1. Introducción	3
1.2. Objetivos	3
1.2.1. General	3
1.2.2. Específicos	3
1.3. Herramientas de software	4
2. Presentación del proyecto	4
2.1. Nombre	4
2.2. Descripción	4
2.3. Objetivos	5
2.4. Alcance	5
2.5. Limitaciones	6
2.6. Fases	6
2.6.1. Análisis de requisitos	6
2.6.2. Diseño y Arquitectura	6
2.6.3. Programación	6
2.6.4. Pruebas	6
2.6.5. Documentación	6
2.6.6. Entrega	6
2.6.7. Mantenimiento	7
3. Identificación de los stakeholders	7
3.1. Listado	7
3.1.1. Primarios	7
3.1.2. Secundarios	7
3.2. Relación con el proyecto	8
4. Identificación y priorización de requisitos	9
4.1. Lista y descripción de los requisitos del proyecto	9
4.2. Lista y descripción de los requisitos No funcionales - Atributos de calidad	10
4.3. Ordenar los requisitos según el impacto de los objetivos del negocio	11
5. Presentación de las vistas de la arquitectura	14
5.1. Diagrama de estructura compuesta	14

5.2. Diagrama de paquetes	15
5.3. Diagrama de componentes	16
6. Identificación de escenarios	17
6.1. Listado de escenarios básicos para cubrir los atributos de calidad	17
6.2. Flujo básico	17
7. Diagrama de Despliegue	18
8. Diagrama de Clases	19
9. Referencias	20

1. Generalidades

1.1. Introducción

El presente documento contiene el diseño arquitectónico propuesto por *Berserkers* para el desarrollo de un sistema de “Compra y venta de Criptomonedas” como un proyecto académico para el curso *Arquitectura de Software* en el semestre 2020-1.

1.2. Objetivos

1.2.1. General

Proponer un diseño arquitectónico a partir de diagramas UML, válido para el desarrollo de un sistema software para la compra y venta de criptomonedas, procurando completar todos los criterios que son considerados necesarios para que dicho sistema pueda ser desarrollado, producido y desplegado de forma óptima como el uso de patrones y diferentes arquitecturas.

1.2.2. Específicos

- Proponer un diseño arquitectónico viable para el desarrollo del sistema software planteado.
- Aplicar los conocimientos adquiridos en clase para desarrollar este diseño.
- Plantear RF y RNF que permitan que los usuarios realicen sus actividades de la mejor manera posible.
- Generar diagramas que permitan mayor entendimiento de la arquitectura propuesta.

1.3. Herramientas de software

RTF:

- [Docs](#) by Google para realizar este documento.
- [Draw.io](#) para la elaboración de los diagramas.
- [Meet](#) by Google para reuniones de equipo.

Desarrollo:

- Python3
- Django
- Bootstrap
- MongoDB

2. Presentación del proyecto

2.1. Nombre

Breyta

2.2. Descripción

Breyta es una *Crypto Wallet* donde sus usuarios podrán crear una cuenta que les permitirá hacer transacciones (enviar/recibir) en la criptomoneda de su elección, por esto es posible tener una billetera para cada criptomoneda que se vaya a transaccionar y asociar todas esas billeteras a una misma cuenta en nuestra aplicación, gracias a esto nuestros usuarios podrán transaccionar en la criptomoneda de su preferencia sin salir de su cuenta, evidentemente el usuario también podrá consultar las transacciones y el saldo de cada una de sus billeteras, además de poder acceder al mercado de divisas proveído por la propia aplicación, donde se muestran las tasas de cambio actualizadas en tiempo real para que los usuarios además de enviar y recibir también puedan comprar y vender sus criptomonedas.

El factor diferencial de esta aplicación frente a las demás es que permite integrar varias billeteras a un mismo usuario y cuenta con un mercado interno para comprar y vender

criptomonedas. Esta información será actualizada mediante estudios y podrá ser visualizada con estadísticas.

