UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ECONOMÍA

BLOCKCHAIN, CRIPTOMONEDAS Y BITCOIN

TESINA

QUE PARA OBTENER EL TÍTULO DE:

LICENCIADO EN ECONOMIA

PRESENTA :

KEVIN ARARI CORDOVA CARRION

DIRECTOR DE TESIS:

JAVIER LARA OLMOS

Ciudad Universitaria, Cd. Mx., 2019

Dedicatoria

Se la dedico a quienes siempre han confiado en mí y me forjan día a día para ser una mejor persona, esas personas que se han sacrificado y se han esforzado por darme buenos momentos, a quienes han creído en mí y me han enseñado que siempre se puede dar mas no importa si la vida te depara una tormenta o un claro, a quienes me han regalado alegría así como también a quien me ha dado conocimiento y sabiduría para continuar persiguiendo mis metas no importando que tan grande sea el reto.

Gracias a todos y cada uno de los que confían en mí y que están a mi lado.

Tabla de contenido

I. Glosario.

Altcoins:Criptomonedas alternativas del Bitcoin.

Arbol de Merkle: Un árbol de Merkle es una estructura de datos basada en hash. Una estructura de datos basada en hash asigna datos a una clave. Una forma simple de esto es la marcación rápida en su teléfono. Asignar un número de teléfono a cada tecla es una estructura basada en hash.

Bitso:Casa de cambios de criptomonedas especializada en México y Latinoamérica.

Blockchain: Sistema base de datos distribuida y segura (gracias al cifrado) que se puede aplicar a todo tipo de transacciones que no tienen por qué ser necesariamente económicas.

BTC/Bitcoin: Capitalización de mercado combinada de precio de mercado multiplicado por el numero de de unidades de divisa existentes.

CPMI: Comite de pagos y de infraestructura de mercados.

Cuasidinero: Se denomina cuasidinero a un tipo de activo financiero caracterizado por contar con menor liquidez que el dinero corriente, al que representa en ciertos periodos de tiempo y en el que puede mediante ciertos mecanismos transformarse ya que existe la posibilidad de que sea canjeado en efectivo.

Deepweb: Mercado negro de la red donde se encuentran drogas, armas, trata de blancas, etc.

eCommerce: método de compraventa de bienes, productos o servicios valiéndose de internet como medio, es decir, comerciar de manera online.

Firmas de circulo: Firma creada por cualquier miembro de un circulo de usuarios

Hash: Funcion resumen

Miners: Gente que se dedica al minar las criptomonedas

Paper: Es un trabajo de investigación o comunicación científica publicado en alguna revista especializada.

Peer-to-peer/p2p: Red de Pares o P2P, es una red de ordenadores en la que todos o algunos aspectos funcionan sin clientes ni servidores fijos, sino una serie de nodos que se comportan como iguales entre sí.

PIN: Personal Identification Number / Número de Identificación Personal

Public ledger: Libro de cuentas publicas

Spam: Bombardeo de basura electronica

Tokens: Fichas Digitales

Torrents: Simplemente, un Torrent es información acerca de un archivo de destino, aunque no contiene información acerca del contenido del archivo. La única información que contiene el Torrent es la localización de diferentes piezas del archivo de destino

II. Abstract

En el presente trabajo se ha investigado sobre las criptomonedas enfatizando en el bitcoin y en lo que es el blockchain, el propósito principal que se ha encontrado es que no es un tema muy concurrido debido a su complejidad y a su actualidad, por lo que el material en español en su mayoría es escaso, se dio a la tarea de buscar fuentes en su mayoría en ingles sobre el tema, muchas de ellas siendo: libros de programación, libros de consulta, informes, papers, artículos, entrevistas y páginas web, por el lado teórico económico en su mayoría de la escuela Austriaca la cual se acomodó más a la idea que se ha querido plasmar sobre el tema. Las criptomonedas tienen las cualidades del dinero y mucha gente las están usando día a día para satisfacer sus necesidades económicas, desde una simple transferencia hasta pagar nominas o mandar remesas, todo esto gracias a la facilidad y la velocidad que nos dan las nuevas tecnologías. En el capítulo dos se intenta explicar de una manera comprensible para cualquier persona con poco conocimiento de programación o de tecnología con el fin de que se comprenda esta innovadora forma de encriptar datos, el blockchain es una tecnología que ha llegado para quedarse y conforme pasen los años más empresas comenzaran a adoptarlo debido a que es costo efectivo y seguro, sin olvidar que conforme pase el tiempo y el poder computacional aumente hará cada vez más complicado burlar los sistemas de seguridad que este tiene, en las últimas páginas del trabajo se han puesto varios gráficos que demuestran donde y por qué en ciertas zonas hay más gente adepta a esta nueva forma de dinero y así concluir esta investigación que da pie para escribir más sobre el tema.

INTRODUCCIÓN.

III. Justificación

El tema de investigación propuesto, surge de la curiosidad por conocer sobre un tema de actualidad en el mundo monetario y de la constante evolución de los servicios financieros por medio de las nuevas tecnologías de comunicación, aunque el plan es hablar un panorama de general de las criptomonedas de manera tanto técnica como funcional, se especificara sobre el Bitcoin, el cual es el que está más en boga en estos tiempos, la intención con este trabajo es proporcionar herramientas para la comprensión de cómo funcionan las criptomonedas y el mercado del Bitcoin, empezando con una breve introducción histórica de tal moneda, para dar paso al funcionamiento del mecanismo del Blockchain; esta parte podrá parecer muy técnica, sin embargo es muy importante si se quiere entender el porqué de la fama de esta divisa y para terminar se finaliza con unos cuantos argumentos que analizan a mis alcances académicos los pros y los contras de esta moneda.

¿Qué es el bitcoin? El bitcoin es en términos simples otra divisa, si lo complicamos un poco es un sistema, y los bitcoins son la divisa en si, como con cualquier divisa el bitcoin lo puedes: ahorrar o gastar en casi cualquier bien o servicio que quieras incluso lo puedes intercambiar por otras divisas, pero a diferencia de las otras esta es una divisa digital y descentralizada y pongamos énfasis en que es descentralizada, es decir, que a diferencia de las demás no depende de algún Estado o autoridad ni un Banco central. Si se le pone así podemos decir que es, de cierta manera como el oro en sus tiempos antiguos: cualquiera puede o podía, cavar y buscar oro, hacer sus monedas y con eso comprar lo que se le antojara, sin embargo, en esta época no puedes hacer transferencias digitales con el oro y en esta época globalizada e interconectada eso le da poder al bitcoin. Ahora, en un

plano más económico tenemos que el bitcoin contrasta con las demás divisas en lo que se trata de dinero fiduciario, no hay bancos centrales que toman decisiones después de analizar el panorama económico, no hay tasas de interés ni tampoco un movimiento de la masa monetaria a placer del banco central, los creadores lo diseñaron con una regla simple la masa monetaria del bitcoin es de 21 millones y esas a su vez se pueden subdividir en 8 y se van soltando en horarios específicos (normalmente 6 por hora). ¿Por qué el bitcoin? El control de las divisas normalmente recae en manos de unos pocos que deciden el rumbo de una parte importante de la economía, en el mundo del bitcoin se hace de manera distinta ya que, si una minoría está en desacuerdo con lo que se está haciendo pueden rechazar que no les gusta simplemente desconectándose de la red causando una separación del sistema que es peer-to-peer.

Cabe aclarar nuevamente que el tema es extenso y poco conocido, por eso se ha vuelto interesante e importante escribir sobre él, si bien al momento de presentar el trabajo siguen saliendo a diario noticias y nuevas criptomonedas, espero que esta tesina sea una herramienta útil para el futuro.

IV. Alcances.

Se pretende que el resultado de la presente investigación ayude a la comprensión de los alcances y de las limitantes que tiene la criptomoneda y el Bitcoin en el mundo financiero, también como se mencionó podrá ser una herramienta para saber cómo funciona el sistema de minado de criptomonedas y la estructura del Blockchain.

V. Objetivo General.

Comprender el contexto histórico de las criptomonedas, el blockchain y el bitcoin, así como el funcionamiento de todos sus mecanismos de transferencia y de obtención.

VI. Marco Teórico y Analítico

El marco teórico en este trabajo será más encaminado a una investigación de corte monográfico, este está elaborado a partir de la lectura y análisis de trabajos y textos en ingles en su mayoría, con unos pocos en el idioma español, es por eso por lo que se me hace impórtate hacer un trabajo de esta índole. En la facultad no encontré ninguna tesis que hablara sobre el tema, así como tampoco encontré libros que trataran el tema, aunque se piense que es una novedad, se me hace importante tener un trabajo de índole monográfica para tener noción del tema.

Por lo cual este trabajo teóricamente está fundamentado en nociones económicas muy elementales y generales, así como también trata temas informáticos y términos un poco más complicados para nosotros que no estudiamos ese tema, el lenguaje que se utilizara lo intentare hacer de lo más básico y comprensible para que cualquiera que sepa lo básico de la ciencia económica pueda entenderlo sin problemas.

Históricamente analizare y expondré el inicio del Bitcoin y de las criptomonedas, de las fuentes que encontré, así como de entrevistas, papers y noticias sobre Satoshi Nakamoto (el creador del Bitcoin), para así dar paso a la parte técnica y terminar

con unas cuantas conclusiones y argumentos económicos sobre el funcionamiento de los mecanismos del bitcoin.

En el primer capítulo se dará una introducción a las criptomonedas en donde se explicará: que son, cuáles son las diferentes criptomonedas, sus inicios y también si cuentan o no como dinero.

Para el segundo capítulo se tiene una explicación sobre el blockchain y el bitcoin, en primer lugar, se explica lo básico que hay que saber sobre estos 2 temas y la importancia de ellos y ahondando en el funcionamiento del blockchain el cual es parte medular de varias criptomonedas, explicando cuál es su objetivo y como es su funcionamiento dentro de todo este sistema.

En el capítulo final se tratan temas de índole más económica comenzando por el papel de las criptomonedas y su papel en la economía, sobre que virtudes tienen y también sobre cuáles son los riesgos de la adopción de estas, en este capítulo también cuenta con varias tablas y gráficos que explican cómo ha crecido el uso de estas divisas digitales y como se ha ido adoptando, así como cuáles son sus usos más comunes.

1. Capítulo 1.

INTRODUCCIÓN A LAS CRIPTOMONEDAS.

