UNIVERSIDAD DE QUINTANA ROO
DIVISIÓN DE CIENCIAS E INGENIERÍA

BLOCKCHAIN Y LAS CRIPTOMONEDAS ACTUALES

TRABAJO MONOGRÁFICO
PARA OBTENER EL GRADO DE

INGENIERO EN REDES

PRESENTA
JOHN SU

SUPERVISORES
MTI. VLADIMIR VENIAMIN CABAÑAS VICTORIA
MSI. LAURA YÉSICA DÁVALOS CASTILLA
DR. JAVIER VÁZQUEZ CASTILLO

CHETUMAL QUINTANA ROO, MÉXICO, NOVIEMBRE DE 2018

UNIVERSIDAD DE QUINTANA ROO
DIVISIÓN DE CIENCIAS E INGENIERÍA

TRABAJO MONOGRÁFICO TITULADO

"BLOCKCHAIN Y LAS CRIPTOMONEDAS ACTUALES"

ELABORADO POR

JOHN SU

BAJO SUPERVISIÓN DEL COMITÉ DE SUPERVISIÓN Y APROBADO COMO REQUISITO PARCIAL PARA OBTENER EL GRADO DE:

INGENIERO EN REDES

COMITÉ DE SUPERVISIÓN

SUPERVISOR: _____

MTI. VLADIMIR VENIAMIN CABAÑAS VICTORIA

SUPERVISORA: _____

MSI. LAURA YÉSICA DÁVALOS CASTILLA

SUPERVISOR: _____

DR. JAVIER VÁZQUEZ CASTILLO

Universidad de Quintana Roo

DCI DIVISIÓN DE CIENCIAS E INGENIERÍA

CHETUMAL QUINTANA ROO, NOVIEMBRE DE 2018

Agradecimientos

A la primera persona que le quiero agradecer es mi asesor Vladimir Veniamin Cabañas Victoria, que sin su ayuda y conocimientos no hubiese sido posible realizar este proyecto. A mis padres, por haberme proporcionado la mejor educación y lecciones de vida. En especial a mi padre Chien-Tao, por haberme enseñado que con esfuerzo, trabajo y constancia todo se consigue, y que en esta vida nadie regala nada. En especial a mi madre Feng-Pi, por cada día hacerme ver la vida de una forma diferente y confiar en mis decisiones. A mis compañeros de clase, con los que he compartido grandes momentos. A mis amigos por estar siempre a mi lado y compartiendo sus experiencias conmigo. A todos mis familiares, por su apoyo. En especial a mi abuelo, por haberme aportado todo desde pequeño. A todos aquellos que siguen cerca de mí y que le regalan a mi vida algo de ellos.

Dedicatoria

A mi familia, principalmente mis padres por su apoyo incondicional brindado durante este proceso, que sin duda alguna no fue fácil no solo para mí, sino para ellos. Que con su esfuerzo, juntos hemos logrado esta meta. A ustedes que día a día me demostraron que no existen barreras cuando quieres lograr algo, que las adversidades no son impedimentos, que cada logro es una gran contribución para crecer emocionalmente, laboralmente, pero sobre todo como ser humano. Que con su humildad y entrega han hecho de mí, una persona con valores, capaz de demostrar a los demás una gran esencia de humildad, con lo que sin duda alguna voy a ejercer esta profesión de todo corazón sin nunca olvidar de dónde vengo y hacia donde quiero llegar.

Resumen

El presente trabajo de investigación consiste en la descripción y comprensión del uso de la tecnología de cadenas de bloques (Blockchain) basadas en qué es, cómo funciona, por qué es muy confiable y por qué las personas deberíamos usarla.

La investigación se realizó con base en la revisión de bibliografía y artículos escritos por expertos en el tema, obteniendo información de diversas fuentes en línea dedicadas a la investigación e implementación de Blockchain y las criptomonedas actuales.

En el capítulo 1 se describen las razones para realizar esta investigación, los objetivos particulares y el cronograma de actividades.

En el capítulo dos, se describen los principales conceptos y el funcionamiento de Blockchain a nivel general, para después explicar su implementación en criptomonedas actuales, como Bitcoin, Litecoin y Ethereum.