2.3. Objetivos

- Crear billeteras de distintas criptomonedas.
- Asociar dichas billeteras a una sola cuenta de Breyta.
- Permitir a los usuarios hacer transacciones con sus billeteras, ya sea a otros usuarios o entre sus propias billeteras. (Ej: Transferir una cantidad de BTC a su billetera de ETH, haciendo el cálculo de equivalencia de la tasa de cambio actual).
- Implementar un mercado interno de criptomonedas dentro de la aplicación y que ésta funcione como una “Casa de Cambio” de dichas divisas.
- Desarrollar una interfaz rápida e intuitiva que permita el desarrollo de los objetivos anteriormente mencionados.

2.4. Alcance

La descentralización de las criptomonedas permite que nuestra aplicación pueda ser utilizada desde cualquier smartphone o computador con acceso a internet, la cuenta en nuestra app no almacenará datos personales de sus usuarios, por lo que el titular de cada una de las billeteras y también de la cuenta en nuestra app tendrá una identidad completamente anónima, solo verificada por nosotros a través de una clave privada y otra serie de verificaciones, para la compra de criptomonedas se permitirá pagar a través de paypal y se hará una consignación directamente a la “Casa de Cambio” de la aplicación, y al recepcionar todas esas compras en un mismo sitio permite que la compra sea completamente anónima porque la casa de cambio es quién se encarga de procesar dichas peticiones y transferir el dinero a las respectivas billeteras.

2.5. Limitaciones

Para optimizar el desarrollo de este proyecto (considerando que es algo meramente académico) y teniendo en cuenta que se tienen pocos conocimientos en Blockchain se simulará las transacciones a través de la base de datos MongoDB.

2.6. Fases

2.6.1. Análisis de requisitos

- Definir los objetivos (propósito) y alcance la aplicación
- Toma de requerimientos con el cliente (Nosotros mismos xd)
- Redacción de Historias de Usuario

2.6.2. Diseño y Arquitectura

- Definición de la arquitectura del proyecto
- Definición de tecnologías y herramientas a utilizar
- Análisis lógico y diagramación de la aplicación

2.6.3. Programación

- Desarrollo del proyecto

2.6.4. Pruebas

- Testing

2.6.5. Documentación

- Documentación del proyecto

2.6.6. Entrega

- Respectiva exposición y presentación al docente y compañeros de clase

2.6.7. Mantenimiento

- Soporte general al proyecto

3. Identificación de los stakeholders

3.1. Listado

3.1.1. Primarios

Clientes: Nosotros 4, dueños y responsables de esta aplicación/servicio/compañía

Accionistas: Ninguno por el momento

Proveedores: Ninguno

Personal interno (grupos de desarrollo)

Gestor del proyecto: Alejandro Mesa Gómez

Diseñador: Cristhian Javier González Rodríguez

Desarrolladores/Programadores:

- Jefe de Desarrollo: Jhon Janer Torres Restrepo
- Desarrolladores: Todos los demás integrantes

Tester: Hernán Javier Aguilar Cruz

3.1.2. Secundarios

Competidores: Otras aplicaciones/servicios de CryptoWallet

Entidades regulatorias:

- Estatales: Propias de cada país que regula el comercio de las criptomonedas basados en sus propias leyes.
- Operacionales: Ninguna más que el propio blockchain de cada moneda, que es descentralizado y no le pertenece a nadie, el cual por cuestiones prácticas será simulado usando MongoDB.

Usuarios: Personas interesadas en tener, comprar, vender y/o transferir criptomonedas.

Banca tradicional: Organizaciones que se ven afectadas por el funcionamiento de nuestra app.

3.2. Relación con el proyecto

Primarios: Aquí se ubican aquellos que se consideran fundamentales para la marcha de cualquier empresa, es decir, los que mantienen una relación directa y estrecha con los negocios. Hablamos, en este caso, de los clientes, los accionistas, los proveedores e incluso los trabajadores o el personal que integra los grupos de trabajo. [\[1\]](#)

Por eso mismo nos incluimos a nosotros mismos como clientes y dueños de la aplicación, como también lo hicimos dentro del “personal interno” (equipo de desarrollo)

Secundarios: Aquí encontramos a todos aquellos stakeholders que no participan directamente en las acciones ni en los procesos comerciales, como por ejemplo los competidores de nuestra marca, las fundaciones y ONGs, el Estado y las normas vigentes, los medios de comunicación, entre otros.

