## 



Bitescom

10/06/2018

**─**

Franco Montes Alberto Daniel  
Hernandez Hernandez Cristian   
Nieves Guzmán Rodrigo Jehu  
Prieto de la Cruz Felipe

Profesora: Reyna Elia Melara Abarca

# Planteamiento del problema

Las criptomonedas es un tema que está causando gran interés alrededor del mundo y no en balde hay quienes dicen que es el nuevo oro, ya que ha estado cobrando gran relevancia en los últimos años donde las personas se han sumando a este ecosistema para averiguar si podría llegar a aportarles algo de valor.

Actualmente existen diversas monedas y cada una tiene un uso práctico distinto, entre las más populares están.

* Bitcoin: Es la primer criptomoneda creada además de la más popular y tiene un límite de 21 millones de unidades.
* Ether : Es la criptomoneda que se utiliza por los usuarios de la plataforma ethereum para realizar pagos a otros usuarios
* Litecoin: existen 84 millones de unidades y utiliza un script que facilita la minería para no requerir equipamiento sofisticado.

Lo que les aporta el valor a estas monedas virtuales es la oferta y la demanda de las mismas en donde también cae la confianza de los usuarios para seguir interactuando con ellas.

En general las criptomonedas tienen 3 características principales

1. **Son descentralizadas**: esto quiere decir que no están gobernadas, ni administradas por ninguna persona, entidad financiera o gubernamental.
2. **Tienen alcance internacional**: Permite que se realicen transacciones alrededor del mundo a través de internet.
3. **Utilizan principios de criptografía**: Esto lo hacen para garantizar la seguridad de las transacciones. La criptografía permite garantizar la autenticidad de las transacciones y controlar la creación de nuevas monedas.

Una pregunta frecuentes es ¿Cómo funciona el proceso de transferencia de cripto monedas? y la respuesta es que los procesos pueden llegar a variar entre las diversas criptomonedas o plataformas, aunque el más común es el siguiente:

Eliges una Exchange o casa de cambio que acepte la criptomoneda que quieres intercambiar, las exchange por lo regular te proporcionan una wallet con un id el cual debes de proporcionar a quien quiera realizarte una transferencia de criptomonedas.

También se pueden realizar distintas operaciones en un Exchange como lo son los fondeos de dinero real, las compras de criptomonedas, la venta de cripto monedas y los intercambios entre diferentes criptodivisas.

El problema con estas Exchanges es que no proporcionan suficiente información práctica para usuarios novatos como lo son las definiciones de criptodivisas, fluctuaciones, sugerencias de cuánto invertir en las temporadas actuales además de que no existe una comunidad activa incluida en ninguna Exchange que ayude o de soporte a los usuarios de las mismas.

Tratar de entrar a este ecosistema sin ningún conocimiento previo acerca de cryptocurrencies puede resultar difícil en la mayoría de las personas, por ello desisten en ser parte de este tema emergente. Esto ha causado que resulte complicado atraer a sectores de personas las cuales no tengan una estrecha relación con la tecnología o economía.

Por ello es necesario una plataforma dedicada a las poblaciones que desean estar en contacto con aquellas criptodivisas, sin necesidad de tener demasiados conocimientos técnicos sobre el tema y así dar cabida a una entrada más amigable a los usuarios, con respecto a estas nuevas tecnologías.

De no ser así no habrá una llegada de más usuarios que interactúen con las cryptocurrencies, esto ocasiona que la oferta y demanda se desestabilicen haciendo que el valor de las criptomonedas baje en gran medida ya que estas dependen en gran medida de las personas que invierten en ellas.

# Propuesta

Crear una Exchange dedicada a las personas que no tengan una estrecha relación con la tecnología o la economía, la cual facilite la información necesaria para que cualquier persona pueda utilizar estas monedas con recomendaciones prácticas de cómo y cuánto fondear, cuando debes de retirar y cómo elegir una cripto moneda.   
La Exchange de criptomonedas se pretende que sea la que los usuarios novatos utilicen por primera vez.

# Documento visión

# Stakeholders

Empresas que quieran invertir en las criptomonedas, personas que tienen amplio conocimiento en las finanzas relacionadas a este tema.

Nosotros los desarrolladores.

# Características

Casa de cambio de monedas virtuales donde podremos comprar, cambiar y vender de una manera fácil enfocada para principiantes en las criptomonedas.