El capítulo 3 contiene mi opinión acerca de las tecnologías implicadas en Blockchain y explico el por qué considero que es una gran tecnología, confiable y que se puede implementar en diversos ámbitos de la vida humana.

Contenido

Índice de figuras

Capítulo 1 Introducción

1.1 Introducción

Las organizaciones públicas y privadas basadas o no en tecnologías, las personas, los equipos informáticos, las aplicaciones, etc. utilizan bases de datos centralizadas en muchas de las actividades que realizan. Los bancos son un claro ejemplo de ello, ya que utilizan una red de base de datos centralizada para mantener toda su información bancaria.

Las actividades de mercadeo, votaciones políticas, información de salud, y un largo etc. utilizan mayormente bases de datos centralizadas; esto nos lleva a la siguiente cuestión: ¿Alguna vez ha pensado en lo que sucederá cuando la persona encargada (o entidad, organización o empresa) de la base de datos cambie la información, lo sabrá alguien?

En los bancos, ¿por qué a los hackers les resulta relativamente fácil obtener datos y cambiarlos para obtener dinero de manera ilícita?

Este problema es realmente simple, la razón es porque es una base de datos centralizada. Si alguien cambia los datos en su interior, puede pasar desapercibido o demorar mucho tiempo en darse cuenta de que hay un cambio desconocido en la base de datos.

¿Alguna vez has pensado en una base de datos descentralizada.

Es un tipo de forma de mantener la base de datos, pero no de una sola persona. En este tipo de mantenimiento, cualquier persona puede tener una copia de todos los registros de los datos. Eso significa que cualquiera que quiera cambiar los datos en su interior tendrá que cambiar los datos en cada persona que posea una copia de la base de datos.

1.2 Justificación

Cuando Satoshi Nakamoto, cuya verdadera identidad aún se desconoce, lanzó el libro blanco Bitcoin: un sistema de efectivo electrónico de igual a igual en 2008 que describió la "versión puramente paritaria de efectivo electrónico" conocida como Bitcoin, la tecnología Blockchain (Cadena de bloques) hizo su debut público.

Blockchain, la tecnología que ejecuta Bitcoin se ha convertido en la última década en una de las tecnologías más innovadoras con el potencial de impactar todas las industrias, desde la financiera hasta la manufacturera y las instituciones educativas. Bitcoin fue ofrecido a la comunidad de código abierto en 2009; brinda la respuesta a la necesidad de confianza digital porque registra información importante en un espacio público y no permite que nadie la elimine.

Es transparente, con sello de tiempo (timestamp) y es descentralizado. Actualmente, hay muchos que creen que Bitcoin y Blockchain son lo mismo, aunque no lo son. Aquellos que comenzaron a darse cuenta alrededor del año 2014 que la tecnología de Blockchain podría usarse para algo más que criptomonedas, comenzaron a explorar y desarrollar innovadoras formas de cómo Blockchain podría cambiar muchos tipos diferentes de operaciones.

En esencia, Blockchain es un gran libro abierto y descentralizado que registra transacciones entre dos partes de manera permanente, sin necesidad de autenticación de terceros. Esto crea un proceso extremadamente eficiente y, según algunas personas, reducirá drásticamente el costo de las transacciones. Cuando algunos empresarios entendieron el poder de Blockchain, hubo una oleada de inversiones y descubrimientos para ver cómo ésta podría afectar las cadenas de suministro (scm), la atención médica, los seguros, el transporte, la votación, la gestión de contratos y más. [1]

1.3 Objetivo General

Describir el proceso de Blockchain, resaltando el por qué debería ser utilizado y por qué puede ser confiable; ejemplificando con la implementación de las criptomonedas actuales.

1.3.1 Objetivos Particulares

i. Identificar los principales componentes de la tecnología Blockchain
ii. Describir el funcionamiento de Blockchain
iii. Describir los mecanismos de confiabilidad de la Blockchain
iv. Ejemplificar el uso de la tecnología de bloques a través de la implementación de las criptomonedas como Bitcoin

1.4 Metodología:

- Elegir cuál será el tema sobre el cual se investigará, puesto que esto ayuda a delimitar los documentos que deberán consultarse.
- Recopilar una lista de títulos (Bibliografía) que puedan –según el criterio del investigador- proporcionar información básica e importante para la Investigación a realizarse.
- Leer y consultar de forma rápida el primer material recopilado.
- Revisar nuevamente el tema escogido, y proceder a su máxima delimitación, a fin de realizar una investigación especializada.
- Con base en el material bibliográfico y el ámbito delimitado sobre el que se realizará la investigación, el investigador deberá realizar un esquema de actividades, que le permitan orientar las distintas tareas que deberá realizar.
- Así mismo, la delimitación del tema llevará al investigador deba ampliar su bibliografía, buscando textos que amplíen el tema escogido de forma especializada.
- Cuando se tengan los documentos bases sobre los que se sustentará la investigación, se deberá entonces proceder a la lectura minuciosa de éstos.