1.1. Criptomonedas

Desde el trueque el ser humano siempre ha intentado intercambiar objetos o servicios por otros de una equivalencia similar, este sistema al presentar dificultades para el intercambio dio paso a una nueva mercancía la llamada dinero-mercancía. Las monedas de metales preciosos fueron las primeras en llegar a ser aceptadas ampliamente debido a su facilidad de transportar, de usar y de su conservación.

El papel moneda fue el siguiente en llegar a manera de evolución necesaria para los estados. Sin embargo, debido a las crisis mundiales presentadas en la primera guerra mundial y el crack del 29 se hizo más difícil cambiar el papel moneda por metales preciosos, en Bretton Woods se estableció que todas las divisas se podrían transformar en dólares y esos dólares en oro. Para 1971 esto fue insostenible y se terminó la convertibilidad del dólar a oro. En 1973 el dinero se convierte puramente en dinero fiduciario.

Dinero electrónico: es el dinero que se emite de forma electrónica a través de la utilización de una red de computadoras, internet y sistemas de valores digitalmente almacenados, es normalmente un medio de pago digital equivalente a determinada moneda. En esta categoría tenemos a las criptomonedas.

No se puede hablar de criptomonedas sin mencionar el Bitcoin, el cual empezó a operar en enero de 2009 siendo esta la primera criptomoneda, la segunda en llegar llamada Namecoin llego hasta dos años después en abril de 2011. En la actualidad podemos encontrar cientos de criptomonedas por la red con valor de mercado y que están siendo intercambiadas, muchas otras han dejado de existir.

Lo que tienen en común las criptomonedas es la base de datos histórica conocida como “public ledger” o mejor conocido como el “blockchain” este se comparte entre todos los participantes de la red y se usan fichas “tokens” nativos como una manera

de incentivar a los participantes para seguir conectados en la red a falta de una autoridad central. Esto es a manera muy básica como funcionan, sin embargo, hay diferencias significativas entre criptomonedas.

La mayoría de las criptomonedas posteriores son clones del bitcoin y solo cambian alguna característica o bien cambia algunos parámetros de los valores para obtenerla, estas se llaman altcoins.

1.2. Las Diferentes Criptomonedas

- Bitcoin

La divisa digital con mayor valor en el mercado y también mayor intercambio, Satoshi Nakamoto invento el Bitcoin con un propósito, evitar usar una organización financiera como tercero. Su método tecnológico principal es el blockchain. Esta criptomoneda no está aliada a ninguna autoridad central y las transacciones están protegidas por una gran red computacional.

- Ethereum[1]

Plataforma computacional descentralizada que cuenta con su propio lenguaje. Los contratos de blockchain son ejecutados por cada participante en el nodo y son activados a través de los pagos por la criptomoneda “ether”

- Dash

Enfocado a la privacidad, fue lanzada en 2014, su precio de mercado ha aumentado significativamente en los últimos meses. En contraste con las demás criptomonedas, las recompensas del bloque se reparten equitativamente entre los

[1] Descripción de las criptomonedas excepto bitcoin fueron encontradas en el trabajo de la universidad de Cambridge *Global Cryptocurrency Benchmarking Study* (Hileman & Rauchs, 2017, pág. 17)

miners y los nodos maestros, el 10% de las ganancias se va a la tesorería para invertir en la plataforma.

- Ripple

La única criptomoneda que no usa un método de blockchain, en cambio una un "libro global de consenso". El protocolo de Ripple es usado por actores institucionales como bancos y negocios financieros. Su token nativo XPR sirve como divisa puente entre divisas nacionales que raramente se intercambian, así como también para evitar ataques de Spam.

- LiteCoin

Lanzada en el 2011 y es considerada plata mientras que el bitcoin sería el oro debido a que su límite total es de 84 millones. Comparte muchas similitudes con el bitcoin, pero sus parámetros clave (algoritmo de minado está basado en un Script)

- Monero

Criptomoneda que apunta a ofrecer dinero digital anónimo usando firmas de circulo, transacciones confidenciales y direcciones ocultas para ofuscar el origen, el nivel de transacción y el destino.

1.3. Los Inicios

"He estado trabajando en un nuevo sistema de dinero electrónico que es completamente peer-to-peer, sin ningún tercero a quien confiar" (Nakamoto, 2008)

La visión de un sistema puramente peer-to-peer para dinero electrónico dejaría que pagos en línea se pudieran mandar directamente de un lado a otro sin la necesidad de pasar por una institución financiera. Las firmas digitales podrían ser parte de la solución, pero estos beneficios si nuestro tercero sigue siendo requerido, la solución podría ser usar una red peer-to-peer. (Nakamoto, 2008)

El problema que encontró Nakamoto fue que el eCommerce estaba exclusivamente sostenido en las instituciones financieras funcionando como mediadores de los pagos electrónicos; si bien en la mayoría de los casos funciona bien hay todavía algunos problemas propios de los sistemas basados en la confianza. Por ejemplo, las transacciones no reversibles no son realmente posibles, las instituciones financieras no pueden evitar mediar en la disputa, el costo de mediación incrementa el costo de la transacción así limitando el costo mínimo de la transacción evitando gastos que podrían ser más casuales. Bajo esta condición los vendedores deben estar al tanto de sus clientes pidiendo más información de la que en realidad necesitan. Este tipo de problemas en su mayoría no existen cuando se paga con efectivo, pero hacerlo por un medio de comunicación sin un tercero en quien confiar no era posible.

La propuesta ingeniosa de Nakamoto fue crear un sistema basado en pruebas encriptadas en lugar de la confianza, dejando que dos partes interesadas pudieran transar directamente entre ellos sin la necesidad de un tercero. Transacciones que serían computacionalmente imprácticas de revertir protegerían a los vendedores del fraude y por el lado de los compradores se pueden poner en funcionamiento mecanismos de análisis de rutina.

El bitcoin no está simplemente limitado a un sistema de pagos simple, también su oferta está definida por el software y su protocolo. Solo veintiún millones de bitcoins existirán y para mayo de 2018 se han minado diecisiete, “El ultimo Bitcoin espera ser creado para el 2140 según especialistas.” (Champagne, 2014) Aunque parece que 21 millones son pocos para una población de siete mil millones de personas debo de aclarar que el bitcoin es altamente divisible, la denominación más pequeña se le llama Satoshi, la cual es 0.00000001 BTC, por lo tanto, tenemos 100 millones de satoshis en un bitcoin.

1.4 ¿Es Dinero?

“Lo hemos llamado concupiscible a causa de la violencia de los deseos que nos arrastran a comer, beber, al amor y a los demás placeres de los sentidos; y lo hemos llamado amigo de las riquezas, porque el dinero es el medio más eficaz para satisfacer esta clase de deseos.”

Platón. La República o El Estado (Humanidades) (Spanish Edition) (Posición en Kindle5918-5920). Grupo Planeta. Edición de Kindle.

Para definir si el bitcoin califica o no como dinero debemos situarnos en cuál es nuestra visión de dinero. Según la cita de Platón tenemos que el dinero puede ser cualquier cosa que nos facilite obtener lo que deseamos, si bien Platón nunca definió ciertamente si tenía que ser una moneda metálica, Aristóteles como buen discípulo continuo con esta línea de pensamiento y agrego la existencia de una sociedad no comunitaria implica el intercambio de bienes y servicios y si en un principio existe un trueque no siempre se puede intercambiar de manera justa o por lo que se desea; entonces este hecho inducirá a la gente a elegir una mercancía como medio de cambio; los metales acostumbran a ser escogidos por sus características de homogeneidad, divisibilidad, manejabilidad y estabilidad relativa del valor.

Se podría continuar con varias referencias y citar a muchos más autores sobre que es el dinero para cada uno, pero; eso no es el tema fundamental de esta tesina, brincaremos en el tiempo hasta encontrarnos con Karl Menger el cual en 1892 escribió sobre el dinero y sus orígenes, de lo más interesante que tiene este texto es que Menger afirma que:

“El dinero no se ha generado por ley. En su origen es de la sociedad, y no una institución estatal. Incluso la sanción que impone la autoridad es una alienación” (Menger, 1892)

En el mismo texto Menger acepta que si bien el Estado en ese momento ayudo a perfeccionar y facilitar el intercambio dando confianza a la moneda, aún hay bastantes dificultades que puede tener hacer pagos y transacciones; ya sea porque se tienen que intercambiar una divisa por otra para que te la acepten, el nivel de confianza que puede tener tu divisa o que simplemente no tenga un reconocimiento lo que deseas intercambiar.

Con esto podemos concluir que si bien el dinero de curso legal es el estándar no es la única manera, el dinero es lo que se acepta socialmente y desde sus orígenes ha estado desprendido del Estado.

Hay que aclarar que el dinero es necesario y tiene que cumplir 3 funciones fundamentales: ser unidad de cuenta, reserva de valor y medio de intercambio. El Bitcoin por lo tanto es considerado dinero, su demanda principal viene de actores económicos que necesitan un nuevo medio de pagos, descentralizado, semi anónimo y a diferencia del dinero fiduciario finito en su volumen.

Estas atribuciones le ganaron mala fama al bitcoin en sus inicios, ya que fue utilizada en los mercados negros del internet, como la ruta de seda de la deepweb, se dice que este mercado está bajo vigilancia y que el bitcoin ayudo a facilitar este tipo de transacciones.

A pesar de este estigma el bitcoin llego a ser de conocimiento popular y se transformó en una nueva forma de pago, la tarjeta Shift apoyada por Visa acepta pagos y transacciones con Bitcoin en donde sea que VISA opere. Mucha gente está a la expectativa de la volatilidad que tomara la moneda y se puede ver que en 2017 alcanzo su clímax de valor llegando a 17,900 Dólares por bitcoin para de ahí ir bajando gradualmente hasta más o menos la mitad de este valor, muchos estudiosos piensan que entre más pronto lleguemos al tope de los 21 millones el valor se estabilizara poco a poco.

Si bien el bitcoin por muchos detractores no califica como dinero debido a la falta de un gobierno que respalde su valor, tenemos que tomar en cuenta que las características principales las tiene y que ha funcionado de manera excelente para

lo que fue diseñado es decir: para hacer transferencias entre partidas de manera igual y sin tener que dar una cuota a un tercero, probablemente de los más beneficiados con esto han sido los que deben de mandar dinero al extranjero o recibirlo, así evitando las cuotas de empresas como Western Union.

También hay que destacar que el Bitcoin no es una deuda, no representa una obligación de nadie ni una promesa, como el dinero metálico, el bitcoin permite preservar la privacidad dejando la decisión en manos del dueño, a diferencia de los billetes o una cuenta bancaria el bitcoin es propiedad del dueño y solo de él.