Pese a que estos últimos no tienen una vinculación directa con los negocios, no por ello están exentos de sufrir consecuencias derivadas de las decisiones que se tomen en el seno de las empresas. En este sentido, incluso las comunidades o las sociedades en general se consideran ejemplos de stakeholders. [\[1\]](#)

Aquí incluimos a los competidores, que como son tantos no pusimos nombres propios de ninguno de ellos, las entidades regulatorias que en el caso de Colombia serían la DIAN, la Superintendencia de Industria y Comercio, los usuarios de nuestra app y la banca tradicional que se vería “afectada” por la operación de nuestra aplicación ya que los usuarios tendrán una nueva posibilidad de manejar su dinero.

4. Identificación y priorización de requisitos

4.1. Lista y descripción de los requisitos del proyecto

HISTORIAS DE USUARIO

Como un [rol]	Quiero [Característica]	Para [Razón]
Usuario	Poder registrarme en la plataforma	Tener acceso a mis billeteras de criptomonedas
Usuario	Ver mis billeteras	Saber cuanto saldo tengo en cada una
Usuario	Comprar criptomonedas con dinero real	Realizar transacciones a otros usuarios de forma anónima
Usuario	Vender mis criptomonedas	Obtener dinero real
Usuario	Cambiar mi saldo entre criptomonedas	Realizar transacciones con distintas divisas de ser necesario
Usuario	Ver las tasas de cambios	Saber si es buen momento para comprar o vender
Usuario	Transferir dinero a otros usuarios	Realizar pagos por bienes y/o servicios
Usuario	Vincular mis billeteras existentes	Administrarlas desde la plataforma
Usuario	Poder eliminar mi cuenta	Darme de baja en caso de alguna eventualidad
Administrador	Visualizar un reporte de las	Conocer el rendimiento de la

	transacciones realizadas por los usuarios respecto a compra y venta en la plataforma	aplicación
Administrador	Visualizar un reporte de las transacciones realizadas entre billeteras, inspeccionando el bloque actual	Obtener estadísticas del movimiento de divisas dentro de la plataforma
Usuario	Visualizar estadísticas relacionadas a las criptomonedas dentro de la plataforma	Conocer cuales son las divisas más populares dentro de la aplicación.

4.2. Lista y descripción de los requisitos No funcionales - Atributos de calidad

En esta aplicación se tendrán en cuenta los siguientes atributos de calidad

- Usabilidad
- Seguridad logística y de datos
- Performance
- Integridad de los datos
- Responsiveness
- Robustez

Usabilidad: El manejo de la aplicación contempla estrategias para su facilidad de uso, garantizando que el usuario pueda entender y acceder a las diferentes funcionalidades a través de una interfaz gráfica intuitiva.

Seguridad logística y de datos: Al ser una aplicación que maneja dinero, la aplicación garantizará un nivel de seguridad que genere confianza a los usuarios y les permita realizar sus transacciones de forma anónima.

Performance: Se tendrá un enfoque importante en el rendimiento de la aplicación, haciendo un buen uso y optimización de los recursos para garantizar que las transacciones se realicen en el menor tiempo posible.

Integridad de los datos: Se verificará que los atributos a trabajar deba ser exacta, completa, homogénea y sólida. Esto, para evitar cruces entre transacciones, intercambios realizados de manera no precisa, o información enviada de manera incorrecta. Así mismo, respetar los procesos a utilizar en la aplicación para considerar la misma una segura.

Responsiveness: La aplicación se debe adaptar a las plataformas presentadas. El diseño web buscado es tal que se pueda ver la misma interfaz de la página en diferentes dispositivos, en este caso para celulares y computadores.

Robustez: Estará en la capacidad de continuar su operación ante cualquier eventualidad o ataque, teniendo como prioridad garantizar la integridad de las cuentas de los usuarios y sus billeteras.