- Ya con el proceso de lectura realizado, el investigador deberá realizar una serie de fichas de contenido, que le garanticen durante el desarrollo de la investigación científica, la recuperación y consulta rápida de los documentos que vaya necesitando.
- Realizado lo anterior, se deberán cotejar las fichas con el esquema de trabajo, a fin de organizar y disponer el fichero según las distintas fases que pretenden abordarse durante la investigación.
- Finalmente, el investigador puede proceder a la redacción de su marco teórico, así como a la elaboración del resto del trabajo, en caso de que éste contemple también una fase de praxis, análisis y registro.

1.5 Alcance

El Blockchain es una invención innegablemente ingeniosa, se descubrió que podría usarse para más que criptomonedas y explorar cómo la Blockchain podría alterar muchos tipos diferentes de operaciones. Vamos a investigar cómo funciona exactamente la tecnología Blockchain, para qué se puede usar, qué tan confiable es y algunas de las criptomonedas actuales como Bitcoin, Litecoin y Ethereum.

Tabla 1 Cronograma de Actividades

Actividad	Cronograma 2018																													
	Enero		Febrero				Marzo				Abril				Mayo				Junio				Septiembre				Octubre			
Selección de tema																														
Revisión bibliográfica																														
Elaboración de Anteproyecto																														
Elaboración del Marco Teórico																														
Elaboración de Conclusiones																														
Revisión de supervisores																														
Presentación de examen																														

