**Título de Proyecto:** Desarrollo de Billetera Virtual para el manejo de criptomonedas que existen en el mercado.

**Integrantes:**

Juan Pablo Galeano Salguero CC: 1143878656

Andrés David Mutis Muñoz CC: 1144096490

Andrés Felipe Posada España CC: 1113539156

**Planteamiento del problema.**

A día de hoy, y a lo largo de las últimas décadas, aquel sustento y representación de la economía llamado dinero, ha sido un el principal actor en la representación de las riquezas de las naciones y la materialización del tiempo invertido de las personas en labores específicas. En base a lo anterior, surgieron inversiones puntuales del dinero en tecnología, causando una inevitable fusión de estos dos términos y la decadencia de los métodos antiguos para transferir información, que, en los últimos años, sería un equivalente del dinero. La evolución tecnológica cambiaría aquella forma en que el ser humano entendería y distribuiría la información y el dinero, y la manera en que lo concebimos.

Con el paso de los años, la digitalización de la información y la facilidad de distribución de la misma, causaría la inclusión de mercados electrónicos sustentados por detalles, referencias, opiniones y envíos a nivel global; causando así, que los bancos empezaran con pequeños pasos hacia la digitalización de todo un esquema que fue la base de la economía mundial, soportado por libros y contadores especializados en toda la información bancaria, y que para aquel entonces, sería la élite y un mundo desconocido para el ciudadano común. Pronto darían su paso en las transacciones virtuales, apoyados en software de seguridad, que aseguraría de igual o mejor forma, el traslado de información entre cuentas pertenecientes al banco, pero ante tal posicionamiento de los bancos llegarían competidores, debido a la gran libertad de información que estaría disponible, promoviendo un ideal donde los bancos no tomarán partida sobre las transacciones realizadas, y de lo contrario, éstas fueran soportadas por las mismas personas de una forma directa y segura. Llegando de tal forma al término Criptomonedas.

* Las criptomonedas han comenzado a cobrar protagonismo durante los últimos años, sin embargo, su origen se remonta a 2008. A pesar de que cada día cuenten con un mayor número de usuarios, su regulación sigue siendo una incógnita.

**¿Qué son las criptomonedas?**

Las monedas virtuales surgieron como una idea revolucionaria hace unos años. En la actualidad son muchos los que creen que se convertirá en el método de pago del futuro, aunque serán mucho más que eso.

Las criptodivisas o monedas virtuales son un método de pago o divisa virtual formada por bits en lugar de por papel o metal. Al igual que el resto de divisas tradicionales pueden ser intercambiadas y operar con ellas en el mercado.

Se caracterizan por ser ***descentralizadas***, es decir, no depender de una entidad bancaria o gobierno: escapan del control de cualquier banco.

Por ejemplo, cuando realizamos una compra online, debemos registrarnos, es decir, identificarnos y facilitar nuestros datos personales y de nuestra tarjeta de crédito. Más tarde, el banco debe verificar que efectivamente dispones de esa cantidad en tu cuenta y, por último, transferir el dinero. Por tanto, dependes de una entidad bancaria.

**Privacidad:** Cuando realizan una compra online, es necesario introducir tus datos personales, las operaciones mediante monedas virtuales son totalmente anónimas.

**Wallet:** Debes poseer un monedero virtual que contendrá tus monedas virtuales. Debes tener en cuenta que existen diversos tipos de monederos virtuales y que el que necesitas dependerá del tipo de moneda virtual que poseas. Cuando realizas una transferencia debes de asegurarte que el monedero receptor al que las envías las admitirá. De lo contrario, las monedas virtuales podrían perderse.

El objetivo de este sistema monetario es desvincularse de cualquier entidad o sistema bancario existente.

Referencia: <https://www.bilib.es/actualidad/blog/noticia/articulo/todo-lo-que-debes-saber-acerca-de-las-monedas-virtuales/>

Bajo la realidad que vivimos actualmente, donde la información es la materia prima que identifica cada una de nuestras transacciones, y, por lo tanto, cada movimiento, compra, transferencia, venta, son constantemente registrados en sistemas que almacenan y procesan la información, ayudando a comercios en la creación de tendencias sobre nuestros gustos y decisiones. Pero, como en todos los mercados, existen ciertos sectores, concretamente Latinoamérica, donde no se logra llegar, a causa de condiciones que impiden la distribución óptima de servicios de carácter necesario, de diversión y ocio.