Independientemente de la visión y la idea que tenga cada uno, si el bitcoin es dinero o no, si solo es una divisa liquida y si su valor está por verse siendo una moneda descentralizada, se me hace importante hablar sobre ella y su funcionamiento.

2. Capítulo 2.

Blockchain y el funcionamiento del Bitcoin.

2.1 Aspectos elementales.

En el sistema del bitcoin todos cooperan para mantener en vigilancia el dinero de los demás, no hay una autoridad central que intervenga. Todas las transacciones son llevadas a cabo por medio de computadoras que se comunican vía internet.

Como ya vimos antes la unidad principal es el bitcoin y también tenemos los Satoshi, en el mercado internacional se puede encontrar abreviado como BTC o XBT. Entre más valor gana el bitcoin más se ha dividido la unidad y los términos más comunes son los siguientes:

1 bitcoin = 1 BTC o XBT

1 BTC = 1,000 mBTC

1 mBTC = 1,000 µBTC

1 µBTC = 100 satoshis = 1 bit

Al principio se hizo mención sobre el public ledger o el libro de cuentas públicas, este indica el número de bitcoins y los dueños de ellos en cualquier momento, en lugar de asociar nombres de personas asociados a las cuentas, tenemos direcciones de bitcoin. Cada dirección puede ser a través de un seudónimo y por eso no es necesario revelar información personal.

Ejemplo de una dirección de bitcoin: **1FnLqyHm1sbdwFmCvJSHnJMEvanukT4gSN**

También estas direcciones pueden transformarse en códigos QR para solo escanearlos, de las cosas importantes a mencionar es que, si bien para mandar un bitcoin debes de tener forzosamente internet, para recibirlos puedes estar desconectado.

En la banca tradicional los movimientos normalmente se hacen actualizando su libro de cuentas privado y en el caso de que su información no esté respaldada o una catástrofe suceda se puede perder toda la información, lo más común son los ataques de hackers o los famosos robos de identidad. En el caso del sistema peer-to-peer esto se vuelve más complicado, porque se cuenta con un libro de cuentas con copias idénticas guardadas en millones de computadoras conectadas a la red por todo el mundo, esto evita el peligro que tiene el sistema centralizado, una sola transferencia manda una instrucción de actualización a todas las copias del libro. Esto podría ser un poco molesto por que si alguien sabe tu dirección puedes ser encontrado en todas las copias del libro del mundo, así como también podrán saber tus transacciones y cuanto tienes en tu balance, lo bueno es que puedes tener varias cuentas y mover entre ellas tu balance.

Para tener acceso a la cartera de bitcoin necesitas una llave privada, normalmente la llave privada es otro código generado por letras y números, digamos que si la dirección de bitcoin es tu cuenta la llave privada es como el PIN para acceder a tu cartera. Lo importante es que teniendo la llave privada puedes generar firmas digitales y cada transacción tiene una firma digital única, por lo tanto, no hay peligro que los demás sepan sobre tus transacciones, esto es fundamentalmente distinto a un pago con tarjeta en línea, cuando tu usa la tarjeta das información que es única de tu tarjeta lo que puede generar un uso malicioso de la misma.

Entender lo básico del funcionamiento del bitcoin es necesario para comenzar a entender el sistema del blockchain, si bien hay muchas pistas de cómo podría funcionar en las siguientes páginas se va a profundizar sobre tema.

2.2. El Blockchain.

Lo primordial para entender el blockchain es saber cómo se organizan y se estandariza la tecnología. Es importante considerar que un software es un sistema que se compone de capas.

Hay 2 maneras de particionar un sistema.

- Aplicación vs Implementación.
- Aspectos funcionales vs Aspectos no funcionales.

Todo lo que pertenece a la capa de aplicación es lo que necesita un usuario (mandar mensajes, escuchar música o ver un video).

Lo que pertenece a la capa de implementación se preocupa por hacer que las cosas pasen (reconocer colores para mandarlos a una pantalla, convertir señales digitales en acústicas o mandar los datos por internet).

En la capa funcional tenemos mandar datos por la red, reproducir música o un video. De aspectos no funcionales tenemos una interfaz gráfica bonita, software rápido o mantener la seguridad del sistema. Una analogía fácilmente reconocible es decir que, los aspectos funcionales son los verbos que describen las acciones y los aspectos no funcionales son los adverbios los que describen como se hace esa acción.

La integridad es de los aspectos más importantes de la capa no funcional cuando hablamos de software. Los 3 componentes más importantes son los siguientes:

La integridad de los datos: los datos usados y mantenidos por el sistema tienen que estar completos, correctos y libres de contradicciones.

- Integridad de comportamiento: El sistema se tiene que comportar como se diseñó y debe de estar libre de errores lógicos.
- Seguridad: el sistema debe poder restringir el acceso a los datos solo a usuarios autorizados.

Con lo anteriormente aprendido podemos empezar a descifrar un sistema, en este caso el sistema de pagos. Lo representare con una tabla.

TABLA 1: ASPECTOS Y CAPAS DE UN SISTEMA DE PAGOS.

Capa	Aspectos Funcionales	Aspectos no-Funcionales
Aplicación	Depositar dinero Sacar dinero Transferir dinero Monitorear el balance de cuenta	La interface gráfica de usuario es estética Fácil de usar Transferir dinero es rápido El sistema cuenta con muchos participantes
Implementaciones	? (aquí normalmente va el motor que se implementara en el sistema)	Disponible las 24 horas del día Antifraudes Mantiene su integridad Asegura la privacidad de usuario

Fuente: Daniel Drescher. Blockchain Basics (Posición en Kindle278). Apress, Berkeley, CA.

Dos tipos de arquitectura de sistema.

Existen bastantes maneras de implementar un sistema de software, de las cosas más importante es definir qué tipo de arquitectura tendrá, y existen 2 formas fundamentales: la centralizada y la distribuida.

En los sistemas centralizados, los componentes están localizados alrededor y conectados con un componente central. En el caso de los sistemas distribuidos forman una red de componentes conectados sin tener un centro.

ILUSTRACIÓN 1: ARQUITECTURA CENTRALIZADA, DESCENTRALIZADA Y DISTRIBUIDA.

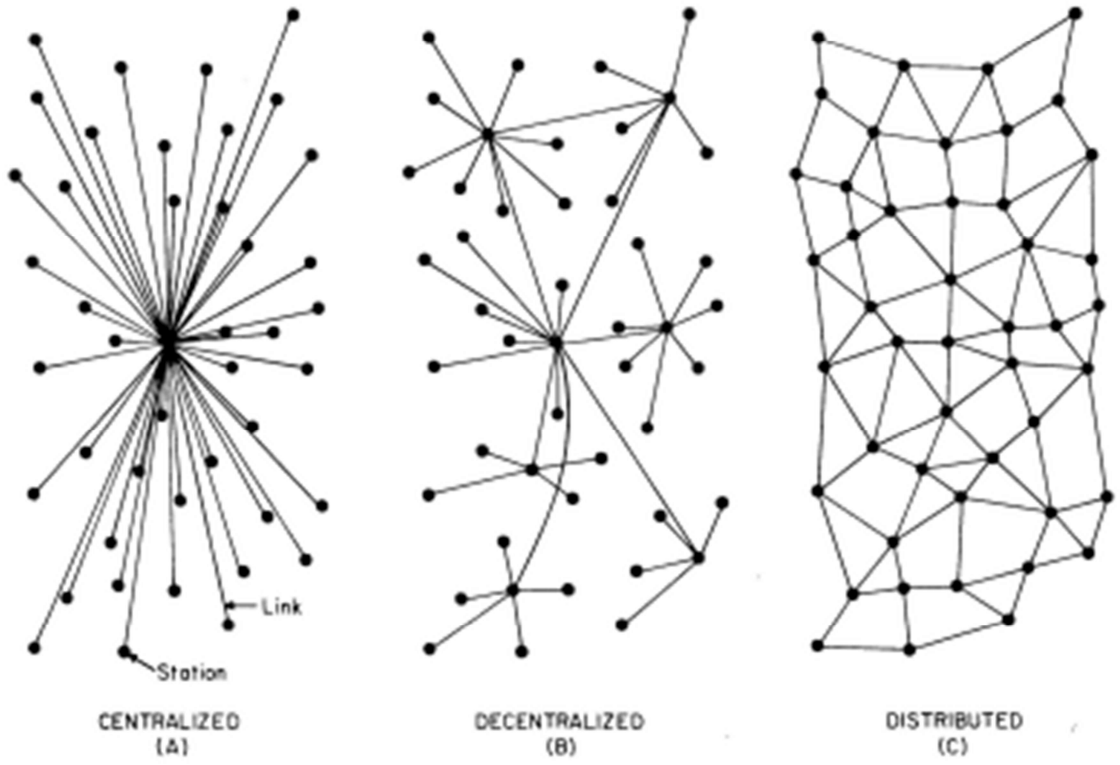


FIG. 1 — Centralized, Decentralized and Distributed Networks

Fuente de la ilustración: (Baran, 1964, pág. 2)

Las ventajas que tiene un sistema distribuido sobre un centralizado son 3 principalmente:

1. Mayor poder computacional
2. Menor costo
3. Mayor confianza

Habilidad de crecer naturalmente

Las desventajas que un sistema distribuido tienen son las siguientes:

1. Coordinación de un superior
2. Comunicación de un superior
3. Dependencia de las redes
4. Mayor complejidad para programar
5. Problemas de seguridad

Los 2 primeros problemas yacen en que no existe una entidad central que coordine y comunique con los demás entes de la red, el tercer problema hace referencia a que las computadoras deben de estar conectadas para que funcione su comunicación, los otros 2 problemas se explican por sí mismos.

2.2.1. El propósito del blockchain

Cuando se diseña un sistema de software, uno debe elegir con que arquitectura se va a hacer y esto es independiente de los aspectos funcionales de las capas funcionales y de aplicación, pueden existir programas idénticos con distintas arquitecturas.

Depende de la arquitectura que se elija se obtendrán los objetivos de distintas maneras, cada uno de ellos tiene maneras distintas en cuanto a la aproximación a cómo manejar la integridad del sistema.

Aquí es donde el blockchain entra en juego: el blockchain es una herramienta para conseguir integridad en un sistema distribuido, puede ser visto como una herramienta para lograr un aspecto no funcional de la capa de implementación.