Capítulo 2 Marco Conceptual

2.1 Tecnología Blockchain

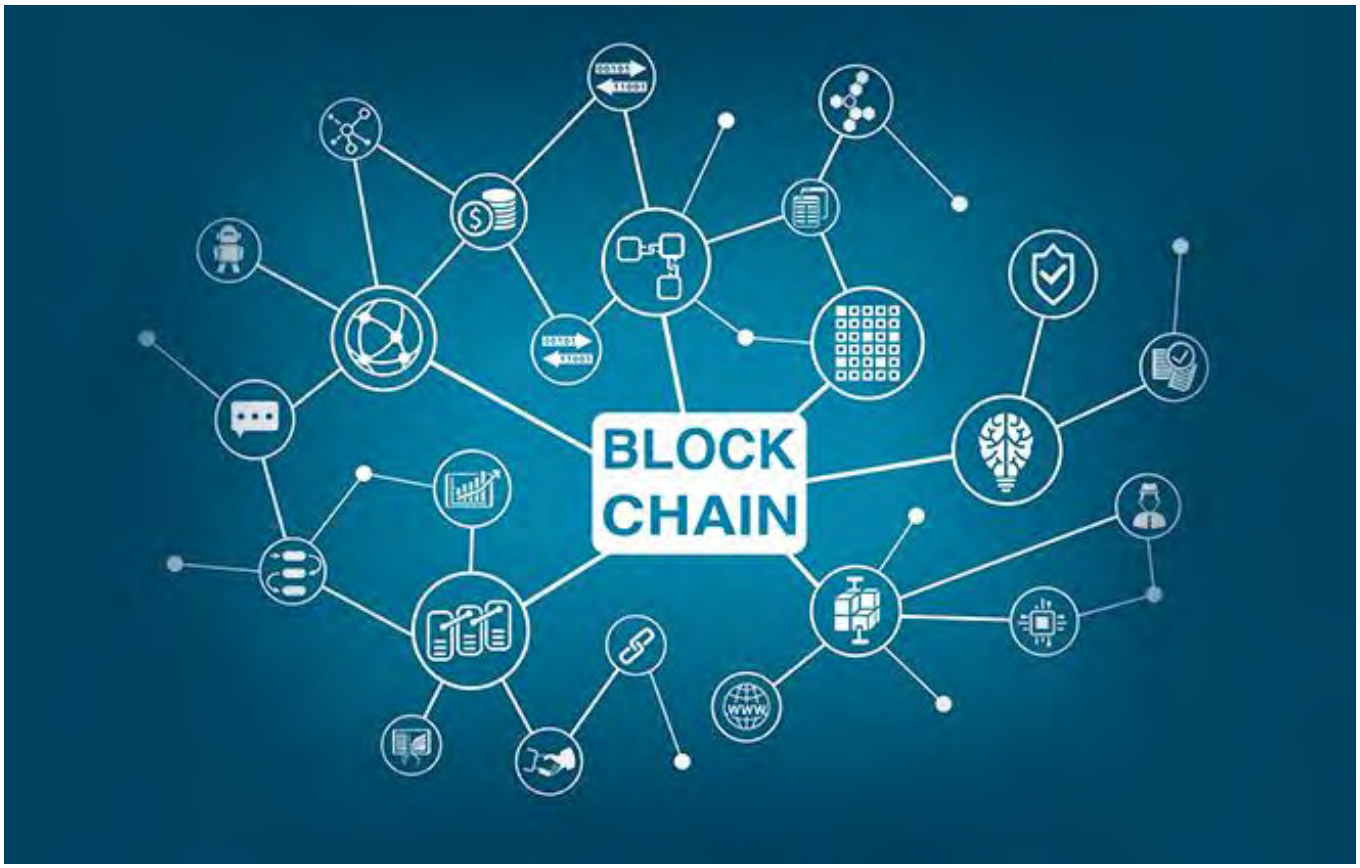

Figura 1 Blockchain (https://youteam.co.uk/blog/wp-content/uploads/2018/05/Blockchain.png)

A pesar de ser desconocido para el público en general, Blockchain es uno de los secretos del éxito y el valor de Bitcoin (una criptomoneda que al tipo de cambio de noviembre de 2018 equivale a $ 95,300.00 MXN). Tiene una historia de décadas, pero comenzó a aparecer en las noticias hace menos de 10 años. Eso es todo gracias a Satoshi Nakamoto, quien decidió basar la mecánica de Bitcoin en Blockchain. [2]

¿Qué es Blockchain?

Blockchain es como un libro de contabilidad electrónico que puede ser compartido de manera abierta para una gran cantidad de usuarios y que va grabando todas las transacciones que se apuntan en ella, sin que exista manera de modificarlas, ya que cada una de las partes de la cadena están contienen datos del bloque anterior de manera tal que se encuentran enlazadas con el bloque anterior.

Cada una de las transacciones se conoce como bloque, de ahí su nombre, y permite tener un libro de contabilidad electrónico en el que muchos usuarios pueden participar de manera abierta y controlada, ya que cada uno de los bloques está vinculado a ese usuario específico.

Una de sus grandes ventajas es el nivel de seguridad que ofrece, ya que esta tecnología impide que los datos registrados puedan ser borrados o modificados una vez que éstos han sido publicados. Esto otorga a este sistema una fuente confiable y fidedigna de todas y cada una de las transacciones hechas en el sistema. [3]

¿Para qué sirve Blockchain?

Al ser una red peer-to-peer, combinada con su capacidad para marcar en el tiempo todas las transacciones y que se puede gestionar de manera autónoma los intercambios de información entre los distintos participantes lo convierte en una herramienta ideal para todo tipo de empresas; ya que no hay necesidad de que exista un administrador, sino que todos los usuarios son los administradores. [3]

Blockchain es un registro público en el que las transacciones entre dos usuarios que pertenecen a la misma red se almacenan de forma segura, verificable y permanente. Los datos relacionados con los intercambios se guardan dentro de bloques criptográficos, conectados jerárquicamente entre sí y esto crea una cadena interminable de bloques de datos.

La función principal de Blockchain es, por lo tanto, certificar transacciones entre personas. En el caso de Bitcoin, ésta sirve para verificar el intercambio de criptomonedas entre dos usuarios, pero es solo uno de los muchos usos posibles de esta estructura tecnológica.

