Criptomonedas

Gilberto Espinoza, Luis Fernando Sotomayor

December 10, 2017

Abstract

Criptomonedas, son dinero digital o virutal, que se basan en la encriptación para su seguridad. Estas nuevas formas de realizar transacciones estan revolucionando el mercado, dado que en principios de este año, 2017, la lider en esta nueva tecnologia, **Bitcoin**. Este tenía un precio de $933.66 USD y para principios de noviembre del mismo año alcanzaba $6440.97 USD, un crecimiento del mas 600% en unos cuantos meses. Marcando una nueva moda nuevas monedas empezaron a emerger, el como estas estan variando, es el objetivo de este documento.

Criptomonedas

Para explicar las criptomonedas utilizaremos al Bitcoin como referencia, dado que fue esta la que empezo el moviemiento y puede decirse que cualquier otra es una modificacion o copia directa.

Una versión puramente electrónica de efectivo permitiría que los pagos en línea fuesen enviados directamente de un ente a otro sin tener que pasar por medio de una institución financiera. Las transacciones son validadas por una red de usuarios, que verificaran que ocurra un doble gasto. Cuando un usuario malintencionado intenta gastar sus criptomonedas en dos destinatarios al mismo tiempo se denomina doble gasto. La mineríía y la cadena de bloques permiten crear un consenso en la red acerca de cuál de las dos transacciones es considerada válida.

Una criptomoneda puede utilizarse como cualquier divisa, intercambiarla por alguna otra o gastarla por algun servicio o producto que la acepte.

Mision y vision

La misión de esta nueva tecnología es dar alternativas a las personas de las monedas reguladas y controladas por algún gobierno entonces el usuario pueda experimentar una condición financiera mas libre y directa. Esto se quiere lograr independientemente de la condición financiera del usuario ya que es un alto porcentaje no cuenta con una cuenta de banco común.

La visión es lograr que las criptomonedas sea mundialmenten aceptadas por los negocios, empresas y los ciudadanos del día al día para que estos operen sin necesidad de terceros, ya sean bancos, gobiernos o parecidos.

El objetivo con las criptomonedas se guarda en que estas deben ser descentralizadas, no imparta que tanto dinero o poder tenga una persona o institucion no puede adueñarse o monopolizar la moneda, asi como el gobierno de Estados Unidos y sus bancos son los que manejan los dolares (USD), en las criptomonedas esto no es posible gracias a la tecnologia P2P. Las criptomonedas ofrecen transacciones internacionales sin impuestos o tarifas ya que son directas entre los usuarios, se validan entre la comunidad, no por un organismo en el que ambos confien, un ejemplo de este

tercero seria Western Union, empresa cuyo servicio es la transaccion de dinero en efectivo a nivel mundial y la cual cobra tarifas.

Como funcionan

Blockchain

La cadena de bloques es un registro público de las transacciones Bitcoin en orden cronológico. La cadena de bloques se comparte entre todos los usuarios de Bitcoin. Se utiliza para verificar la estabilidad de las transacciones Bitcoin y para prevenir el doble gasto. Es una contabilidad pública compartida en la que se basa toda la red de la criptomoneda. Todas las transacciones confirmadas se incluyen en la cadena de bloques. De esta manera los monederos Bitcoin pueden calcular su saldo gastable y las nuevas transacciones pueden ser verificadas, asegurando que el cobro se esta haciendo al que realiza el pago. La integridad y el orden cronológico de la cadena de bloques se hacen cumplir con criptografía.

Algunas criptomonedas al crear un nuevo bloque genera nuevas monedas y se las transfiere a la persona/minero/cliente que verificó y envió el bloque al blockchain.

Por ejemplo Bitcoin, cada nuevo bloque minado genera una recompensa en Bitcoins que se entregan al minero que generó el bloque.