Como ya se había adelantado en el primer capítulo el sistema peer-to-peer es fundamental en el funcionamiento de varias criptomonedas, el sistema peer-to-peer consiste de computadoras las cuales ponen sus recursos computacionales disponibles para otros. Las ventajas de estos sistemas es su habilidad de dejar a los usuarios interactuar directamente en lugar de pasar por intermediarios, por este medio los sistemas peer-to-peer incrementan la velocidad de procesamiento y reducen los costos.

Los sistemas peer-to-peer distribuidos forman una red de miembros iguales que interactúan directamente uno con el otro sin una coordinación central, un ejemplo que viene a la mente de hace ya unos años son los programas que funcionaban para bajar la música como: Napster, Ares, Limewire o los torrents, estos demostraron el poder de los sistemas peer-to-peer, eliminando intermediarios como disqueras y tiendas de discos, dando espacio a los productores para interactuar directamente con los consumidores.

Una parte importante del sistema financiero actual es una intermediación entre los abastecedores de dinero y los consumidores, mucho de ese es un bien inmaterial y digital, por ende, una digitalización y la adopción del sistema peer-to-peer puede cambiar el panorama financiero, así como paso con la música. El Blockchain se está transformando en una herramienta para mantener la integridad de sistemas puramente peer-to-peer y dar así la oportunidad de transformar industrias eliminando la intermediación.

El termino blockchain puede ser ambiguo para mucha gente e incluso para alguien que conoce más o menos del tema aun es complicado definirlo, muchas veces el termino depende de la persona a la que le preguntes y el contexto que ellos tienen.(Drescher, 2017)

El blockchain puede referirse a lo siguiente:

1. Una estructura de datos
2. Un algoritmo
3. Un portafolios de tecnologías
4. Un grupo de sistemas que distribuyen por medio del peer-to-peer y tienen un área de aplicación común. (Posición en Kindle680)

La aplicación más prominente del blockchain es gestionar y clarificar la propiedad, pero no es la única.

El blockchain es un sistema peer-to-peer con libros (Ledgers) que utiliza una unidad de software que consiste en un algoritmo, el cual negocia la información contenida en bloques de datos conectados y ordenados de manera conjunta para encriptarlos y asegurarlos para mantener así su seguridad.

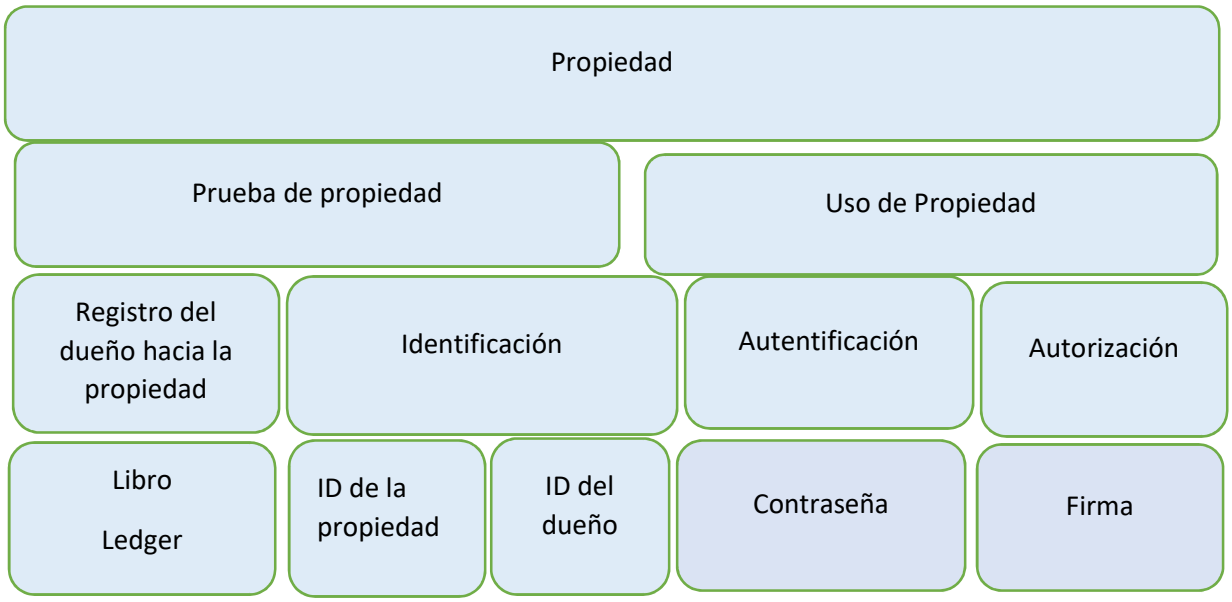
La propiedad.

Definir propiedad, primordialmente consta de 3 elementos.

1. Identificar al propietario
2. Identificar el objeto del cual se es propietario
3. Un registro del dueño hacia el objeto

Ahora un diagrama para entender mejor la propiedad nos servirá en el futuro para entender más sobre el tema.

ILUSTRACIÓN 2: CONCEPTOS DE PROPIEDAD



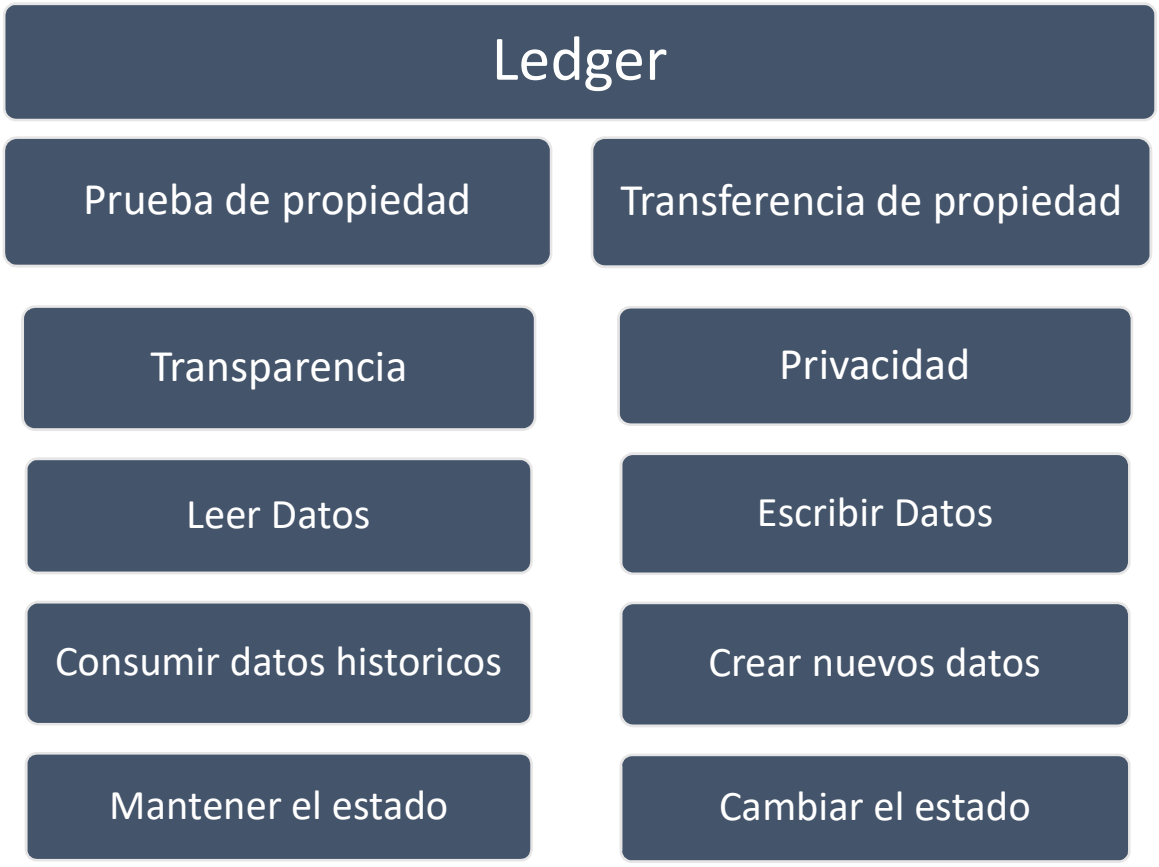
Fuente: (Drescher, 2017)

En cuanto a seguridad tenemos 3 conceptos de importancia para comprender el tema.

1. Identificación: reclamar ser alguien o algo por medio de cierto identificador. La identificación no prueba que realmente eres lo que dices, solo que eres cierta persona.
2. Autenticación: El propósito es prevenir que alguien mienta sobre quien es, esto significa comprobar que realmente eres quien dices, normalmente se hace por medio de algo que este únicamente conectado a tu persona.
3. Autorización: Te da acceso a recursos o servicios específicos dadas las características ir propiedades de tu identidad, estas es consecuencia de la autenticación.

Conocer estos conceptos nos ayuda a comprender mejor el Ledger, el cual tiene como función llenar dos roles opuestos. Por una parte, comprobar la propiedad, la cual esta guardada en una base de datos históricos preservados, y por otro lado este tiene la facultad de dar permiso a la transferencia de propiedad, lo cual implica que nuevos datos están entrando y siendo escritos en él.

ILUSTRACIÓN 3: CONCEPTOS Y PRINCIPIOS DE UN LEDGER



Fuente: (Dannen, 2017)

La relación que tiene el libro de cuentas o ledger con el sistema de blockchain es la siguiente:

1. Un único libro es usado para mantener la información de propiedad, lo que equivale a una sola estructura del blockchain guardando datos de propiedad.
2. Los libros son guardados en los nodos (computadoras) del sistema peer-to-peer
3. El algoritmo blockchain es responsable de dejar que los nodos individuales colectivamente lleguen a una versión consistente del estado de propiedad y dependiendo de esto se basa el veredicto
4. La integridad en este sistema es la habilidad de hacer una declaración verdadera acerca de la propiedad
5. La criptografía es necesaria para crear medios fidedignos de identificación, autenticación y autorización para crear seguridad en los datos.

Hay que recalcar que cuando se habla del doble gasto nos referimos a 2 cosas.

1. Un problema causado por copiar bienes digitales
2. Un problema que puede aparecer en Ledgers peer-to-peer

En este caso nos referimos a la vulnerabilidad de los Ledgers en los sistemas de distribución peer-to-peer. El blockchain es un medio para resolver estos problemas de doble gasto.