# Alternativas y competencia

Bitso, Bitfinex, Bittrex, HitBTC, Binance, GDAX, Kraken, Poloniex, Bithumb

# Objetivos

* Brindar facilidad a los usuarios nuevos para el entendimiento de este ecosistema.
* Desarrollar un sitio web para permitir el intercambio de Cripto monedas a pesos mexicanos y viceversa.
* Interactuar con Interfaces de desarrollo bancarias para emitir transacciones de fondeo y retiro.

# Especificación de requerimientos Reglas de negocio

* El sistema no permitirá transacciones con campos obligatorios vacíos.
* Poner órdenes de compra o venta.
* Se podrá ver el historial de compras, ventas e intercambios realizados.
* El proceso de compras será el siguiente: solicitud de compra, creación de contrato inteligente, cerrar la transacción.

# Requerimientos funcionales

|  |  |  |
| --- | --- | --- |
| **id** | **Nombre** | **Descripción** |
| **REQF1** | Ver Ether | Visualizar la cantidad de *Ether* en el *Exchange* |
| **REQF3** | Ver Token | Visualizar la cantidad de *Token* en el *Exchange* |
| **REQF4** | Depositar Token | Depositar *Tokens* desde la extensión de *MetaMask* al *Exchange* |
| **REQF5** | Depositar Ether | Depositar E*ther* desde la extensión de *MetaMask* al *Exchange* |
| **REQF6** | Retirar Tokens | Retirar *Tokens* de la página y posteriormente se depositarán en la *Wallet* |
| **REQF7** | Retirar Ether | Retirar *Ether* de la página y posteriormente se depositarán en la *Wallet* |
| **REQF8** | Comprar Token | Realizar orden de compra de *Token* en la *Exchange* |
| **REQF9** | Vender Token | Realizar orden de venta de *Token* en la *Exchange* |
| **REQF10** | Enviar *Token* | Enviar *Token* a otro usuario usando su *dirección de usuario* |

# Requerimientos no funcionales

|  |  |
| --- | --- |
| **Id** | **Descripción** |
| **REQNF1** | Se usará el framework Truffle en su versión 6.1.0 para el desarrollo del sistema. |
| **REQNF2** | Las pruebas del sistema se realizarán en una red privada con la herramienta TestRPC. |
| **REQNF3** | Se utilizará MetaMask para gestionar las cuentas. |
| **REQNF4** | Se mostrarán los datos de la cuenta activa en todas las páginas dentro del exchange, como lo es la dirección de la cuenta activa y la dirección del Exchange. |
| **REQNF5** | La interacción entre el sistema y el usuario será por lo general a través de botones de acción y campos de texto. |
| **REQNF6** | La interfaz gráfica del sistema deberá ser sencilla y estará separada por secciones intuitivas, debido a que facilita su comprensión. |

# Especificación de casos de uso

Casos de uso:

Caso 1: Iniciar sesión correctamente en tu cuenta.

El usuario ingresará su id y su contraseña en la interfaz exchange login.

En el caso de que el usuario no se acuerde de la contraseña, debe haber una opción que le enviará un correo con los pasos a seguir para recuperarla.

Lo mismo si se le olvida su ID

Cuando se ingrese un usuario este se debe validar que se encuentre en la base de datos, de lo contrario usar los casos de la alternativa A.

Alternativa A:  
Si no se encuentra el usuario en la base de datos:

-Debe crear una cuenta.

-No permitir la conexión.

Crear una cuenta

Comprobar los datos personales de la cuenta

Depositar/recibir fondos en monedas fiduciarias

Retirar ...

Depositar/recibir fondos en criptomonedas

Retirar …

Emitir orden de compra de divisa

… de venta …

Visualizar gráfico de precio

CU 2 CREAR UNA CUENTA  
PRECONDICIÓN El usuario ha ingresado al home del sitio y ha hecho clic en el botón Crear cuenta  
DESCRIPCIÓN El Sistema deberá comportarse como se describe en el siguiente caso de uso cuando el usuario del Sistema solicite crear una cuenta  
Secuencia Paso Acción  
 1 El usuario solicita al Sistema comenzar el proceso de crear una cuenta   
 2 El Sistema solicita al usuario los datos correspondientes a:  
• Correo electrónico  
• Nombre  
• Apellidos  
• Fecha De Nacimiento  
• País  
• Número de Celular  
 3 El usuario proporciona al Sistema los datos mencionados en el paso anterior   
 4 SI los datos proporcionados coinciden con una cuenta registrada,  
 4. 1 Se realiza el caso de uso recuperar cuenta  
 5 El Sistema solicita al usuario los datos correspondientes a:  
• Contraseña  
• PIN de seguridad  
 6 El usuario proporciona al Sistema los datos mencionados en el paso anterior  
 7 El Sistema informa que el usuario se ha registrado correctamente  
POSTCONDICIÓN El usuario del Sistema se ha creado una cuenta y el Sistema ha registrado los datos asociados en el paso 2 y 5.   
  