Una transacción es una transferencia de valores entre monederos Bitcoin que será incluida en la cadena de bloques. Los monederos Bitcoin disponen de un fragmento secreto llamado clave privada, utilizada para firmar las operaciones, proporcionando una prueba matemática de que la transacción está hecha por el propietario del monedero. La firma también evita que la transacción no sea alterada por alguien una vez ésta ha sido emitida. Todas las transacciones son difundidas entre los usuarios y por lo general empiezan a ser confirmadas por la red en los 10 minutos siguientes a través de un proceso llamado minería.

Mineros

La minería es un sistema de consenso distribuido que se utiliza para confirmar las transacciones pendientes a ser incluidas en la cadena de bloques. Hace cumplir un orden cronológico en la cadena de bloques, protege la neutralidad de la red y permite un acuerde entre todos los equipos sobre el estado del sistema. Estas normas impiden que cualquier bloque anterior se modifique, ya que hacerlo invalidaría todos los bloques siguientes. La minería también crea el equivalente a una lotería competitiva que impide que cualquier persona pueda fácilmente añadir nuevos bloques consecutivamente en la cadena de bloques. De esta manera, ninguna persona puede controlar lo que está incluido en la cadena de bloques o reemplazar partes de la cadena de bloques para revertir sus propios gastos.

Usar potencia de procesamiento para producir un bloque válido, y como resultado "extraer" algunas bitcoins. Las reglas de la red se establecen de forma que la dificultad se ajusta para mantener la producción de bloques en aproximadamente uno cada 10 minutos. De esta forma, un mayor número de mineros participantes en la actividad de minería, implicará una mayor dificultad en la generación de un bloque para cada minero individual. Una mayor dificultad total implicará, para un atacante, una más difícil sobreescritura del extremo de la cadena de bloques con sus propios bloques (lo que le permitiría el doble gasto de sus monedas.

Consiste en un tipo de trabajo que realiza un cliente, que por lo general es la realización de un cómputo en un ordenador, ese trabajo es verificado en el servidor. Lo común es que estos cómputos deben ser difíciles para el cliente pero debe ser fácil de verificar por el servidor. En Bitcoin se usa

POW para verificar transacciones y generar nuevos bloques, este proceso se conoce como minado (mining).

Además de la importancia para el mantenimiento de la base de datos de transacciones, la minería es también el mecanismo por el que las bitcoins son creadas y distribuidas a las personas en la economía bitcoin. Las reglas de la red se establecen de tal forma que en los próximos cien años, décadas más o menos, serán creadas un total de 21 millones de bitcoins.

También existe la opción de comprar poder de computo online a alguna empresa, esto es pagar una cantidad de dinero para que un hardware trabaje minando las monedas sin que uno mismo tenga que conseguir el equipo necesario, esta una opción pero representa un riesgo ya que tu mismo no controlas el hardware.

Una opción que esta siendo muy popular ultimamente es es el "Pool Mining", un grupo de mineros, se dedican a resolver un proceso y como comparten recursos, reparten la recompesa pero esta la consiguen mas seguido al tener mas podera su disposición.

Centros cambio

En esta carrera por alcanzar la cúspide de la innovación lideran países como Argentina, Brasil y México. Esta última nación se ha destacado por innumerables proyectos de desarrollo de la tecnología de contabilidad distribuida (DLT) y un ecosistema cada vez más nutrido y variado de startups, que le depara un prometedor futuro tecnológico a la economía mexicana.

En conjunto con el sector empresarial dedicado a las tecnologías de contabilidad distribuida, las monedas criptográficas han llegado a México con el objetivo de incluir a la población a un sistema financiero más accesible y justo; ofreciéndole tanto facilidades transaccionales a los ciudadanos como la posibilidad de invertir a largo plazo.

Bitso

México alcanzó durante este año su máximo histórico de transacciones bitcoin con 242 mil dólares en transacciones locales, cifras que aumentaron en conjunto con otros países de Latinoámerica. Asimismo, esta criptomoneda tiene un fuerte ecosistema en el país con más de 81.000 usuarios, según datos de una de las mayores casas de cambio del país, Bitso.