Por lo tanto, en aquellas situaciones en las cuales se desea adquirir cierto producto que no se fabrica o se comercializa, de forma directa, en mi localidad o país, y se opta por solicitar el producto en medios externos, surgen diferentes inconvenientes con respecto al estándar utilizado para el valor de moneda de cada país, causando que las comisiones por los envíos sean demasiado altas, en comparación con lo que podría cobrarse en una cartera virtual.

Otro problema presentado es la dificultad para llevar el dinero de forma virtual en tu celular, ya que muchas compañías que prestan servicios de este tipo, tienen un tope de dinero de poder manejar, esto dificulta que las personas puedan acumular ciertas cantidades de dinero, y poderlo transportar a dónde quieran, simplemente llevando su computador en la mochila.

Esto no representaría ningún riesgo al ser hurtado o extraviado ya que el sistema de seguridad debidamente aplicado permitiría a la persona poder asegurar su dinero virtualizado, y simplemente abrir su cuenta en otro sistema con sus respectivos datos.

Por lo tanto, el desarrollo de una Billetera Virtual ayudaría a solucionar y agilizar muchos procesos que requieren altos costos y una gran cantidad de tiempo para las personas.

**¿Cómo funcionan las monedas virtuales o criptomonedas?**

Las monedas virtuales permiten realizar transacciones que van de usuario a usuario, es decir, no existe un intermediario. Cada usuario posee un monedero virtual en el cual se administran sus monedas virtuales, ya que es posible manejar varias criptomonedas con una misma billetera, esta funcionalidad es limitada por algunos monederos virtuales. Las transacciones que se realizan quedan registradas en una base de datos pública conocida como *blockchain*que permite a los usuarios estar al día de las operaciones de la comunidad. Es por esto por lo que la moneda se considera descentralizada, porque permite que todos los usuarios, de cualquier país, ejerzan el mismo control sobre el sistema. Todas las transacciones poseen una firma digital correspondiente al usuario que realiza el envío. Además, cada bitcoin está registrado, lo que permite saber en cuántas transacciones ha participado y dónde se encuentra en cada momento.

Existen un grupo de usuarios que se encargan de verificar dichas transacciones, registrarlas en el libro de cuentas y de asegurar el funcionamiento de la red. Son los conocidos como mineros. El sistema de minería de la red permite todas estas acciones a través de un programa de software y hardware especializados. Como recompensa a estos mineros encargados de ejecutar los códigos que permitan la seguridad del *blockchain*, reciben bitcoins. Esta fue la primera forma que tenían los usuarios de obtener dicha moneda virtual. Como curiosidad, la primera transacción ejecutada con bitcoins fue realizada por Lazlo Hanyecz quien ofreció 10.000 bitcoins por unas pizzas.

Cabe aclarar que las criptomonedas tienen un límite, en el caso del bitcoin ya que es la más famosa y fue la pionera en este mercado, su límite es que solo pueden crearse 21 millones de bitcoins, mucho creerán que esto impide que el bitcion pueda ser una moneda bien vista del futuro, por que su limite es poco comparado con la cantidad de población mundial, pero esto nunca será un impedimento, pues los bitcoins pueden dividirse hasta en 8 cifras decimales (0.000 000 01 BTC) e incluso unidades más pequeñas si es que así se lo requiere en el futuro.

Otro elemento importante es la cartera o monedero que usarás para recibir tus pagos por minar. Esta puede ser tipo hardware o fría (Trezor, Ledger, KeepKey, OpenDime, etc), tipo software o aplicación (Coinomi, Wasabi, Exodus, Jaxx, etc) o en línea (MyCrypto, Blockchain, Bitgo, etc).

Las [carteras](https://www.criptonoticias.com/criptopedia/como-elegir-monedero-cartera-bitcoin-criptomonedas-criptoactivos/) frías las puedes adquirir en tu tienda (física o en línea) de equipos electrónicos de confianza, mientras que las de tipo software puedes descargarlas desde la tienda de aplicaciones de tu dispositivo móvil (App Store o Google Play Store) o directamente desde el sitio web oficial de la cartera, donde también podrías encontrar versiones para ordenadores de escritorio y portátiles.

Las carteras en línea, por su parte, son poco recomendadas por muchos expertos; ya que son muy propensas a ataques o hackeos. Lo mismo pasa con las carteras que ofrecen las [casas de cambio](https://www.criptonoticias.com/seguridad-bitcoin/robo-fraude/detectados-hackers-robaron-usd-200-millones-casas-cambio/) u otros servicios que custodian tus fondos en criptomonedas. En este caso, no solo tienes en contra las posibilidades de que ataquen a la plataforma que te da acceso a tus criptomonedas; sino que, además, no tienes las llaves privadas de tu monedero.

