

UNIVERSIDAD PERUANA DE CIENCIAS APLICADAS



ASIGNATURA:

Matemática Computacional

SECCIÓN: SV42

CICLO: 2020-01

TEMA:

Informe de trabajo parcial

DOCENTE:

Luis Alberto Iquise Mamani

INTEGRANTES:

Mario Piero Arroyo Camacho	u201610533
Gonzalo Sebastian Laqui Chalan	u201712153
Sebastian Diaz Torres	u201717471
Gerardo Huaman La Cruz	u201817801
Daniel Monteagudo Carrión	u201811322

Índice

1._ Introducción

2._ Objetivos

3. _ Fundamento teórico

3.1 ¿Qué es una criptomoneda?

3.2 Arquitectura base de una criptomoneda

3.3 Criptomonedas del mercado actual

3.4 Temas propuesto para el desarrollo de la criptomoneda

4._ Resultados

4.1 Idea Concebida para programar

4.2 Diagrama de clases

4.3 Diseño de interfaz

5._ Bibliografía

1. Introducción

Hoy en día satisfacemos la adquisición de cualquier producto mediante la compra de este, ya sea con una tarjeta, un billete, entre otros, sin embargo, sólo pocos son efectuados con una moneda virtual. Existen diferentes formas de efectuar una compra con una moneda virtual, entre las más importantes está: Bitcoin.

Bitcoin es una moneda virtual con una estructura y alcance desigual a las monedas físicas que todos conocemos, puesto que, casi el 100% de este, no está controlado por ningún Estado, institución financiera, banco o empresa. Su propósito reside en actuar de la misma manera que el dinero físico, pero mejor, ya que ofrece una seguridad de alta.

La filosofía del bitcoin tiene su origen en 2009, cuando Satoshi Nakamoto la creó con el objetivo de que esta fuese utilizada para hacer compras únicamente por internet de manera anónima.

2. Objetivos

Al finalizar este proyecto, nuestro grupo deberá lograr los siguientes objetivos:

- Demostrar el funcionamiento de una criptomoneda
- Crear una criptomoneda utilizando los conceptos aprendidos
- Aprender sobre manejo del blockchain
- Conocer más sobre el dinero digital, sus transacciones y sus funcionamiento.
- Aplicar conocimientos adquiridos de Matemática Computacional
- Implementar el proyecto en el lenguaje C++

3. Fundamento teórico

3.1 ¿Qué es la criptomoneda?

Son monedas que pueden ser intercambiadas o usadas al igual que las demás monedas (euro, dólar, etc) pero su principal diferencia es que estas son digitales y utilizan criptografía. Es decir, no pueden ser falsificadas. Otro punto a favor es que, el intercambio de estas monedas se hace directamente con el usuario destino, ya que son totalmente independientes y no existen terceros en este proceso.



Como todo software avanzado, las criptomonedas cuentan con una arquitectura sólida. Conformado por una red informática P2P, que según Ramón Jesús Millan Tejedor es “una red que no tiene clientes y servidores fijos”, es decir, la comunicación entre computadoras a través de la red, para ciertas tareas, se efectúan sin la necesidad de un usuario la mayor parte del tiempo; asimismo teniendo como resultado, la simulación de un servidor por parte de las computadoras. La criptografía también forma parte de su arquitectura, se trata de un nivel de protección que va más allá de la forma en cómo nos comunicamos los seres humanos; su función principal es evitar la modificación de datos de valor, por parte de los usuarios, por medio de algoritmos complejos y métodos matemáticos.

3.2 Arquitectura base de una criptomoneda

¿Qué es Blockchain?

Conocido en español como “cadena de bloques” , es un registro único, consensuado y distribuido en nodos en la red. En cada nodo podemos encontrar cadenas de bloques que contienen un registro con todas las transacciones realizadas, además de información del bloque anterior, del mismo y del bloque siguiente.

Es considerado de alta seguridad, ya que solo basta la disponibilidad de un bloque de esta cadena para acceder a toda la información de la misma, debido a que cada bloque guarda una copia de la cadena.



¿Qué es Encriptar?

Encriptar consiste en bloquear los datos mediante un código secreto que oculta un verdadero mensaje. De tal manera que si alguien accede a ellos, encontrará que la información carece de sentido. Existen dos tipos de cifrados: simétrico y asimétrico.

El cifrado simétrico es la técnica antigua, utiliza una clave secreta para cifrar los datos. Es decir, el remitente y el receptor conocen la clave. Por otro lado, el cifrado asimétrico es un método que es nuevo en implementar esta usa dos claves una pública y otra privada, las claves públicas permiten que cualquiera envíe información a otra persona, pero cada persona conoce su clave privada.