Volabit

Volabit es otra casa de cambio mexicana que ofrece compra de bitcoins por medio de transferencias o depósitos de dinero fiat, permitiendo tanto a las personas que poseen cuenta bancaria como a los desbancarizados acceder al dinero criptográfico. Los usuarios pueden depositar sus pesos en los locales 7-Eleven, las farmacias Benavides, farmacias del Ahorro o Extra

Cajeros Automaticos

Otro método para acceder a unos cuantos bitcoins son los cajeros automáticos especializados en esta criptomoneda. México es el segundo país de América Latina con mayor cantidad de ATM de bitcoin, contando con tres (3) dispositivos instalados en todo su territorio —según fuentes de Coin ATM Radar—; la nación es superada solamente por República Dominicana que posee cuatro (4) cajeros en su capital, marca que se rompió recientemente.

Los pobladores y turistas de las ciudades de Tijuana, La Fonda y Ciudad de México han sido los beneficiados de estos servicios. En el caso de Tijuana, el ATM se encuentra en el local IMAXESS – Diagnostic Imaging, específicamente en el sector Madero, calle Jalisco. La máquina permite tanto comprar bitcoins con dinero fiat, como retirar fondos en monedas criptográficas a cambio de pesos

mexicanos; con un límite de compras de 750,000 pesos y un máximo de venta de 74,500 pesos mexicanos.

Por otro lado, en Ciudad de México el cajero se ubica en el local Fantastico Comics del sector Felix Cuevas. El dispositivo permite no sólo comprar bitcoins, sino también litecoin y dash. Asimismo, el ATM compra y vende criptomonedas bajo un máximo de 6,000 pesos mexicanos.

Por último, el hotel y restaurante La Fonda en la carretera Tijuana Ensenada, también cuenta con su propio cajero que únicamente acepta bitcoins, el cual solo permite comprar esta criptomoneda por un máximo de 20,000 pesos mexicanos.

Bitcoin

Historia

Bitcoin es la primera implementación de un concepto conocido como "moneda criptográfica", la cual fue descrita por primera vez en 1998 por Wei Dai en la lista de correo electónico "cypherpunks", donde propuso la idea de un nuevo tipo de dinero que utilizara la criptografía para controlar su creación y las transacciones, en lugar de que lo hiciera una autoridad centralizada.

La primera especificación del protocolo Bitcoin y la prueba del concepto la publicó Satoshi Nakamoto en el 2009 en una lista de correo electrónico. Satoshi abandonó el proyecto a finales de 2010 sin revelar mucho sobre su persona. Desde entonces, la comunidad ha crecido de forma exponencial y cuenta con numerosos desarrolladores que trabajan en el protocolo Bitcoin.

La anonimidad de Satoshi a veces ha levantado sospechas injustificadas, muchas de ellas causadas por la falta de comprensión sobre el código abierto en el que se basa Bitcoin. El protocolo Bitcoin y su software se publican abiertamente y cualquier programador en cualquier lugar del mundo puede revisarlo o crear su propia versión modificada del software.

Al igual que los programadores actuales, la influencia de Satoshi se ha limitado a que los cambios que hizo los adoptaran los demás y, por tanto, no controlaba Bitcoin. Así, conocer la identidad del inventor del Bitcoin es igual de relevante que saber quién inventó el papel.

Satoshi Nakamoto

Satoshi Nakamoto es la persona o grupo de personas que crearon el protocolo Bitcoin y su software de referencia, Bitcoin Core. En 2008, Nakamoto publicó un articulo acerca de Bitcoin en el sitio de criptografia *mewdowd.com*.

En 2009, lanzó el software Bitcoin, creando la red del mismo nombre y las primeras unidades de moneda.

Se desconocen su identidad y su nacionalidad. Si bien los pocos datos disponibles sobre él apuntarían a Japón, nunca escribió absolutamente nada en japonés, ni hizo versión japonesa del cliente Bitcoin ni una página inicial en japonés para bitcoin.org.