En otros sectores (por ejemplo el comercial), Blockchain puede certificar el intercambio de acciones, puede operar como si fuera un notario y "validar" un contrato; en el ámbito electoral podría ser un mecanismo que ayude a que los votos emitidos en una votación en línea sean confiables y casi imposibles de alterar. [4]

¿Por qué Blockchain es seguro?

Una de las mayores ventajas de Blockchain es el alto grado de seguridad que garantiza. De hecho, una vez que una transacción se certifica y se guarda dentro de uno de los bloques de cadena, ya no se puede modificar ni alterar. Cada bloque consta de un puntero que lo conecta al bloque anterior, una marca de tiempo que certifica la hora en la que el evento realmente tuvo lugar y los datos de la transacción.

Estos tres elementos aseguran que cada elemento de la Blockchain sea único e inmutable, cualquier solicitud para modificar la marca de tiempo o el contenido del bloque cambiaría todos los bloques subsiguientes. Esto se debe a que el puntero se crea con base en los datos en el bloque anterior, lo que desencadena una reacción en cadena real. Para que ocurra cualquier modificación, sería necesario que el 50% más una de la red aprobase el cambio: una operación posible pero difícilmente viable, ya que la Blockchain se distribuye por todo el mundo entre millones de usuarios. [2]

Blockchain es una tecnología que ha demostrado su valía, pero eso no significa que se haya aplicado en todas partes, es una herramienta increíblemente versátil y capaz de tocar una amplia gama de industrias, cada una muy diferente de las demás. [2]