   
  
CU 3 CONSULTAR LA CARTERA  
PRECONDICIÓN El usuario ha proporcionado los datos de identificación para acceder a su cuenta y estos han sido validados por el Sistema  
DESCRIPCIÓN El Sistema deberá comportarse como se describe en el siguiente caso de uso cuando el usuario del Sistema solicite una consulta de su cartera  
Secuencia Paso Acción  
 1 El usuario solicita al Sistema comenzar el proceso de consultar su cartera   
 2 El Sistema tendra que mostrar al usuario:  
  
• El equivalente en pesos al valor total de sus criptomonedas más los fondos no invertidos en criptomonedas  
• El monto total de los fondos no invertidos  
• El monto total de sus fondos en Ethereum  
  
  
   
 3   
Si el usuario decide hacer un depósito para fondear su cuenta en pesos.  
 3.1 Se realiza el caso de uso Realizar depósito para fondear en pesos  
 4 Si el usuario decide hacer un depósito para fondear su cuenta en Ethereum  
 4.1 Se realiza el caso de uso Realizar depósito para fondear cuenta en ethereum  
 5 Si el usuario decide hacer un retiro de su cuenta en pesos.  
 5.1 Se realiza el caso de uso Retirar Pesos  
 6 Si el usuario decide hacer un retiro de su cuenta en Ethereum   
 6.1 Se realiza el caso de uso Retirar Ethereum  
 7 Si el usuario decide convertir Pesos en Ethereum   
 7.1 Se realiza el caso de uso Convertir pesos a Ethereum  
  
   
CU 4 FONDEAR EN PESOS  
PRECONDICIÓN El usuario ha accedido a su cartera digital y ha solicitado depositar fondos en pesos mexicanos  
DESCRIPCIÓN El Sistema deberá comportarse como se describe en el siguiente caso de uso cuando el usuario del Sistema solicite realizar un fondeo de su cuenta en pesos  
Secuencia Paso Acción  
 1 El usuario solicita al Sistema comenzar el proceso de Depositar fondos en pesos mexicanos a su catera  
 2 El Sistema tendra que mostrar al usuario las siguientes opciones para realizar el fondeo de su cartera en pesos mexicanos  
  
• Transferencia vía SPEI   
• Depósito en efectivo  
 3 El usuario elige una opción para depositar fondos en su cartera  
 4 Si el usuario elige la opción de Transferencia vía SPEI  
 4.1 El Sistema le muestra en pantalla una CLABE, nombre del beneficiario y Banco receptor para realizar el depósito   
 4.2 El usuario toma los datos y realiza un depósito en su plataforma de banca en línea  
  
 4.3 El Sistema confirma la transferencia del depósito y actualiza los fondos no invertidos en pesos según la cantidad depositada  
 5 Si el usuario elige la transferencia por Depósito en Efectivo  
 5.1 El Sistema muestra un numero de Cuenta OXXO PAY  
 5.2 El usuario toma los datos y realiza el depósito a la cuenta generada por el Sistema  
  
 5.3 El Sistema confirma la transacción y actualiza los fondos de la cartera del usuario  
  
   
CU 5 FONDEAR EN ETHER  
PRECONDICIÓN El usuario ha accedido a su cartera digital y ha solicitado depositar fondos en Ethereum  
DESCRIPCIÓN El Sistema deberá comportarse como se describe en el siguiente caso de uso cuando el usuario del Sistema solicite realizar un fondeo de su cuenta en Ethereum  
Secuencia Paso Acción  
 1 El usuario solicita al Sistema comenzar el proceso de Depositar fondos en Ethereum  
 2 El Sistema muestra en pantalla una dirección Ethereum y un código QR correspondiente a la dirección para el depósito de fondos  
 3 El usuario realiza la transferencia   
  