Por todo lo que se sabe, es totalmente desconocido fuera de Bitcoin, y su clave PGP se creó apenas unos meses antes de la fecha del bloque de génesis. Parece estar muy familiarizado con la lista de correo sobre criptografía, pero en esa lista no hay mensajes suyos no relacionados con Bitcoin. Utilizaba una dirección de correo electrónico de un servicio anónimo de alojamiento de correo (vistomail) así como otra de una cuenta gratuita de correo web (gmx.com) y enviaba siempre los mensajes a través de una conexión Tor. Se ha especulado con que su identidad habría sido creada expresamente con antelación como una manera de protegerse a sí mismo o a la red Bitcoin. Es posible que eligiera el nombre "Satoshi" porque puede significar sabiduría o razón.

Eventos sociales, politicos y economicos que impactaron el Bitcoin

Corea de Norte ataca casas de cambio

Sin embargo, siempre hay una parte negativa para cada situación, y una de ellas ha sido el aumento de acciones ilícitas para poder tener un posesión al menos un bitcoin. Una de las trabas más renombradas en los últimos ha sido Kim Joung-un y Corea del Norte, pues según expertos en seguridad los hackers del país están buscando la manera de acceder a casas de cambio de bitcoin.

Corea del Norte tiende a enfocar su espionaje cibernético, en actividades relacionadas con el Estado. Sin embargo esto cambió desde el año pasado, cuando la compañía de ciberseguridad Fireeye empezó que darse cuenta que el país estaba poniendo como blanco a entidades bancarias y a todo el sistema financiero mundial. En 2017 se han detectado diversos ataques a las casas de cambio de Corea del sur, y esta actividad ya se está expandiendo a grupos bancarios en Europa, incluyendo a una compañía de cajeros automáticos.

Si bien se sabe que Corea del Norte siempre está detrás de alguna estrategia sospechosa, estos ataques constantes a las casas de cambio de Bitcoin muestran un nivel considerable de desesperación. El país se encuentra aislado del mundo debido a sanciones a nivel mundial, y las mismas solo cobraron más poder desde que Donald Trump se instaló en la Casa Blanca.

Usuario final

Wallets

Un software que se comunica con la red para poder realizar operaciones de envío y recepción de la criptomoneda.

Que son

Las *wallets* guardan las llaves privadas que tu necesitas para acceder a la dirreccion del bitcoin y gastar tus fondos. Vienen de distintas formas, diseñadas para distintos dispositivos.

La wallet oficial de Bitcoin es *Bitcoin Core* la misma palicacion se utiliza para la mineria si es que sea desea, pero hay muchas alternativas, una para cada nueva moneda que emerge, adicionalmente hay wallets que soportan diferentes monedas e incluso puedes hacer el cambio de una a otra desde la misma. Estas crecen cada vez, dandote en tiempo real varaiciones de los precios.

Como funcionan

Estas guardan tu "dirreccón", tu llave privada única para que se use de referencia para que los demas usuarios puedan mandarte monedas, tambien, pueden generar un codigo QR, que al ser escaneado ejecuta la transferencia, entonces con simplemente compartir esta imagen uno puede mandar y recibir monedas digitales, por lo cual esta informacion debe ser tratada con sumo cuidado

Como obtener Bitcoins

Uno puede obtenerlos de diversas maneras, casas de cambio, trabajo por ello, o una simple transferencia en un local. La forma mas común es comprarlos a traveés de una casa de cambio, en México podemos mencionar *Bitso* y *Volabit* empresas que estan respetando las regulaciones que rodean las criptomopnedas.

Otro método es el tipico minado pero para un usuario que no quiere o no pueda sumergirse mucho en el mundo de esta nueva tecnologia, llega a ser un metodo que involucra mucha energia y tiempo.

Empresas que aceptan bitcoin como metodo de pago

Dish La cadena de television de paga empezo a aceptar Bitcoin desde Agosto del 2014. Esta esta asociada a *Coinbase.com* para realizar tales trasacciones.

Newegg La tienda en linea para la compra de gadgets, partes y equipos de computo no pudo quedarse atrás y empezó a recibir bitcoin como metodo de pago utilizando a BitPay como medio para el manejo de cambio.