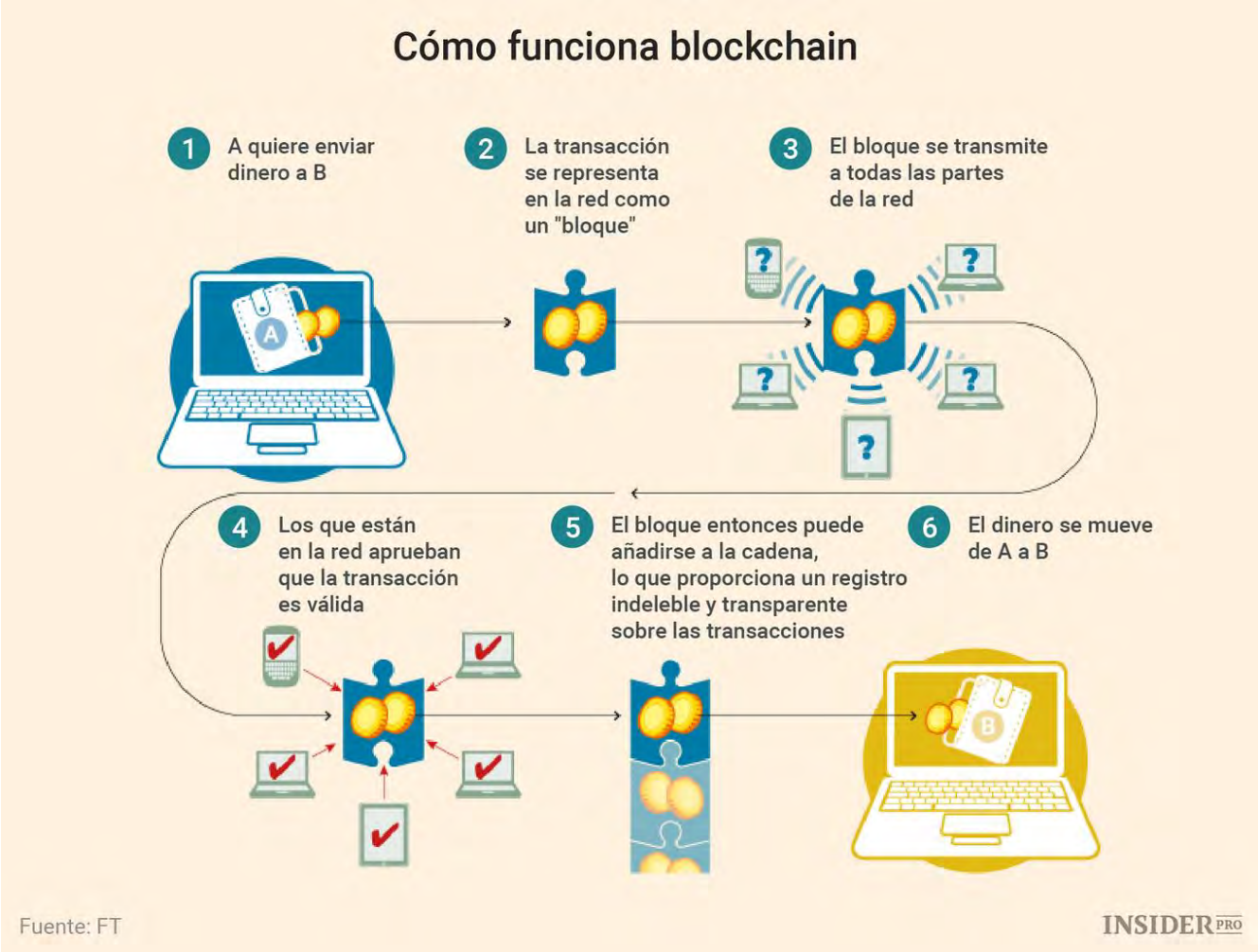

Figura 2 Funcionamiento de Blockchain (https://i.blogs.es/eb1a62/Blockchain/1366_2000.png)

Blockchain y la privacidad

No es necesario que los datos personales y los identificadores se almacenen específicamente en la red. El sistema transforma la información, como el nombre, el número de teléfono, la dirección de correo electrónico y las contraseñas, en un valor numérico de una longitud fija, denominado valor hash en términos informáticos. Los datos se procesan para proporcionar un token único que se puede indexar y recuperar rápidamente en una base de datos, pero que hace que el usuario sea prácticamente anónimo para todas las partes de la cadena. [5]

Áreas de impacto

La industria financiera es generalmente el usuario más activo de Blockchain, pero no es la única industria que la aprovecha, en el tema de la identidad digital, hay experimentos interesantes que apuntan a otorgar una identidad y derechos a los refugiados a nivel transnacional, proporcionándoles escrituras de propiedad basadas en esta tecnología.

En términos de derechos y transferencia de propiedad, sus aplicaciones de la tecnología Blockchain son numerosas y potencialmente revolucionarias. Eso también es cierto en la ciudad inteligente y el Internet de las cosas, donde el Blockchain es muy valioso para certificar la confiabilidad de la información transmitida por objetos y sensores.

Con respecto a los plazos de impacto de la "revolución de la Blockchain", es necesaria una distinción. Cuando una sola empresa o un pequeño grupo de empresas pueden actuar sin tener que tocar el marco legislativo y normativo, veremos los primeros resultados en el año. Si requiere grandes acuerdos dentro del ecosistema de referencia o en el nivel legislativo, obviamente llevará más tiempo. [2]

2.2 Aplicaciones de Blockchain

La tecnología Blockchain es una revolución en los sistemas de registro. La naturaleza de la tecnología Blockchain hace que la imaginación se vuelva loca, porque la idea ahora se puede aplicar a cualquier necesidad de un registro confiable. También está poniendo todo el poder de la criptografía en manos de las personas, impidiendo que las relaciones digitales requieran una autoridad de transacción para lo que se consideran 'transacciones de extracción'. [6]

Blockchain como sistema de registro se puede usar para:

1. **Identidad digital**

Las claves criptográficas en manos de individuos permiten nuevos derechos de propiedad y una base para formar relaciones digitales interesantes. Debido a que no se basa en cuentas y permisos asociados con cuentas, porque es una transacción push y porque la propiedad de claves privadas es propiedad del activo digital, esto coloca una forma nueva y segura de administrar la identidad en el mundo digital que evita exponer usuarios a compartir demasiada información personal vulnerable. [6]

2. **Tokenización**

A los efectos de autenticar un elemento físico único, los elementos se vinculan con un token digital correspondiente. Esto esencialmente significa que se usan tokens para unir los mundos físico y digital. Estos tokens digitales son útiles para la gestión de la cadena de suministro, la propiedad intelectual y la detección de falsificaciones y anti-falsificación. [6]

3. **Gestión de datos interorganizacional**

La tecnología Blockchain representa una revolución en la forma en que se recopila la información entre organizaciones que requieran compartirla. No solo se trata de mantener una base de datos, sino de cómo administrar un sistema de mejor manera los registros de ésta. [6]