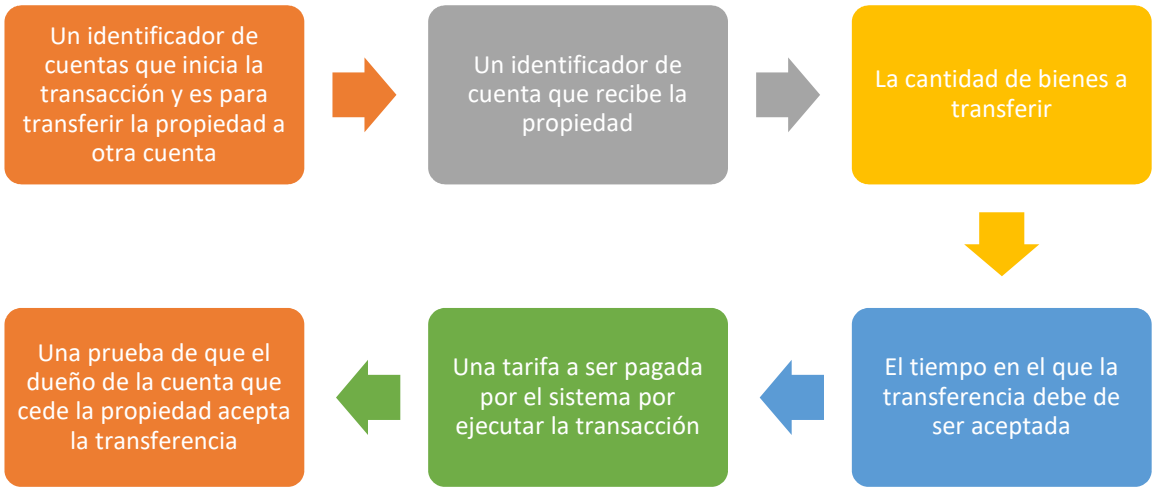
Para diseñar un sistema peer-to-peer de distribución de Ledgers que gestionen propiedad se deben asignar las siguientes tareas:

1. Describir la propiedad
2. Proteger la propiedad de accesos no autorizados
3. Guardar la información de las transacciones

4. Preparar los Ledgers para ser distribuidos en medios poco confiables
5. Formar un sistema de Ledgers para transferirlos
6. Agregar y verificar nuevas transacciones en los Ledgers
7. Decidir que Ledgers representan la verdad

La transferencia de datos proporciona la siguiente información para describir la transferencia de propiedad:

ILUSTRACIÓN 4: TRANSFERENCIA DE PROPIEDAD



Fuente de los datos para la ilustración: (Bheemaiah, 2017)

El historial completo de los datos de transacción es una auditoria que provee evidencia de cómo la gente adquiere y cede propiedad, cualquier transacción que no está en ese historial se toma como que jamás existió.

Para mantener integridad, solo los datos de transacción son agregados a la estructura de datos del blockchain y deben cumplir con estos 3 criterios: Exactitud formal, exactitud semántica y la autorización.

2.2.2 Las Funciones Resumen

Las funciones resumen o “Hash” transforman cualquier tipo de datos en un numero de longitud fija, independientemente de los datos de entrada y existen varios tipos de función que difieren entre otras con respecto al valor hash que producen.

Las funciones criptográficas hash son un importante grupo de funciones resumen que crean firmas digitales para cualquier tipo de datos, estas funciones tienen las siguientes propiedades:

1. Dan valores hash para cualquier dato de manera rápido.
2. Determinantes.
3. Pseudoaleatorias.
4. Uso unilateral.
5. Resistentes a la colisión.

La aplicación de funciones hash a los datos pueden ser logradas usando los siguientes patrones: hash repetitivo, hash independiente, hash combinado, hash secuencial, hash jerárquico.

Estos valores pueden ser usados: para comparar datos, para detectar si los datos se supone que quedaron sin cambiar o han sido alterados, para referirse a los datos en una manera de cambio sensitiva, para guardar una colección de datos, para crear tareas intensivas computacionalmente.

La criptografía que se obtiene gracias a las funciones hash hace difícil que una persona no autorizada accede a los datos, las actividades de mayor importancia en la criptografía son: la encriptación la cual protege los datos haciéndolos ilegibles y le des encriptación la cual descifra esos datos utilizando una llave criptográfica.

La criptografía asimétrica siempre usa dos llaves complementarias las cuales se necesitan para acceder, cuando utilizamos en la vida cotidiana este tipo de

criptografía tenemos una llave publica la cual encripta la información y solo el dueño de la llave privada correspondiente la puede leer y viceversa.

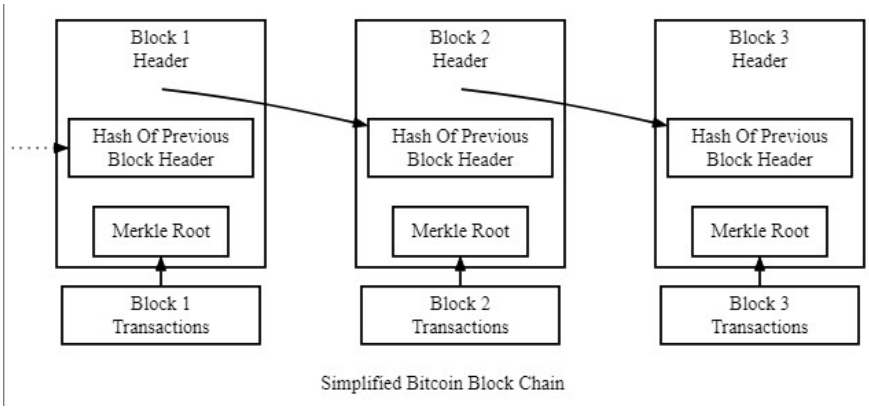
El blockchain utiliza este medio para cumplir dos metas fundamentales:

1. Identificar cuentas: las cuentas son llaves criptográficas públicas.
2. Autorizar transacciones: el dueño de la cuenta que transfiere propiedad crea un texto cifrado con las correspondientes llaves privadas y esta solo puede abrirse cuando llega a emparejarse con la llave pública correspondiente.

La función de estas llaves es para proveer una firma digital única que esta encriptada por medio de un hash específico. Estas firmas digitales en el blockchain pueden rastrear una transferencia de esa única llave privada.

Lo que intenta hacer el blockchain es mantener todo el historial de transacciones de manera ordenada. Las unidades principales son llamadas bloques, cada bloque del blockchain contiene un encabezado y un árbol de Merkle

ILUSTRACIÓN 5: BLOCKCHAIN SIMPLIFICADO



Fuente: (Bashir, 2017, pág. Posicion de Kindle 1850)

Los encabezados dan la apariencia de una ficha de biblioteca digital, donde cada tarjeta esta acomodada a como fue agregada a la librería, tener este encabezado hace que se preserve el orden de cada bloque, estos se identifican por su valor

criptográfico hash y contiene una referencia al encabezado precedente para mantener el orden y este a su vez esta guardado en la raíz del árbol de Merkle.

Los pasos para cambiar los datos del blockchain son complejos a propósito para evitar fraudes o disputas, su naturaleza es radical y es de todo o nada, se cambia toda la estructura de datos o no se hace nada, para agregar nuevas transacciones se tienen que seguir estos pasos en orden:

1) Crear un nuevo árbol de Merkle que contiene los datos de las nuevas transacciones.
2) Crear un nuevo encabezado que contiene el hash de referencia del encabezado anterior y la raíz del árbol de Merkle que contiene los datos de la nueva transacción.
3) Crear una referencia hash en un encabezado nuevo, el cual es el primero en la estructura blockchain actual.

Por este intrincado sistema el blockchain protege el historial de las transacciones para que no se puedan manipular, este historial se hace inmutable a partir de las siguientes dos ideas:

- Guardar la información de transacciones de un modo sensible a los cambios, el cual cuando es cambiado necesita reescribir los datos desde el punto de cambio hasta el encabezado de la cadena.
- Requerir la solución del hash para escribir, reescribir, o agregar cada encabezado de todo el blockchain. El hash de cada bloque es único por cada encabezado, lo que hace una tarea titánica cambiar cada hash de cada encabezado tomando en cuenta que este contiene el código de este bloque más el del bloque anterior.

Se había mencionado que el sistema peer-to-peer es el ideal para que funcione este sistema, las razones son las siguientes: utiliza el internet el cual crea una red omnipresente, cada computadora tiene una dirección única, aunque estas se

conecten o desconecten no hay problema en algún momento recibirán una actualización, la comunicación se lleva por medio de “chisme” es decir; cada nodo (computadora) recibe el mensaje y este lo mandara a sus pares de la misma manera, los duplicados entonces serán filtrados según sus valores hash, cada nodo puede ordenar la información dependiendo el encabezado y la estampa de tiempo de cada bloque.

El sistema peer-to-peer siempre está conectado, crea nuevas conexiones y distribuye nueva información.

El algoritmo del blockchain está basado en los siguientes conceptos:

1) Validar las reglas para los datos de transacción y encabezados de bloque
2) Premiar a usuarios por mandar bloques validos de las siguientes maneras: evaluar bloques nuevos creados por otros, e intentar ser el nodo que crea un nuevo bloque.
3) Castigo por atentar contra la integridad del sistema
4) La competencia entre pares se basa en la velocidad de procesamiento

Por estas razones es más fácil ser un nodo sano que intenta ser premiado a ser un nodo malintencionado que necesita ser más rápido que las demás computadoras de la red.

TABLA 2: CAPAS DE APLICACIÓN E IMPLEMENTACION DEL BLOCKCHAIN

Capa	Aspectos Funcionales	Aspectos no-funcionales
Aplicación	Aclarar propiedad. Transferir propiedad.	Altamente disponible. Confiable. Abierto. Pseudo anónimo.
Implementación	Lógica de propiedad. Seguridad de transacción. Lógica de procesamiento de transacción. Lógica de almacenaje. Lógica de consenso. Arquitectura puramente peer-to-peer.	Seguro. Resiliencia. Consistente en eventualidades. Mantener integridad.

Fuente: Elaborada a partir de los datos anteriores.

3. Capítulo 3.

Criptomonedas y la economía.

Como ya se mencionó antes el bitcoin bien puede ser usado como dinero habrá que hacer unas anotaciones extra sobre el tema.

La escuela austriaca es la que más conviene para hablar sobre este tema, ellos creían que el dinero emergía de una competencia entre varios medios de cambio, el más aceptado va a ser el que quede como dinero, los otros medios pueden coexistir y se les puede llamar cuasidinero, también creían que la inflación proviene del incremento de la oferta monetaria, y para combatir la inflación es necesario el progreso tecnológico o por disminución de la oferta monetaria, por lo tanto podríamos decir, que ellos estaban a favor de una oferta monetaria fija.