**¿Cómo se puede invertir o adquirir criptomonedas?**

Las criptomonedas se pueden conseguir de 2 maneras, una sería comprando directamente mediante internet y la más difícil, es mediante la minería. Actualmente los gobiernos cuentan con un sistema monetario encargado de imprimir el “dinero”, a este medio de cambio se le considera de uso legal y sirve para la compra de bienes ó servicios. En el universo de las criptomonedas, el dinero no se crea, sino que se tiene que descubrir, a este proceso se lo conoce como minería. “La minería de criptomonedas se puede definir como el conjunto de procesos necesarios para poder realizar validaciones, así como el procesamiento de las transacciones de una criptomoneda dentro de una cadena de bloques o más conocida como Blockchain”. Es muy importante mencionar que los mineros utilizan potentes dispositivos informáticos, los cuales les ayudan a competir entre ellos para encontrar antes que los demás, la solución de complejos problemas matemáticos. Al encontrar dicha solución, el minero estará resolviendo el problema, por lo tanto, las transacciones se verificarán y se añadirán a la cadena de bloques, recibiendo como recompensa, una cantidad específica de la criptomoneda que estén minando. Incentivar a los mineros con los pagos de una cierta criptomoneda para validar sus transacciones, hace que la moneda digital sea segura y de uso confiable.

Al minar criptomonedas como Bitcoin, participas en la verificación de las transacciones realizadas en su red y en la emisión de nuevas criptomonedas. Si has leído o escuchado sobre la minería de criptomonedas antes, seguramente se te hace familiar la palabra algoritmo. Existen dos tipos de algoritmo que son cruciales para saber cómo minar una criptomoneda en particular: el algoritmo de minería y el algoritmo de consenso.

**El algoritmo de minería** (hashing algorithm, en inglés) está estrechamente relacionado con el procesamiento de datos. El hardware minero que necesites depende mucho del algoritmo de minado que use la criptomoneda de tu preferencia. Especialmente si se trata de dispositivos ASIC, ya que estos son desarrollados para trabajar únicamente con un algoritmo específico.

**El algoritmo de consenso**, por su parte, está más relacionado con el acuerdo entre todos los miembros (nodos) de una red de criptomonedas en cuanto a su funcionamiento: qué transacciones cumplen con los criterios de validez, el orden de los bloques en la cadena, etc. Conocerás más detalles sobre las funciones de los algoritmos de minado y consenso más adelante. De momento, nos enfocaremos en los dos tipos de algoritmo de consenso más populares entre las redes de criptomonedas: la prueba de trabajo (PoW) y la prueba de participación (PoS).

Los métodos de validación como la minería de criptomonedas, se denominan prueba de trabajo ó PoW y son una de las razones por las que las criptomonedas y la tecnología Blockchain se consideran tan innovadoras.

PoW (proof of work, por sus siglas en inglés) es un algoritmo de consenso que se basa en **resolver un acertijo mediante cálculos matemáticos**. El minero trata de conseguir de la forma más veloz posible la respuesta a dicho acertijo, que le permitirá anexar un nuevo bloque de transacciones a la cadena.

Las probabilidades de que dos mineros den con la misma respuesta de forma simultánea son prácticamente nulas, por no decir imposible. El acertijo de cada bloque requiere una solución distinta y aleatoria, de modo que no se pueda predecir fácilmente. Este mecanismo buscar impedir el doble gasto de monedas; es decir, que alguien que ya transfirió una criptomoneda pueda volver a transferirla a alguien más como si nunca la hubiera gastado.

Resolver el acertijo de un bloque implica obtener la recompensa que este ofrece. Pero, para llegar a esa respuesta antes que otro minero, **tu hardware debe procesar grandes cantidades datos a alta velocidad**. Por eso es importante contar con equipos mineros potentes y adecuados para minar tu criptomoneda predilecta.

La prueba de trabajo es el algoritmo de consenso más comúnmente utilizado en la minería de criptomonedas. [Bitcoin](https://www.criptonoticias.com/criptopedia/que-es-bitcoin-btc/), la primera de todas las criptomonedas usa PoW y para poderla minar es necesario contar con hardware especializado. Otras criptomonedas reconocidas que usan la prueba de trabajo son [monero](https://www.criptonoticias.com/criptopedia/que-es-monero-xmr/) (XMR), ethereum classic (ETC), zcash (ZEC), [bitcoin cash](https://www.criptonoticias.com/criptopedia/que-es-bitcoin-cash-bch/) (BCH), etc.