4.3. Ordenar los requisitos según el impacto de los objetivos del negocio

1. Poder registrarme en la plataforma:
 - [RF] Crear una función o método que permita guardar la información de la persona que está ingresando y comprobar si es correcta.
 - [RNF] Tener en cuenta el caso de error en el registro para que sea intuitivo y de manera lógica poder enseñarle al usuario si existe un fallo en el proceso.
2. Ver mis billeteras:
 - [RF] El usuario podrá revisar sus billeteras mediante la ID del mismo, con la cual se proporciona información de las billeteras que tiene la cuenta.
 - [RNF] Generar un ambiente agradable para la vista del usuario, que sea intuitivo y cómodo a la vista, para que sea más claro el uso de las billeteras.
3. Transferir dinero a otros usuarios

- [RF] El sistema realiza un proceso en el que permite transferir dinero mediante un código en el intercambio.
 - [RF] Se verifica si existe el dinero a transferir de primera mano, y si el usuario al cual se quiere hacer la transferencia está en el sistema.
 - [RNF] Se utilizan patrones para controlar la seguridad de los datos y la integridad de los mismos. En este caso, para controlar fallos al momento de hacer una transacción.
4. Vincular mis billeteras existentes
- [RF] Los usuarios pueden hacer uso de otras billeteras creadas anteriormente mediante su cuenta.
5. Comprar criptomonedas con dinero real
- [RF] El usuario realiza la compra de criptomonedas mediante la plataforma, de tal manera que se revise si tiene el monto del dinero total, y cuál sería el cambio a criptomonedas.
 - [RNF] Se realiza una interfaz en la que el usuario pueda visualizar de manera clara qué criptomonedas están disponibles y a qué precio.
6. Vender mis criptomonedas
- [RF] El usuario realiza la venta de criptomonedas en la plataforma.
 - [RNF] Se garantiza de que se pueda hacer la transacción para vender las criptomonedas del usuario, y se notifica si se realiza la misma.
7. Cambiar mi saldo entre criptomonedas
- [RF] El usuario revisa el valor de las criptomonedas y decide si quiere cambiar su saldo. Se revisa si la operación se puede realizar.
8. Ver las tasas de cambios
- [RF] Se provee información al usuario sobre las criptomonedas y su cambio.
9. Poder eliminar mi cuenta
- [RF] El usuario puede eliminar su cuenta si así lo desea.
 - [RNF] Se genera una vista en donde se le hace claridad al usuario si desea eliminar su cuenta, y de ser así, notificarle si lo hizo.
10. Visualizar un reporte de las transacciones realizadas por los usuarios respecto a compra y venta en la plataforma
- [RF] El usuario puede ver la información de su cuenta en donde se tiene un informe de las transacciones hechas por él, utilizando su ID y el tipo de transacción que se ha hecho para hacer un recuento de las mismas.

11. Visualizar un reporte de las transacciones realizadas entre billeteras, inspeccionando el bloque actual

- [RF] Se utiliza el bloque para verificar las transacciones entre billeteras y así mismo genera un reporte.

12. Visualizar estadísticas relacionadas a las criptomonedas dentro de la plataforma

- [RF] Se generan estadísticas mediante estudios con relación a las criptomonedas utilizadas en la plataforma, y se envían estos datos para dar uso de esta información en la plataforma.