El teorema de regresión de Mises, bajo esta idea tenemos que el valor de una divisa se deriva de que los usuarios asumen que esta mantendrá su valor con el paso del tiempo. Una divisa tiene valor hoy por que los propietarios esperan poder usarlo mañana para obtener bienes y servicios, y a su vez el valor de hoy es el reflejo del valor de ayer, si volvemos en el tiempo alguna vez esa divisa tuvo su valor respaldada en una *commodity* de donde tomo el valor. Entonces tenemos que el dinero fiduciario toma valor del dinero respaldado por metales preciosos.

El dinero digital toma valor del dinero fiduciario, el concepto de dinero digital según el Comité de Pagos y de Infraestructura de mercados es: valor guardado electrónicamente en un dispositivo como el chip de una tarjeta o un disco duro en una computadora personal. Este concepto se ha ido ampliando y se han incluido ya varios mecanismos de medio de pago digitales. Las criptomonedas podrían entrar en categoría de dinero electrónico, pero en la mayoría de las jurisdicciones no satisfacen legalmente el concepto. Por ejemplo: la mayoría del valor del dinero digital debe estar reflejado y poder ser transferido a una divisa soberana, en el caso de las criptomonedas estas tienen un valor en sus propias unidades y la mayoría son activos con un valor determinado por oferta y demanda, similar a commodities

como el oro, la diferencia es que las commodities es el valor intrínseco. Por lo que tenemos comprobado el teorema de regresión de Mises.

Tal vez la innovación más fuerte que está asociada con las divisas digitales o criptomonedas es el sistema de pagos el cual es el blockchain el cual se explicó ampliamente en el capítulo 2. Gracias a este esquema basado en Ledgers se tiene una red fuerte que puede trabajar de forma descentralizada y con bajo riesgo de falla. Este sistema bien podría ser adoptado por los bancos y así apuntar a una mejora en la eficiencia de ciertos problemas con los que a veces se cuentan.

Si bien este es uno de los factores importante para el auge de las criptomonedas y de las divisas digitales, existen otras características que han estimulado la innovación en el sistema de pagos "tradicional" como la reducción del costo y el incremento en la velocidad de transacciones, sobre todo en las áreas de comercio electrónico y transacciones internacionales.

Por el lado de la demanda en su mayoría son instituciones privadas y no bancarias las que buscan ganar con las criptomonedas y las divisas digitales, estas ganancias pueden venir de: revender la divisa, aceptar transacciones y cobrar cuotas, así como por medio de intermediación. Los puntos que podrían influenciar el futuro de las divisas digitales son los siguientes[2]:

- Fragmentación: se cuenta que existen más de 600 y el numero va aumentando, pueden contar con distintos protocolos de: transacción y confirmación, así como distintos modos a su límite de oferta. Esta diversidad puede ser la que ayude o afecte a llegar a un sistema definitivo.
- Escalabilidad y eficiencia: debido a su escala limitada el número de transacciones que se procesa actualmente está lejano a la magnitud que tiene el sistema tradicional, sin embargo; con el auge que se ha presentado en los últimos años se puede observar que si es posible soportar un alto número de transacciones simultaneas. En cuanto a eficiencia conforme la tecnología siga evolucionando y abaratándose hará

[2] (Infrastructures, 2015, p. 7)

que sea posible tener mayor poder computacional y con ello acelerar el crecimiento de la red digital.

- Pseudo-anónimo: Este punto ya lo discutí al principio, dejando de lado factores morales el blockchain da la oportunidad de hacer transacciones anónimas evitando así ser víctima de fraudes, robos de identidad o robo de cuentas, si bien como explique en el capítulo anterior, hay un registro de todas las transacciones de todas las personas, la encriptación hace posible que puedas mantener tu identidad a salvo.
- Preocupaciones técnicas y de seguridad: el mayor problema que aquí encontramos es que las redes pequeñas de criptomonedas y divisas digitales tienen que crecer para tener más copias en sus Ledgers y así llegar al consenso de saber cuáles son los datos correctos.

Por el lado de la demanda tenemos que las innovaciones de los Ledgers públicos han influenciado en la preferencia de los usuarios.

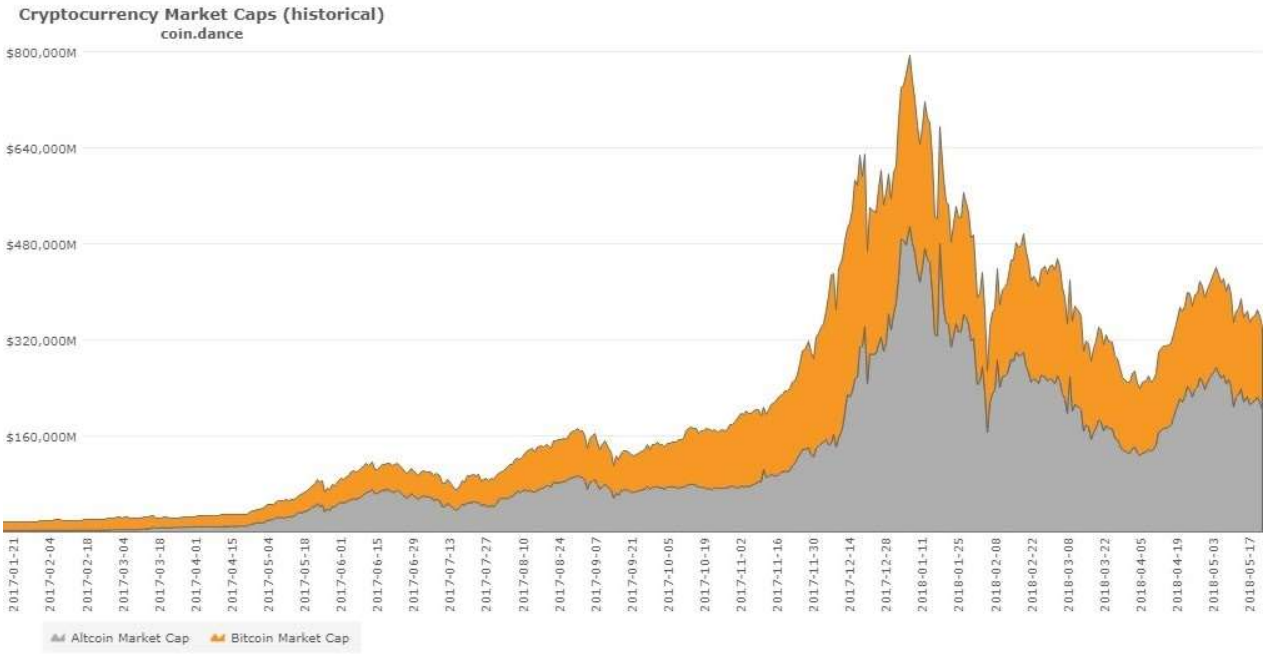
- Seguridad: el principal punto por el lado de la demanda de las divisas digitales es que al estar basado en el blockchain tenemos seguridad extra a que, si se usara un sistema centralizado con una sola base de datos, a parte existen los nodos que son “testigo” de todo movimiento que se haga, lo cual provee de seguridad al usuario en caso de tener una disputa.
- Costo: Las tarifas de transacción son menores que con otros métodos de pago y en algunos esquemas se llega a premiar por tan solo ser parte del bloque creado o por revisar una versión correcta del mismo, por esta razón estos esquemas son atractivos para los usuarios y para los proveedores, sin olvidar la eliminación de intermediarios.
- Usabilidad: Es como usar dinero fiduciario solo que, en otra divisa, con el avance y la mayor adopción esto se va haciendo cada vez más común y fácil.
- Peligro de perdida y volatilidad: En este caso tenemos un contra de las divisas digitales y en general de cualquier otra divisa, el problema es que

esta puede ser más frágiles frente a ataques especulativos, si no se tiene completo conocimiento del mercado el usuario puede perder o ganar debido a lo volátil que está siendo el activo.

- Irrevocabilidad: la naturaleza del ledger hace que sea complicado hacer malas jugadas.
- Velocidad: las divisas digitales normalmente hacen transacciones más rápido que los sistemas centralizados, esto dependerá del tamaño de la red y del poder computacional total de la misma.
- Privacidad y anonimato.

El usuario ha encontrado varios beneficios en las criptomonedas y en las divisas digitales, Bitcoin siendo el líder desde el principio de esta etapa.

ILUSTRACIÓN 6: CAPITALIZACIÓN DE MERCADO

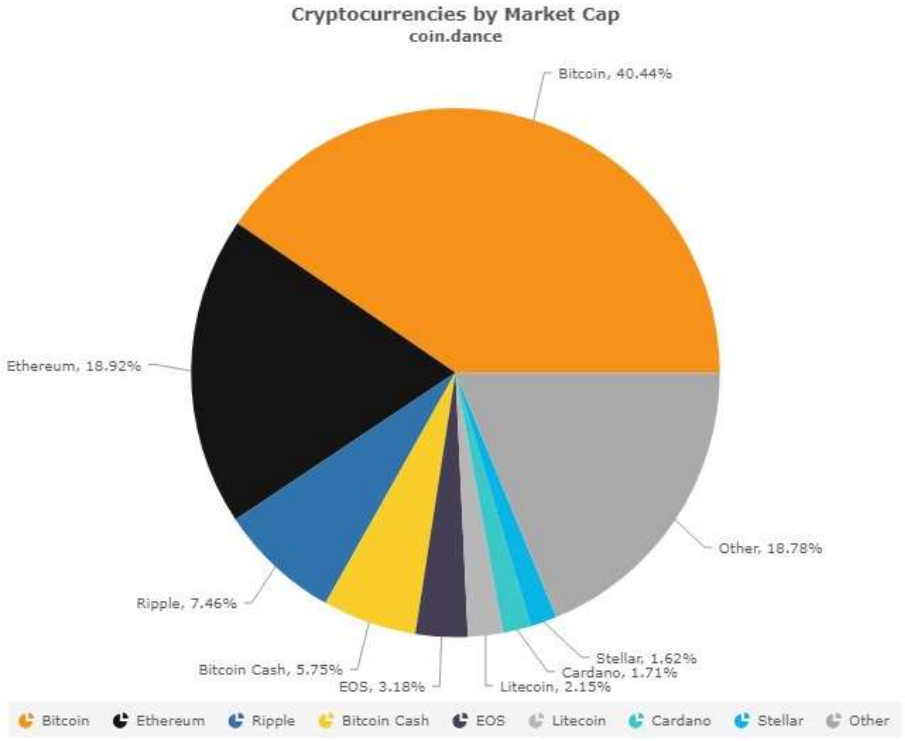


Fuente: Datos de (coindance, 2018)

Como se puede observar en la **ilustración 6** la capitalización de mercado combinada de todas las criptomonedas ha crecido desde tener un valor aproximado de 40 mil millones en enero de 2017 hasta el pico en los últimos días de diciembre de ese mismo año y principios de enero de 2018 con valores que llegaron casi a los 800,000 millones de dólares, para ir descendiendo poco a poco teniendo una capitalización combinada de casi 420,000 millones de dólares para mayo de 2018. También se puede apreciar que si bien el bitcoin fue líder en la primera etapa el interés que genero este provocó un interés por otro tipo de criptomonedas las que incluso han llegado a estar igualadas o han superado al bitcoin en capitalización de mercado. La criptomoneda que tiene mayor competencia con el bitcoin es Ethereum la cual se liberó en julio del 2015 y para marzo del 2016 ya contaba con una capitalización del mercado del 10% del total[3] mientras que bitcoin tenía el 80%, en la gráfica 7 la cual se encuentra en la siguiente página, se puede observar como Ethereum ha ido ganando terreno frente al bitcoin llegando a subir al 18.92% y bitcoin ha perdido bastante hasta llegar al 40.44%. Esta pérdida del bitcoin se debe al surgimiento de nuevas criptomonedas, caída del valor del bitcoin y también a que conforme se va acercando poco a poco a los 21 millones de unidades de bitcoin se va haciendo más complicado minar nuevos bloques.