4. **Para los gobiernos**

Los gobiernos tienen un interés en los tres aspectos componentes de la tecnología Blockchain. En primer lugar, están los derechos de propiedad sobre la posesión, revocación, generación, reemplazo o pérdida de claves criptográficas. También tienen un interés en quién puede actuar como parte de una red Blockchain. También, tienen interés en los protocolos de Blockchain, ya que autorizan las transacciones, ya que los gobiernos a menudo regulan la autorización de transacciones a través de regímenes de cumplimiento (por ejemplo, los reguladores del mercado de valores autorizan el formato de las operaciones de intercambio de mercado). Por esta razón, el cumplimiento regulatorio es visto como una oportunidad de negocio por muchos desarrolladores de Blockchain. [6]

5. Para instituciones financieras

Los sistemas tradicionales tienden a ser engorrosos, propensos a errores y enloquecedoramente lentos. Los intermediarios a menudo son necesarios para mediar en el proceso y resolver conflictos. Naturalmente, esto genera estrés y cuesta tiempo y dinero. Por el contrario, los usuarios encuentran que la Blockchain es más barata, más transparente y más efectiva. No es de extrañar que cada vez más servicios financieros utilicen este sistema para introducir innovaciones, como los bonos inteligentes y los contratos inteligentes. La primera paga automáticamente a los tenedores de bonos sus cupones una vez que se cumplen ciertos términos preprogramados. Estos últimos son contratos digitales que se ejecutan por sí mismos y se mantienen a sí mismos, nuevamente cuando se cumplen los términos. [6]

6. Para pistas de auditoría

Al usar la infraestructura cliente-servidor, los bancos y otras grandes instituciones que ayudan a las personas a formar relaciones digitales a través de Internet se ven obligados a proteger la información de la cuenta que tienen sobre los usuarios contra los piratas informáticos. Si bien los bancos pueden gastar miles de millones de dólares para mantener segura la información, el sistema está pidiendo a las empresas que hagan lo mismo. Estamos compartiendo la misma información con estas empresas que con los bancos, después de todo. Sin embargo, las empresas están bajo ataque y han sido pirateadas, lo que a veces resulta en la exposición de los detalles financieros íntimos de los clientes. La tecnología Blockchain ofrece un medio para crear automáticamente un registro de quién ha accedido a la información o los registros, y para establecer controles sobre los permisos necesarios para ver la información. [6]

Blockchain como una plataforma de aplicación se puede usar para:

1. Para la contratación inteligente

Blockchain es donde se forman y aseguran las relaciones digitales. Por ejemplo, entre varios de los bancos más grandes del mundo y algunas compañías de seguros, se está buscando construir una plataforma para establecer nuevas relaciones digitales entre ellos. [6]

2. Para el gobierno automatizado

Bitcoin es en sí, un ejemplo de gobierno automatizado, o un DAO (organización autónoma descentralizada). Este y otros proyectos siguen siendo experimentos de gobernanza, y falta mucha investigación sobre este tema. [6]

3. Para los mercados

Establecer una identidad digital única para expresar derechos de propiedad particular (por ejemplo, puede ser propiedad o bien inmueble, activos, productos entre otras cosas). Las reglas sobre cómo se pueden realizar transacciones sobre estos activos se pueden codificar mediante un protocolo de Blockchain. [6]

4. Para la racionalización de la compensación y la liquidación

En el mundo del comercio de acciones, a menudo se escucha el término 'T + 3'. Esto significa que una operación (T) es seguida por tres días antes de que la operación sea aceptada (liquidada). Actualmente existen formas diferentes a la tecnología de Blockchain para disminuir el número de días para que una transacción pueda ser liquidada, pero con mayor riesgo y no sin comprometer la seguridad. Con la tecnología de Blockchain tenemos una ecuación T + 0. [6]

5. Transferencias de bienes raíces, terrenos y títulos de propiedad

Uno de los objetivos principales de Blockchain es eliminar el papel de la ecuación, ya que los rastros de papel suelen ser una fuente de confusión. Si va a comprar o vender un terreno, una casa o un automóvil, deberá transferir o recibir un título. En lugar de manejar esto en papel, Blockchain puede almacenar títulos en su red, lo que permite una visión transparente de esta transferencia, y presenta una imagen nítida de la propiedad legal. [6]