5. Presentación de las vistas de la arquitectura

5.1. Diagrama de estructura compuesta

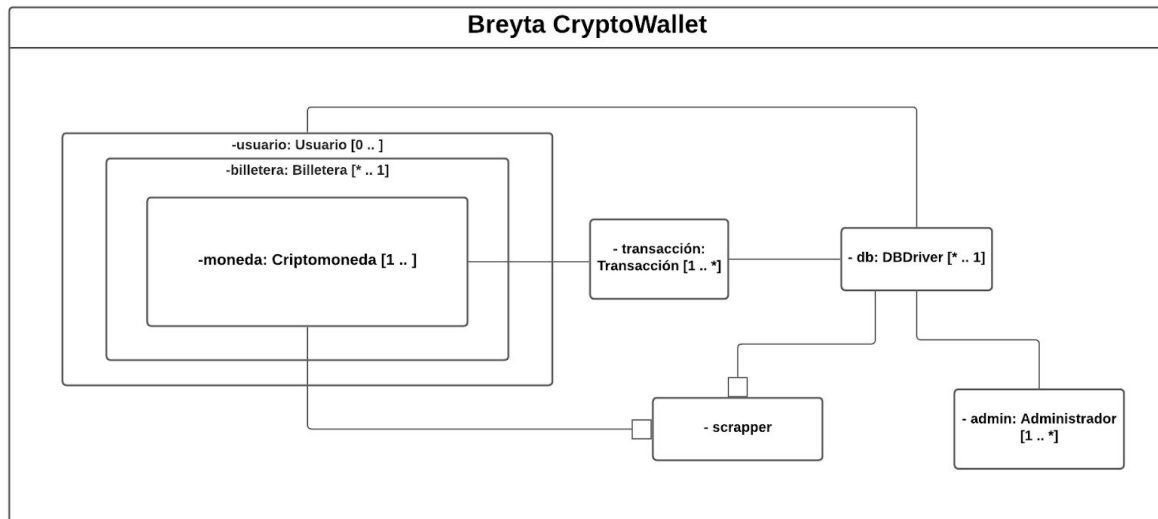


Figura 1: Diagrama de Estructura compuesta para la capa de modelo de negocio.