[3] Según los datos de CoinMarketCap

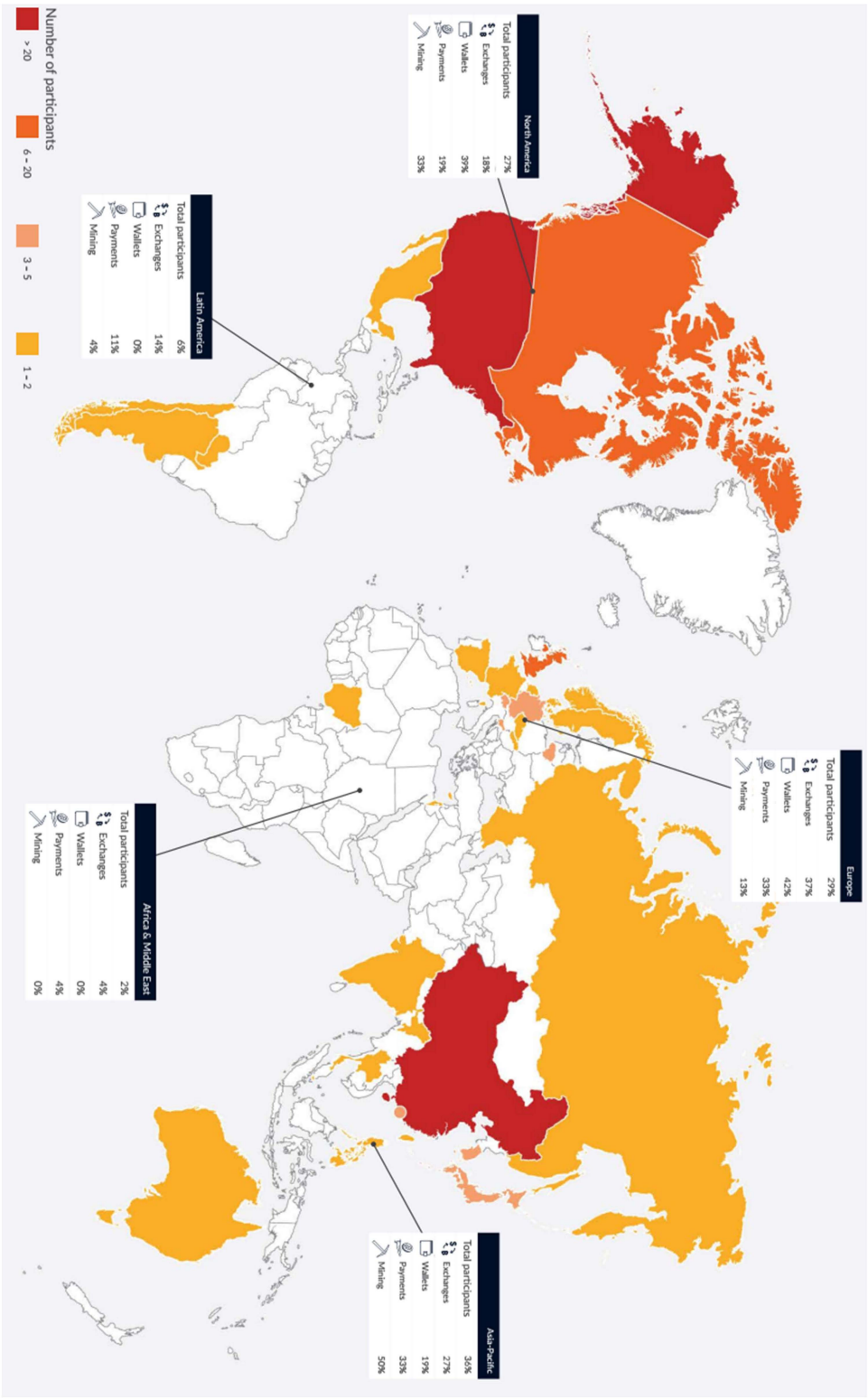
ILUSTRACIÓN 7: CAPITALIZACIÓN DE MERCADO EN PORCIENTO POR CRIPTOMONEDA



Fuente: (coindance, 2018)

En el grafico 8, podemos observar un mapa de la distribución de participantes en el uso de las criptomonedas: el rojo representa países con mayor uso de ellas, hasta llegar al blanco en el cual la participación es nula, si bien los datos son de marzo del 2017, el panorama no ha cambiado mucho, tenemos en primer lugar que donde más penetración han tenido las criptomonedas es en Asia teniendo el 36% y también teniendo la mayor participación en minado con 50%, esto es debido a que China siendo el país productor más grande de hardware de computadora junto con Corea del Sur y Japón siendo fuertes participantes tecnológicos tienen el poder computacional para minar en grandes cantidades. En segundo lugar, esta Europa el cual cuenta con un 29% y teniendo la mayor participación en carteras con un 42% esto debido a lugares donde la fiscalización o la legislación de las criptomonedas aún no está tipificada por la ley. El siguiente es Norte América donde se encuentra el 27% donde el minado tiene un 33%, las carteras un 39% los intercambios un 18%

ILUSTRACIÓN 8: DISTRIBUCIÓN GEOGRÁFICA DE PARTICIPANTES.



Fuente: (Hileman & Rauchs, 2017).

y los pagos un 19%, esto se debe en el caso del minado a que Estados Unidos y Canadá son grandes consumidores de electrónicos, México en los últimos años ha tenido un auge importante en este rubro pero no se compara a los vecinos del norte mientras que en carteras muchas páginas están registradas en estos países para dar mayor "confianza" a los usuarios que quieran tener ahí sus criptomonedas, en cuanto a pagos e intercambios veremos más adelante las divisas más importantes por las cuales se intercambian las monedas. En penúltimo lugar se encuentra América Latina la cual tiene una participación del 6% siendo sus ramas más importantes los intercambios con un 14% y los pagos con un 11%. En último lugar esta África y medio oriente con apenas una participación del 2% y solo aceptando pagos e intercambios ambos con el 4% del total mundial.

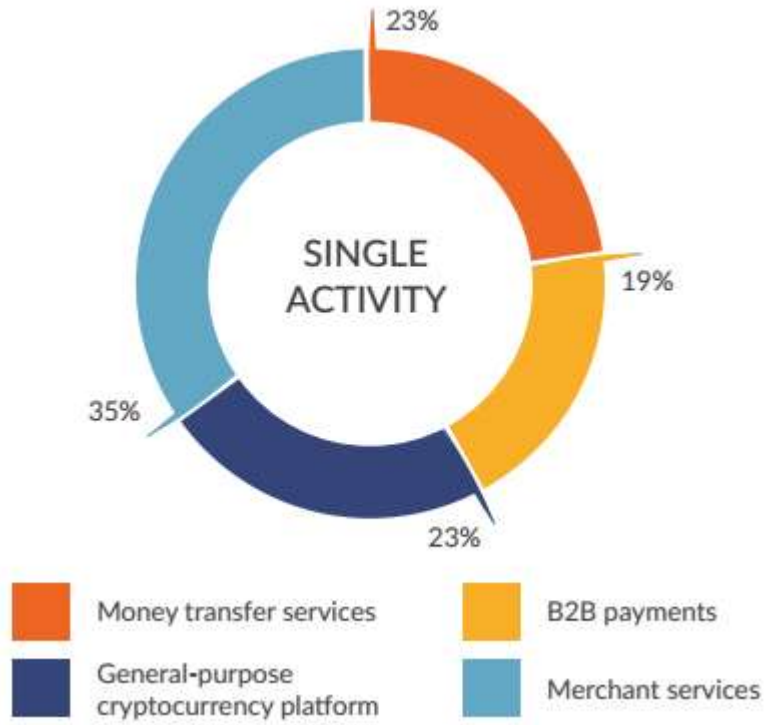
TABLA 3: TAXONOMIA DE LAS PRINCIPALES PLATAFORMAS DE PAGO

Caso de Uso	Actividad de Pago	Descripción
Carril de pago (usa las criptomonedas para ahorrar tiempo y dinero en transferencias internacionales de divisas nacionales)	Servicios de transferencia de dinero.	Servicios que principalmente se dedican a transferencias internacionales para individuos, están denominadas en divisas nacionales. Estas incluyen remesas tradicionales y pagos de facturas.
	Pagos B2B	Plataformas que facilitan de pagos a negocios, denominadas en divisas nacionales, muchas de las veces se hacen a través de fronteras.
Pagos en criptomonedas.	Servicios Mercantiles	Servicios que procesan pagos para mercaderes que aceptan criptomonedas. Puede ofrecer servicios mercantiles adicionales como un carrito de compras o puntos de ventas.
	Plataformas de propósito general para criptomonedas.	Plataformas que ejecutan una variedad de transferencias de criptomonedas, incluido el pago instantáneo a otros usuarios de la plataforma, nómina y otros servicios. Estos pagos también pueden ser cambiados por divisas nacionales.