3.3 Criptomonedas del mercado actual

3.3.1 Bitcoin

El primer cliente software de código abierto para correr nodos de la moneda fue lanzado por Satoshi Nakamoto el 9 de enero de 2009 a través de la plataforma SourceForge. El programador Hal Finney es una de las primeras personas en adoptar, apoyar y contribuir a Bitcoin, además, descargó el software Bitcoin el día en que fue lanzado, y recibió 10 bitcoins de Nakamoto, lo cual fue también la primera transacción bitcoin del mundo.

Actualmente, es la criptomoneda más conocida y valorada en todo el mundo. Además, se le considera la criptomoneda pionera con respecto al mundo virtual. Su valor ha sido tan grande que convirtió en millonarios a muchos de sus propietarios. Actualmente, el valor de un Bitcoin equivale a 7,220.48 dólares. Sin embargo, su gran demanda le permitió el ascenso hasta los 21,000 dólares durante el 2017.



3.3.2 Ethereum

Fue desarrollada por el programador Vitalik Buterin en el año 2013. Es posiblemente la segunda criptomoneda más conocida en el mundo virtual. Es la mejor alternativa del Bitcoin, ya que también permite realizar transacciones de manera rápida y sencilla. Ether, como las demás criptomonedas, no cuenta con reconocimiento alguno de la gran mayoría de los países. Por lo tanto no tienen el estatus de moneda de curso legal ni de bien o cosa transferible.



3.3.3 Litecoin

Lanzada en el año 2011 por , el ex-trabajador de Google, Charlie Lee. Es conocida como la hermana pequeña de las criptomonedas.



Además, es la más utilizada por las personas que tienen menos experiencia en el trading, ya que tiene un uso simple y sencillo.

3.3.4 XRP

Fundada por la empresa Ripple Labs en el año 2012. Anteriormente, se le conocía por el nombre “Ripple” o “Ripple credits”. Es la criptomoneda favorita de los bancos, ya que les permite realizar una transacción a cualquier banco del mundo en menos de 10 segundos.



3.3.5 Dogecoin

Fue creada por el programador, y antiguo ingeniero de IBM, Billy Markus en el año 2013. Es una criptomoneda derivada de Bells, que tiene como imagen al perro Shiba Inu, del conocido meme

“Doge”. Esto la convierte en la moneda con más seguidores en todas las redes sociales.



3.4 Temas propuestos para el desarrollo de la criptomoneda

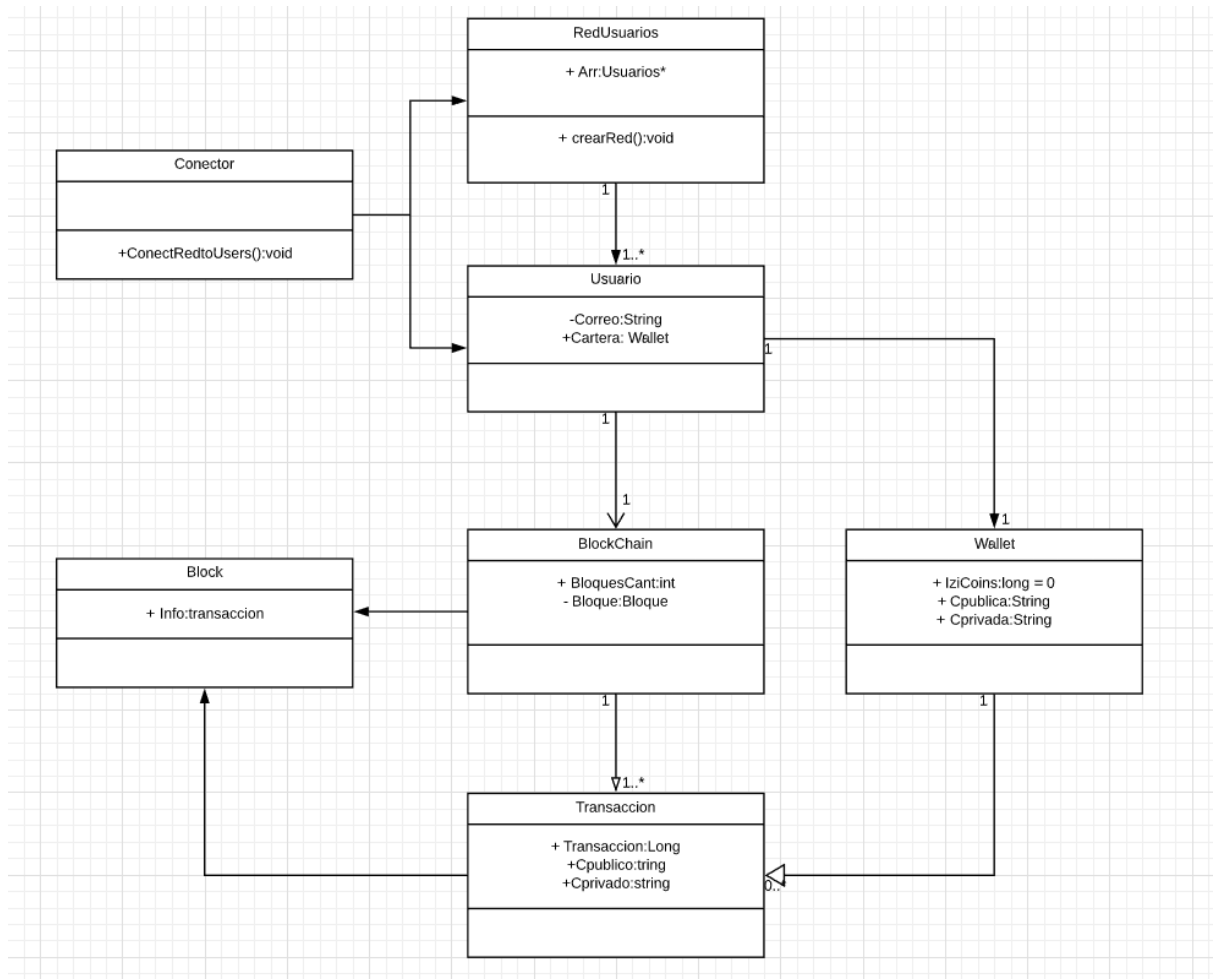
Por motivos de tiempo y ejecución, definiremos nuestros usuarios de manera estática, es decir, en tiempo de compilación el programa reconocerá a 5 usuarios registrados, aquellos podrán hacer uso de la moneda virtual. Esto trae como resultado un mejor control de las funciones principales.