La otra forma en la que puedes conseguir criptomonedas, es mediante la compra. Puedes comprar **criptomonedas**en páginas de internet especializadas en la compra-venta de las mismas. Estas plataformas cuentan con un sistema de usuarios, los cuales pueden pagar las criptomonedas deseadas con tarjeta de crédito o transferencia bancaria. También se puede comprar criptomonedas en las plataformas de trading o inversiones.

El precio se establece con relación al valor de la moneda que se desee adquirir y la oferta y demanda que desarrolle en el mercado, por lo que puede variar, aumentando o devaluando su valor monetario, por lo que invertir en criptomonedas conlleva un alto grado de riesgo.

**¿Qué tan rentable será el mercado de las criptomonedas en 2020?**

Así como la "fiebre del oro" atrajo a cientos de miles de buscadores del metal a California a mediados del siglo XIX, hoy los mineros buscan en sus computadores oro digital bajo la forma de criptomonedas.

Oro o humo, según cómo se mire, el bitcoin —la moneda digital más emblemática de las 4.000 que existen en el mercado— ha estado sujeto a una volatilidad extrema.

Cuando fue creado, en enero del 2009, el bitcoin valía menos de un dólar, en 2017 casi llegó a los US$20.000, al año siguiente se desplomó hasta los US$3.200, en 2019 saltó otra vez a los US$13.800 y por estos días se acerca a los US$9.000.

¿Ha sido rentable? Quienes los compraron al inicio han tenido una rentabilidad de 9.000.000%, según el medio económico *Bloomberg*. Y por las dudas, no sobran ceros en la cifra.

Efectivamente estamos hablando de una **rentabilidad de nueve millones por cien.**

El dinero que utilizamos diariamente es emitido por el banco central de un país. En Estados Unidos es la Reserva Federal el organismo encargado de crear dólares.

Pero en el mundo del dinero digital no hay una autoridad encargada de acuñar criptomonedas.

Las crean los llamados "mineros", para lo que usan la **tecnología *blockchain*** (cadena de bloques).

Se hace con computadoras que trabajan resolviendo problemas matemáticos. El que lo hace más rápido, recibe como recompensa nuevos bitcoins.

Es por eso que los que tienen una mayor potencia digital instalada, tienen más probabilidades de resolver el problema matemático o**"resolver el bloque"** de operaciones.

Actualmente, cada vez que los mineros descubren un nuevo bloque (algo que ocurre cada 10 minutos), **reciben como recompensa 12,5 nuevos bitcoins**.

Cada día se emiten 1.800 bitcoins. Pero eso cambiará en mayo de este año cuando se produzca un fenómeno conocido como "*halving*del sistema", una reducción a la mitad de la recompensa en bitcoin que reciben los mineros.

Como a partir de mayo solo se emitirán **900 bitcoins al día**, los entusiastas del sistema vaticinan que el precio subirá.

**"Eso provocará un incremento de precio, seguro"**, dice Javier Pastor, de la empresa Bit2Me.

Después de los dos *halving*previos —en 2012 y 2016— hubo un alza en el precio del bitcoin del 8.000% en el primer caso y de un 2.000% en el segundo, según datos de *Bloomberg*.

Pero muchos analistas de mercado dicen que esta vez las condiciones son distintas y nada garantiza que se produzca un incremento.

Por lo pronto, el mercado de las criptomonedas no ha logrado convertirse en un medio de intercambio generalizado como algunos proyectaron hace una década.

Casos de fraude, robo y otros incidentes también han hecho que los inversores tengan mayor cautela, especialmente desde la caída estrepitosa que lo llevó a un valor apenas superior a los US$3.000.

Sin embargo, quienes han obtenido gigantescas rentabilidades siguen optimistas y argumentan que el éxito que ha tenido la tecnología *blockchain*es una clara señal de que las criptomonedas llegarán a las nubes, además de ser algo innovador, y lo innovador se pone de moda.

Aunque también es probable que el escrutinio de los **entes reguladores** se intensifique.

Nadie puede saber con exacta precisión si el mercado de las criptomonedas terminará siendo el nuevo oro digital o el nuevo humo digital. Eso solo lo puede decir el paso del tiempo.

Referencias:

<https://www.bbc.com/mundo/noticias-51023616>

<https://www.blockchain.com/>

<https://www.bbva.com/es/computacion-cuantica-5g-y-blockchain-tecnologias-que-marcaran-la-proxima-decada-en-la-banca/>

<https://www.invertirenbolsaweb.net/como-invertir-en-criptomonedas/>

<https://www.avatrade.es/educacion/trading-para-principiantes/minar-criptomonedas>

<https://www.criptonoticias.com/criptopedia/como-minar-bitcoin-criptomonedas/>