5.2. Diagrama de paquetes

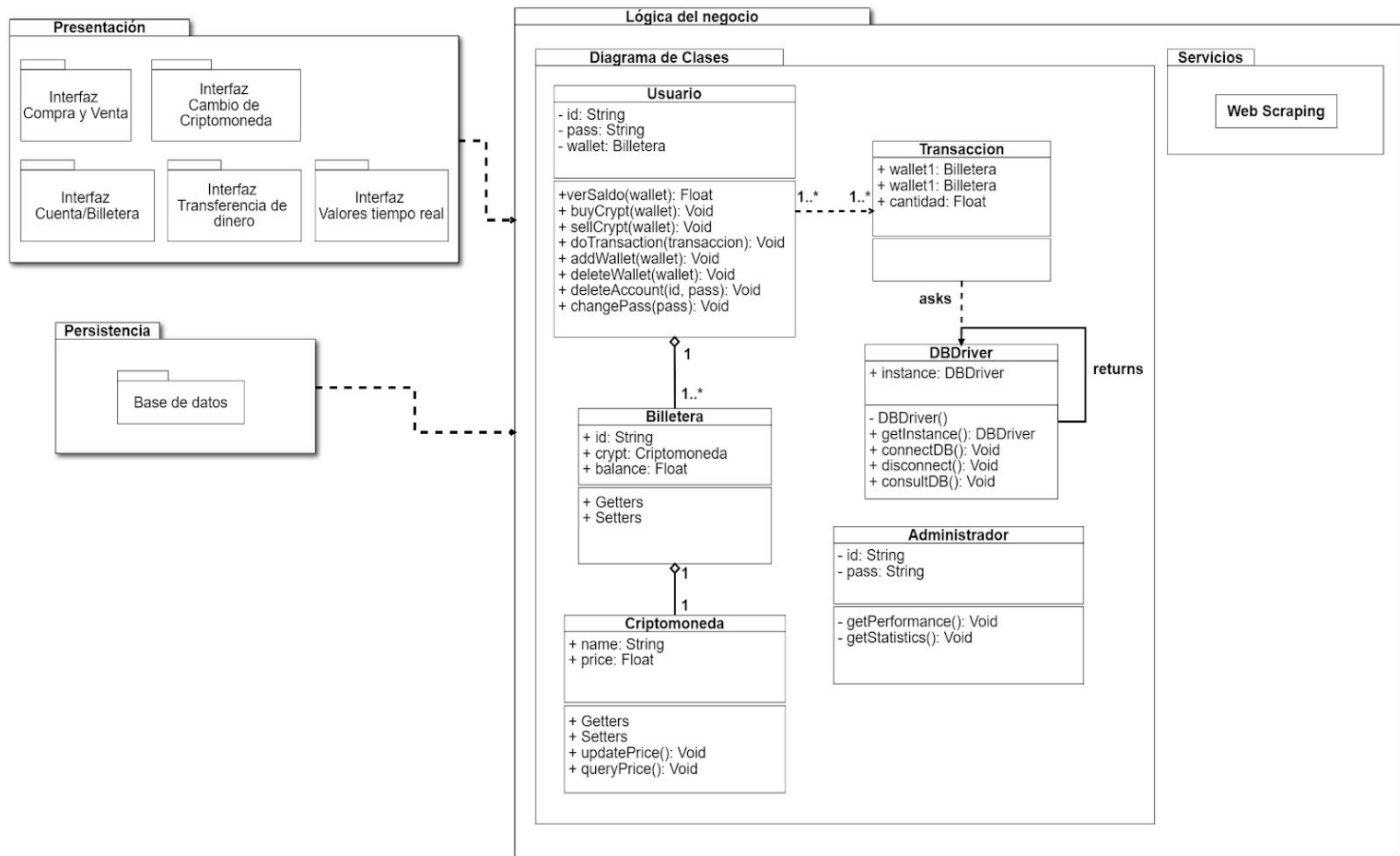


Figura 2: Diagrama de paquetes

5.3. Diagrama de componentes

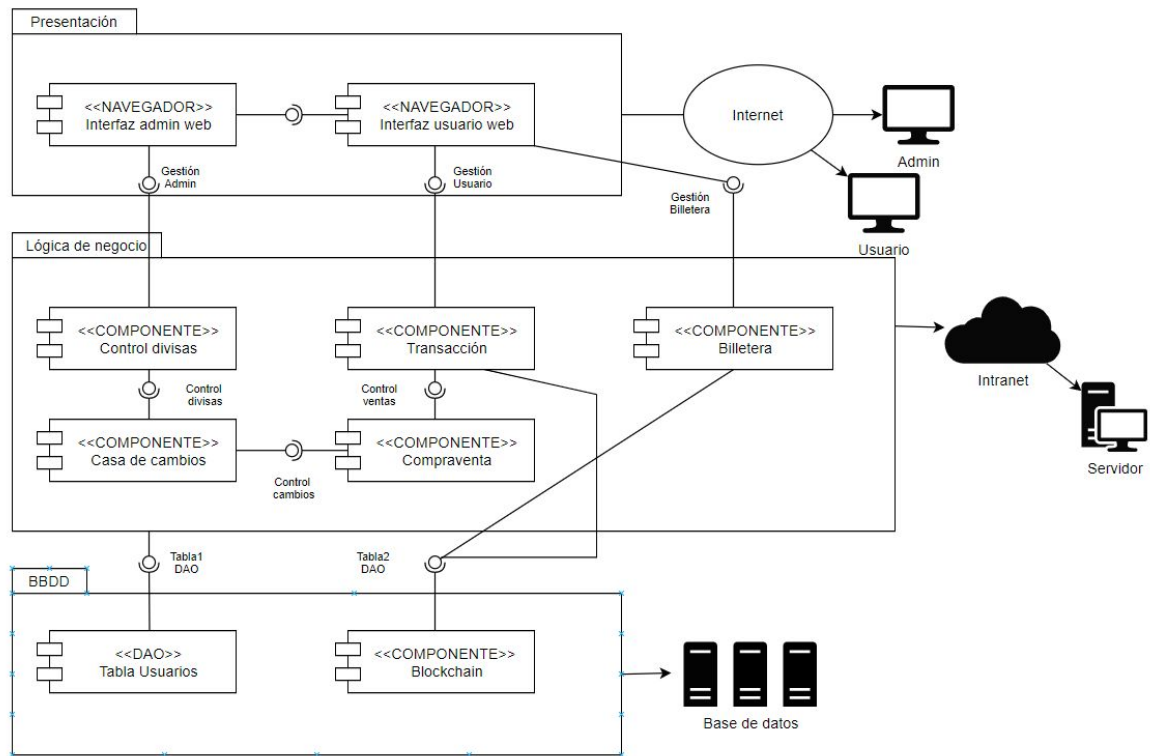


Figura 3: Diagrama de Componentes

6. Identificación de escenarios

6.1. Listado de escenarios básicos para cubrir los atributos de calidad

- El usuario podrá acceder a la aplicación a través de cualquier dispositivo inteligente con acceso a internet (app móvil) o computador (página web).
- El usuario podrá registrarse (crear una cuenta) de forma gratuita en la aplicación.
- La aplicación le permitirá al usuario crear una nueva *billetera* para la criptomoneda de su interés y agregarla a su cuenta.
- La aplicación deberá verificar la unicidad de cada billetera para evitar plagios o duplicación de las mismas.
- Cada cuenta tendrá una ID única asignada de forma aleatoria por la aplicación, por lo que se garantiza su unicidad y su imposibilidad de duplicación.
- Las tasas de cambio ofrecidas para la compra y venta de criptomonedas se actualizarán constantemente en tiempo real y serán acordes al mercado.
- Antes de realizar una transacción el sistema verificará que el usuario emisor tenga el saldo suficiente para efectuar dicha operación.
- La aplicación contará con todos los RNF expuestos anteriormente para que la experiencia del usuario sea la mejor posible.
- Como la billetera es independiente de la cuenta de nuestra aplicación un usuario podrá asociar a su cuenta billeteras creadas previamente como también podrá desvincular las billeteras creadas en la aplicación.