 4 El Sistema confirma la transacción y actualiza los fondos de la cartera del usuario

CU 6 Venta de TOKEN

PRECONDICIÓN: El usuario debe de estar logeado y con fondos en ether

DESCRIPCIÓN: El Sistema deberá comportarse como se describe en el siguiente caso de uso cuando el usuario del Sistema solicite realizar un intercambio entre ether a bitcoin

secuencia Paso Acción

1 El sistema solicitará el nombre simbólico de la criptomoneda

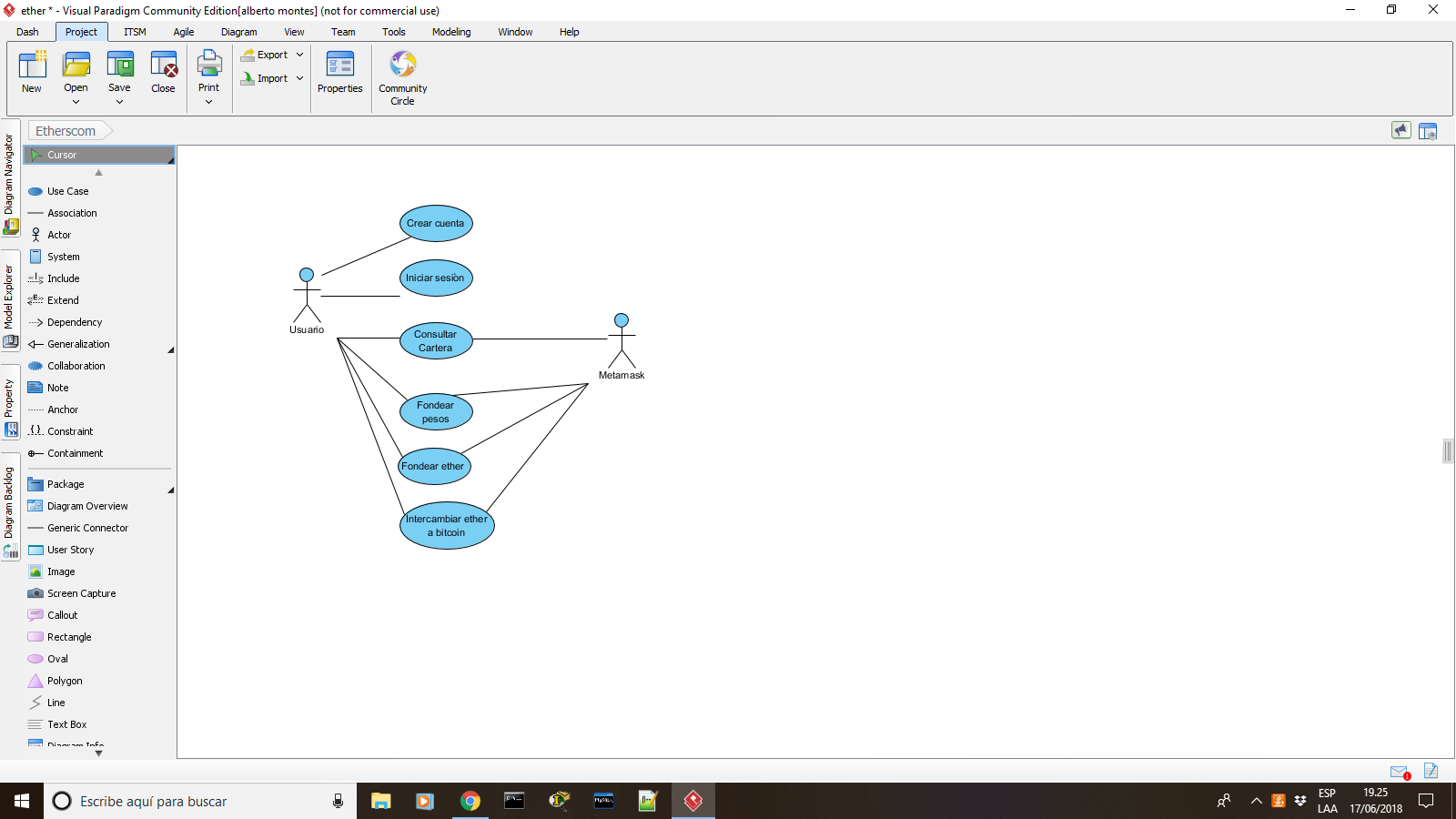
2 El sistema solicitará la cantidad de TOKENS que deseas vender