4. Resultados

Ideas concebidas para programar

- Establecer formularios entendibles y útil para el usuario-máquina.
- Establecer una lista de 5 usuarios con criptomonedas otorgadas para la realización de deposito o transferencia.
- Establecer el precio de la criptomoneda en una forma volátil.
- Establecer un monedero virtual, donde se verifica las transacciones hechas por el usuario.
- Establecer un servidor maestro, todas los procesos o funciones serán realizados desde una sola computadora
- Encriptado sencillo pero seguro, implementar la función encargada del cifrado y descifrado de datos: RSA.

4.2 Diagrama de Clases



4.3 Diseño de Interfaz

IZICOIN

INICIO

TRANSACCIONES

CONFIGURACIÓN

PREGUNTAS FRECUENTES

1 IZC = \$ 3,053.90

Cerrar Sesión

MI BANCO

Enviar

Recibir

6,00 IZC

\$ 18.324.4

Mis Transacciones

Trasacción	16/04/2020	Enviado	3,00
Transacción	10/04/2020	Enviado	1,00
Trasaccion	02/04/2020	Recibido	10,00

BLOCKCHAIN

Este proceso es realizado bajo los terminos y condiciones acordados previamente

My Wallet

IZICOIN



DOLLARS

Receptor

-Para iniciar el proceso de transferencia, seleccione el boton de "Transferir"

Cancelar

Transferir

5. Bibliografía

- Millán, R. (s.f.) “*Características de las redes P2P*”. Consultoría estratégica en tecnologías de la información y comunicaciones. Recuperado de:
https://www.ramonmillan.com/libros/librodistribucionlibrosredesp2p/distribucionlibrosredesp2p_caracteristicasp2p.php#conceptop2p
- Moreno, B. , Soto, F. , Valencia, N. , Sánchez, A. (2018). “*Criptomonedas Como Alternativa de Inversión, Riesgos, Regulación y Posibilidad de Monetización en Colombia*”. Recuperado de:

<https://expeditiorepositorio.utadeo.edu.co/bitstream/handle/20.500.12010/4746/TESIS%20ESPECIALIZACION%20CRIPTOMONEDAS-BIBLIOTECA.pdf?sequence=1&isAllowed=y>

- Nin, J. (2018). *“Todo lo que querías saber sobre Bitcoin, criptomonedas y Blockchain y no te atrevías a preguntar”* Recuperado de:
https://www.planetadelibros.com/libros_contenido_extra/38/37925_Bitcoin_Criptomonedas_Y_Blockchain.pdf
- Padró, L. (2019). *“Criptomonedas y la tecnología blockchain. “Valladolid Blockchain””* Recuperado de:
<https://uvadoc.uva.es/bitstream/handle/10324/40317/TFG-E-835.pdf?sequence=1&isAllowed=y>