6.2. Flujo básico

1. El usuario accede a la página web o aplicación móvil de nuestra aplicación
2. El usuario se registra (Crea una cuenta)
3. El sistema le asocia una ID a dicha cuenta a través de algoritmos *SHA*
4. El usuario crea una *billetera* de alguna criptomoneda de su interés
5. El usuario podrá recibir criptomonedas en dicha billetera a través de transferencias o compra de las mismas.
 - El usuario podrá ver la tasa de cambio (precio) de las monedas disponibles para la venta
 - Si el usuario desea comprar criptomonedas deberá suministrar un medio de pago válido para la aplicación

6. El usuario podrá poner sus criptomonedas a la venta a través de la “Casa de Cambio” incorporada en la aplicación asumiendo los términos y condiciones de la misma (esto incluye la tasa de cambio)
7. El usuario podrá consultar el saldo de su(s) billetera(s)
8. El usuario podrá transferir criptomonedas a otros usuarios o a sí mismo entre sus propias billeteras

NOTA: Los pasos no enumerados en el flujo no distinguen ningún orden para su realización.

7. Diagrama de Despliegue

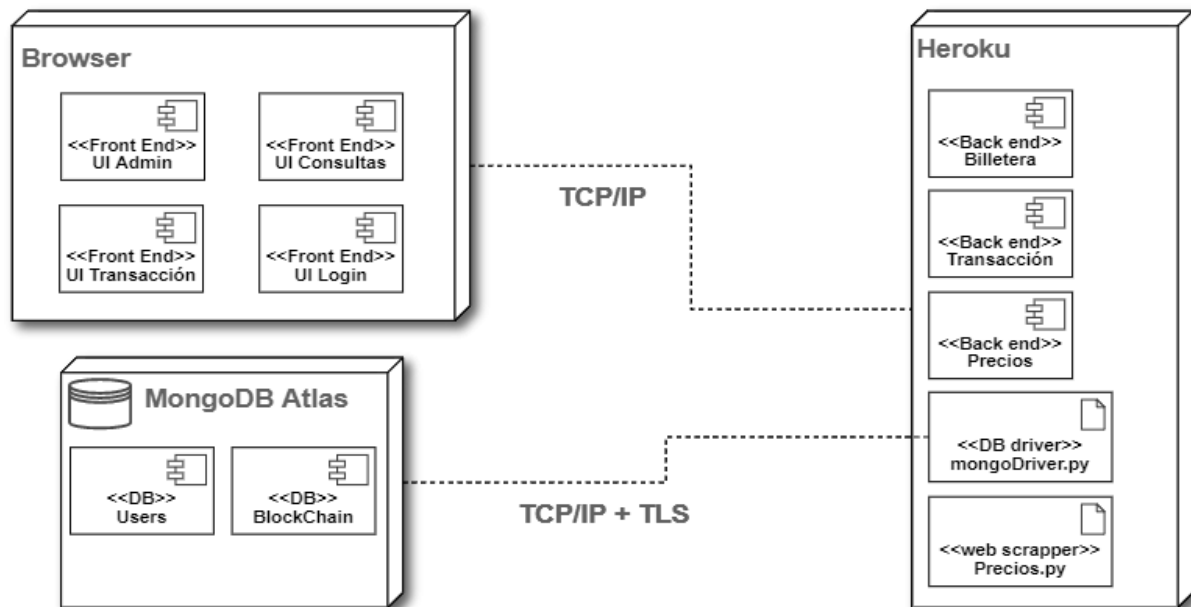


Figura 4: Diagrama de Despliegue.