3 El sistema pide la cantidad de GAS que deseas utilizar para la transacción

5 Pulsar botón vender

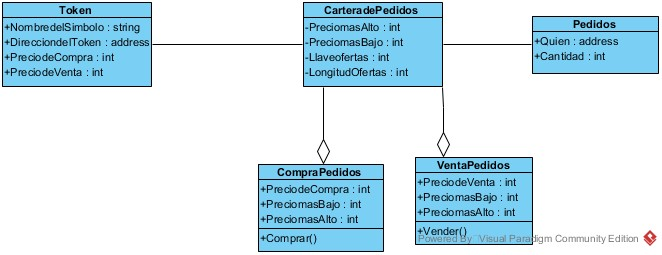
6 Si la información es correcta se mostrará la orden de venta en la UI009

# Diagrama general de casos de uso



# Diseño

# -Diagrama de clases

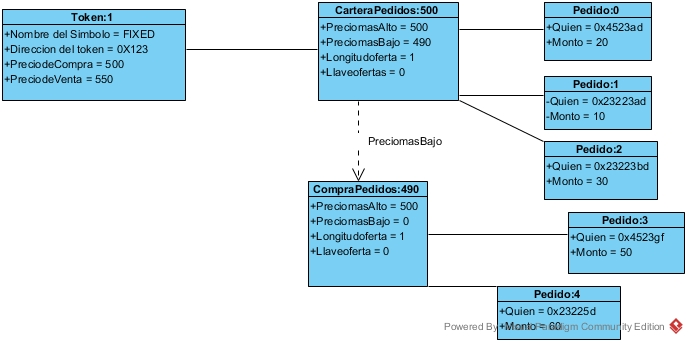


# 

# Clases propias del software implementadas del proyecto

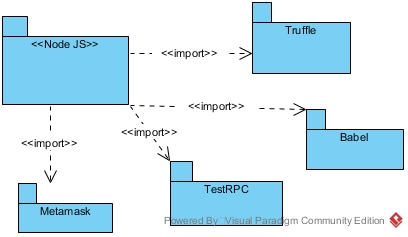
Token, CarteraPedido, CompraPedido, VentaPedido, Pedido

# Diagrama de objetos

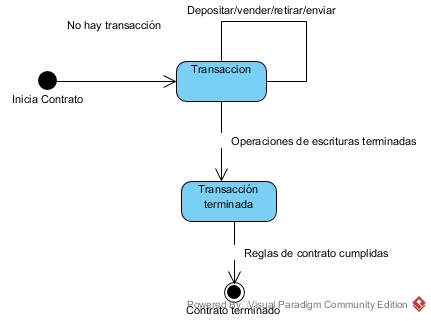


# Diagrama de interacción: DSS, de secuencia y de comunicación

# Diagrama de Paquetes



# Diagrama de máquina de estados



# Arquitectura propuesta y su justificación

¿Modelo mvc o descomposición modular?

Diagrama de componentes, los implementados propiamente para el proyecto o los relevantes

# Diagrama de despliegue

# Diagrama de Entidad Relación (Este lo podemos sustituir por uno de la blockchain )

# Interfaces gráficas del sistema y los diagramas que ilustran la navegación entre interfaces

# **GLOSARIO**

**Cuenta** **Metamask**: Es una cuenta simulada con un identificador de usuario que se utiliza para depositar o retirar

**Dapps**: Descentralized apps (Aplicaciones Descentralizadas)

**Dirección de usuario**: Es una clave única que identifica al usuario. Esta se usa para hacer transferencias

**Ether**: Criptomoneda de ethereum

**Ethereum**: Plataforma descentralizada, permite la creación de contratos inteligentes basado en el modelo blockchain

**Gas**: Costo que tiene al realizar una operación o conjunto de operaciones en la red de Ethereum, por lo general se utilizan las unidades **WEI** o **GWEI** (GIGA WEI)

**Metamask**: Es una extensión de google chrome que funciona para simular una wallet y sus cuentas

**Orden**: Petición que espera una respuesta

**Token**: Representa una criptomoneda

**Wallet**: Es una cartera digital que puede guardar criptodivisas

**Wei**: Unidad de Ether, equivale a 1/1,000,000,000