Fuente: (Hileman & Rauchs, 2017)

Con la tabla de anterior como guía se puede dar idea de cómo funciona el sistema de pagos con criptomonedas y cuál es su uso en el mercado, la mayoría de los usos que se le dan a estas es para servicios mercantiles, con los comerciantes aceptando pagos en criptomonedas y los clientes comprando con estas, la mayoría de las plataformas que se usan permiten, comprar, guardar y transferir, otras compañías aceptan pago de servicios o incluso remesas y el menor porcentaje lo tienen los pagos de empresas B2B.

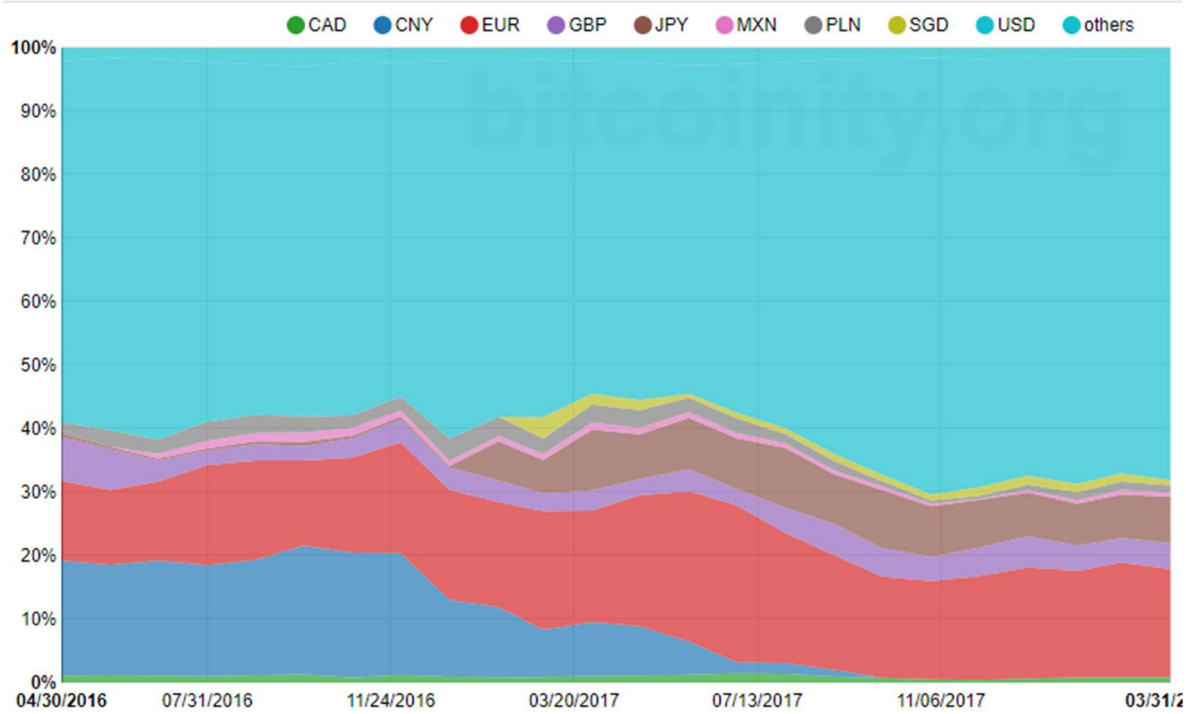
ILUSTRACIÓN 9: PORCENTAJE DE ACTIVIDADES DE LAS PLATAFORMAS DE PAGO



Fuente: (Hileman & Rauchs, 2017)

Como ya se mencionó en la tabla 3, muchas de las transacciones que se hacen con criptomonedas también involucran el uso de monedas nacionales, a continuación, un gráfico con las principales divisas utilizadas en los intercambios, sorpresivamente el peso mexicano esta normalmente en el puesto número cinco de intercambio, a veces sobre pasando al dólar canadiense.

ILUSTRACIÓN 10: PRINCIPALES DIVISAS INTERCAMBIADAS POR BITCOIN



Fuente: (Bitcoinity, 2018)

Según Daniel Vogel el presidente de Bitso afirma que esto es debido a que muchos mexicanos no tienen oportunidad de acceder a ciertos servicios financieros como tarjetas de crédito o cuentas de banco, la mayoría de los casos eran jóvenes adultos que no tenían acceso a tarjetas y prefieren comprar bitcoins para hacer compras en línea. (Connell, 2017).

Los 5 segmentos que se encuentran según el son los siguientes.

- Los que quieren invertir en la bolsa cantidades pequeñas, según él eso es imposible en la BMV.
- Comercio electrónico.
- Especulación.
- Remesas.
- Productos alrededor de la plataforma Bitso.

Otra de las razones que expone es que desde la devaluación que ha sufrido el peso mucha gente prefiere comprar bitcoins como activo para no perder tanto como ha perdido el peso, muchas de estas personas son gente que está viviendo temporalmente en los estados unidos o simplemente es gente en México que prefiere tener su ahorro en criptomonedas esperando a que el valor del bitcoin no se desplome.

Ω. Conclusiones.

Durante este texto se tuvo la razón de exponer de la manera más simple y comprensible para cualquier persona, cuáles son las razones por las que las criptomonedas son dinero, en específico el bitcoin. Si bien pueden existir detractores, escépticos o simpatizantes, bien podemos decir que bajo la teoría de la escuela austriaca nos encontramos ante una nueva forma de dinero que ha sido aceptada y está creciendo conforme pasan los años, han llegado nuevos miembros a la competencia que ayudan a mejorar la tecnología y la manera de asegurar un mejor mercado digital, así como también han llegado muchos astutos charlatanes que solo copian el funcionamiento pero no tienen la misma seguridad o simplemente ven a quien estafar, puedo afirmar que conforme pase el tiempo solo las mejores criptomonedas perduraran.

En cuanto al blockchain durante este trabajo de ardua investigación, se explicó su forma de funcionamiento que aunque es compleja se intentó hacer comprensible de la mejor manera, fue menester explicar el blockchain debido a que es la base de la mayoría de las grandes criptomonedas circulando en este momento y se ha llegado a la conclusión de que es un sistema de seguridad y encriptamiento que llego para quedarse, sus pros sobrepasan por mucho a sus contras teniendo este copias digitales en fichas repartidas por todo el mundo, haciendo que sea muy difícil actuar de manera maliciosa; si bien el blockchain premia a los nodos con mayor poder computacional y la oportunidad para que un usuario común y corriente pueda minar bitcoins se hace cada vez mínima, no es imposible gracias a la gran comunidad que se ha creado alrededor de este nuevo tipo de divisa digital.

En cuanto al ámbito económico se tiene que los usuarios buscan evitar la intermediación de los bancos para facilitar sus necesidades de consumo o de hacer llegar de activos a otras personas, sin mencionar que buscan seguridad y proteger su identidad. En el caso de México y de otras regiones encontramos que las personas acuden a este tipo de activos por falta de atención del sector financiero

bancario el cual no les ofrece una opción para satisfacer sus necesidades como consumidores o vendedores.

El tema es complicado y poco frecuentado, así como también da para una infinidad de páginas y textos sobre él. Se ha logrado hacer un trabajo de investigación y se ha elegido lo que es más importante para este texto y sud fines, podemos aventurarnos a dar un vistazo a lo que depara el futuro, y preguntarse. ¿Si esta nueva forma de dinero es quien va a sustituir a lo que existe actualmente? Eso es solo cosa de tiempo para saberlo, de lo que hay certeza es que el blockchain llegó para quedarse y evolucionar según las necesidades de los usuarios.

Anexos

Bibliografía.

Baran, P. (1964). *Memorandum RM-3420-PR.* California: The Rand Corporation.

barski, C., & Wilmer, C. (2015). *Bitcoin for the befuddled.* San Francisco: No Starch press.

Bashir, I. (2017). *Mastering Blockchain.* Livery Street: Packt.

Bheemaiah, K. (2017). *The Blockchain Alternative.* Paris: Apress.

Bitcoinity. (22 de Mayo de 2018). *Bitcoinity*. Obtenido de https://data.bitcoinity.org/markets/rank/2y?c=c&t=ae

Bonneau, J., Miller, A., Clark, J., Narayan, A., Kroll, J., & Felten, E. (2015). SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. United States.

Caetano, R. (2015). *Learning Bitcoin.* Birmingham: Packt Publishing.

Champagne, P. (2014). *The Book Of Satoshi.* United States: e53 Publishing.

Chiu, J., & Koeppl, T. (2017). The Economics of Cryptocurrencies.

coindance. (22 de mayo de 2018). *coindance*. Obtenido de https://coin.dance

Connell, J. (2 de Enero de 2017). *Bitcoin.com.* Obtenido de https://news.bitcoin.com/why-volume-is-exploding-at-mexican-bitcoin-exchange-bitso/

Dannen, C. (2017). *Introducing Ethereum and Solidity.* New York: Apress.

Drescher, D. (2017). *Blockchain Basics.* Frankfurt: Apress.

elBitcoin.org. (2014). *Bitcoin La moneda del futuro.* elBitcoin.org.

Feenstra, R. C. (s.f.). *Macroeconomia internacional.* Barcelona: Reverté.

Franco, P. (2015). *Understanding Bitcoin.* West Sussex: John Wiley & Sons.

Garay, J. A., Kiayias, A., & Leonardos, N. (2017). The Bitcoin Backbone Protocol:.

Hileman, G., & Rauchs, M. (2017). *Global Cryptocurrency Benchmarking Study.* Cambridge: University of Cambridge.

Infrastructures, C. o. (2015). *Digital currencies.* Bank for International Settlements.

Kelly, B. (2015). *The Bitcoin Big Bang.* New Jersey: John Wiley & Sons.

Krugman, P. R. (s.f.). *Economia Internacional.* Espana: Pearson.

Menger, K. (Jun de 1892). On the Origin of Money. (R. E. Society, Ed.) *The Economic Journal*, 239-255. Obtenido de https://is.muni.cz/el/1456/podzim2009/MPE_MOEK/um/8972262/menger1892.pdf

Nakamoto, S. (Noviembre de 2008). *Bitcoin: A Peer-toPeer Electronic Cash System.* www.bitcoin.org.

Platon. (2013). *La republica o El Estado.* Barcelona: Planeta.

Poon, J., & Dryja, T. (2016). The Bitcoin Lightning Network:.

Prusty, N. (2017). *Building Blockchain Projects.* Birmingham: Packt.

Szmigielski, A. (2016). *Bitcoin Essentials.* Livery Place: Packt Publishing.

Viglione, R. (2015). Does Governance Have a Role in Pricing? Cross-Country Evidence from Bitcoin Markets. *University of South Carolina - Department of Finance.* South Carolina.

Gráficos y tablas.