Steam La plataforma de compra de videojuegos online acepto Bitcoin como metodo de pago cuando la moneda apenas valia $20 USD.

Criptomonedas vs Moneda clasica

Diferencias

EL dinero clasico puede imprimirse y reproducirse tanto como el gobierno lo desee provocando inflacion y que el poder adquisitvo disminuya, BTC no puede ser reproducido si no creado, recordemos que el el limite es 21 millones de unidades.

Descentralizacion, BTC no depende de alguna institucion para tener valor o para utilzarse, se basa en si misma, confia en si misma y los usuarios comparten esa confianza, aceptamos dinero clasico por que los demas lo aceptan, pero este al final depende de las accciones de los bancos, la bolsa y el gobierno; BTC depende unicamente de sus usuarios.

Primero que todo Bitcoin no pertenece a ningún Estado o país y puede usarse en todo el mundo con igualdad. Esto lo hace de mucha utilidad, en especial para las personas que no poseen cuentas bancarias tradicionales. El Bitcoin se puede cambiar a euros u otras divisas y viceversa, como cualquier moneda.

Fácil proceso de creación de su cuenta digital Bitcoin. Ciertamente, es más fácil crear una cuenta digital de Bitcoin que crear una cuenta bancaria tradicional. Cualquier persona puede crear una cuenta digital en segundos, sin tener que proveer sus detalles personales, y sin enviar su historial crediticio. Además, la rata de aceptación de la cuenta digital Bitcoin es del 100

Quien "controla" cambio de Bitcoin a USD

Nadie, los intercambios entre divisas tipicas a BTC, son realizadas por empresas pero estas no lo controlan, solo ofrecen el servicio a una escala mas grande. Comprar criptomonedas de algun centro de cambio no seria distinto a comprarle a tu amigo unos y pagarle en efectivo.

Como funciona este cambio

Se realiza de igual manera que comprar algun otro servicio con su tarjeta bancaria, pagamos la luz, el telefono el cable y se descuenta el total entonces tienes tu servicio en tu casa, con bitcoin enlazas tu "wallet" es decir, un direccion única que te identifica como usuario de bitcoin, esta tu la guardas y proteges ya que esta es como una cuenta donde los datos de tus bitcoin son guardados y ese es el "servicio" que compraste

Analisis BTC vs ETH vs BCH

La principal accion que realizaremos en el analisis es probar correlacion entre los datos y ver si es significativa la informacion que encontremos.
Para ayudarnos, tambien interpretaremos graficos de los datos.
Tambien intetaremos correlacionar Bitcoin con Ethereum.
precio mas bajo en bitcoin cada anio se puede corresponder a algun suceso? Cambio mas abrupto de cresta a valle o viceversa del precio

series de tiempo de las criptomonedas sobreponer la media de cada mes y anio sobreponer el precio mas alto y bajo de los dias Comparar bitcoin a las demas monedas mostrar las diferencias extremas entre bitcoin y las demas monedas hay dependencia entre el precio de las monedas? probar usando la media mensual probar usando la media global

cantidad de mondeas vs tiempo es una serie hipergeometrica?

cantidad de monedas vs precio hay dependencia?

tamano promedio de blockchain vs cantidad de bitcoin hay dependencia? vs tiempo aumenta o disminuye?

tiempo vs hash rate dificultad dependecnia?

miners revenue vs tiempo numero de mondeas dependecia?

costo por transaccion vs tiempo vs numero de monedas cuando fue mas conveniente ser minero? ahora mismo es rehabituable ser minero? predecir si lo sera en un futuro

Conclusiones

Cómo es que el precio historico de las diferentes criptomonedas cambia en el tiempo?

Se puede predecir el precio de las criptomonedas?

Las criptomonedas son volatiles o estables?

Se relaciona la fluctiación de precio de una criptomoneda con otra?

Los cambios de precio se dan con respecto a temporadas?

predicciones de terceros de btc

predicciones propias

1 Bibliografia