8. Diagrama de Clases

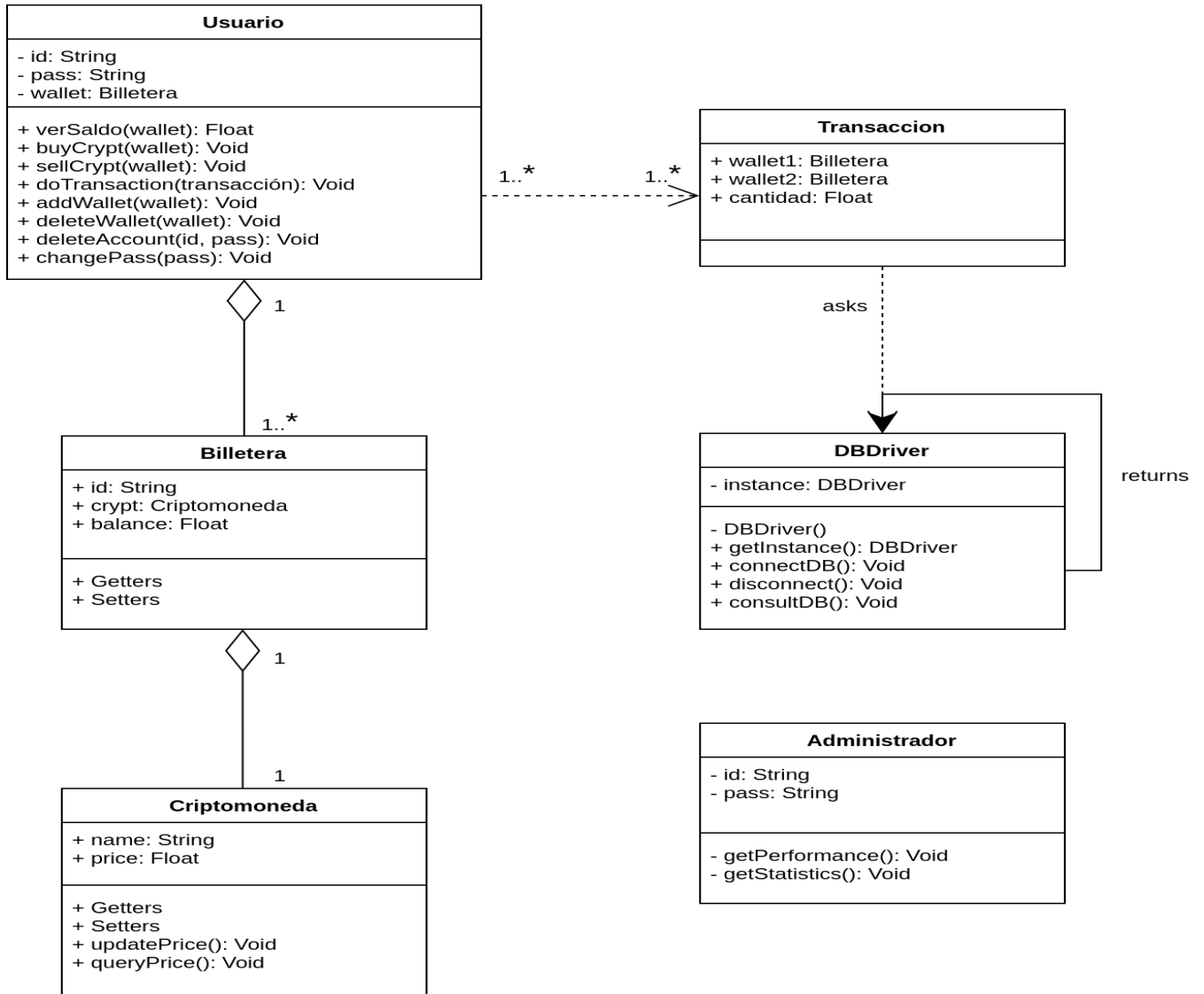


Diagrama 5: Diagrama de Clases.

9. Referencias

- [1] OBS Business School. (2017). *Stakeholders: Ejemplos Para Entender El Concepto*. From:
<https://obsbusiness.school/es/blog-investigacion/marketing-y-comunicacion/stakeholders-ejemplos-para-entender-el-concepto>