6. Para automatizar el cumplimiento regulatorio

Más allá de ser un repositorio confiable de información, la tecnología Blockchain podría permitir el cumplimiento regulatorio en forma de código. En otras palabras, cómo se hacen válidos los bloques podría ser una traducción de la prosa legal del gobierno en un código digital. Esto significa que los bancos podrían automatizar informes regulatorios o autorizaciones de transacciones. [6]

2.3 Algunos usos del mundo real de la tecnología Blockchain

Blockchain es el libro digital, distribuido y descentralizado que subyace a la mayoría de las monedas virtuales y que es responsable de registrar todas las transacciones sin la necesidad de un intermediario financiero, como un banco. En otras palabras, es un nuevo medio de transmisión de fondos y/o información de registro. ¿Por qué la necesidad repentina de Blockchain? Blockchain es la visión de los desarrolladores que creían que el sistema bancario actual tenía fallas. En particular, consideraban que los bancos que actuaban como terceros y las tarifas por robo de transacciones eran innecesarios, y se burlaron de la idea de que la validación y liquidación de los pagos podría demorar hasta cinco días hábiles en las transacciones transfronterizas. Con Blockchain, las transacciones en tiempo real son una posibilidad (incluso a través de las fronteras), mientras que los bancos se quedan fuera de la ecuación por completo, presumiblemente reduciendo las tarifas de transacción. [7]

1. Procesamiento de pagos y transferencias de dinero

Podría decirse que el uso más lógico para Blockchain es como un medio para acelerar la transferencia de fondos de una parte a otra. Como se señaló, con los bancos eliminados de la ecuación y la validación de las transacciones en curso las 24 horas del día, los siete días de la semana, la mayoría de las transacciones procesadas a través de una Blockchain se pueden liquidar en cuestión de segundos. [7]

2. Monitorear las cadenas de suministro

Blockchain también es especialmente útil cuando se trata de monitorear las cadenas de suministro. Al eliminar las pistas basadas en papel, las empresas deberían poder identificar rápidamente las ineficiencias dentro de sus cadenas de suministro, así como localizar artículos en tiempo real. Además, Blockchain permitiría a las empresas, y posiblemente incluso a los consumidores, ver cómo los productos se realizaban desde una perspectiva de control de calidad mientras viajaban desde su lugar de origen hasta el minorista. [7]

figura 3 Monitorear las cadenas suministro(https://ungerboeck.com/images/blog/images/DataMonitoring.png)

3. Programas de recompensas por lealtad al por menor

Blockchain podría revolucionar aún más la experiencia minorista convirtiéndose en el objetivo de las recompensas de lealtad. Al crear un sistema basado en tokens que premia a los consumidores y almacenar estos tokens dentro de una Blockchain, incentivaría a los consumidores a regresar a una determinada tienda o cadena para realizar sus compras. También eliminaría el fraude y el desperdicio comúnmente asociados con los programas de recompensas de lealtad basadas en papel y en tarjetas. [7]

4. Protección de derechos de autor

En un mundo con un creciente acceso a internet, las leyes de copyright y propiedad sobre música y otros contenidos se han vuelto borrosas. Con Blockchain, esas leyes de derechos de autor se reforzarían considerablemente para la descarga de contenido digital, asegurando que el artista o creador del contenido que se compra obtenga su parte justa. Blockchain también proporcionaría datos de distribución de regalías transparentes y en tiempo real a los músicos y creadores de contenido. [7]

5. Votación digital

Blockchain ofrece la posibilidad de votar digitalmente, pero es lo suficientemente transparente como para que cualquier regulador pueda ver si algo ha cambiado en la red. Combina la facilidad del voto digital con la inmutabilidad (es decir, la naturaleza inmutable) de la Blockchain para que su voto realmente cuente. [7]

6. Seguridad alimentaria

Otro uso de Blockchain podría ser el rastreo de los alimentos desde su origen hasta su plato. Dado que los datos de Blockchain son inmutables, se podrá rastrear el transporte de productos alimenticios desde su origen hasta el supermercado. Además, si hubiera una enfermedad transmitida por los alimentos, Blockchain permitiría que la fuente del contaminante se encuentre considerablemente más rápido de lo que puede ser ahora. [7]

7. Copia de seguridad de datos inmutables

Blockchain también podría ser la forma perfecta de hacer una copia de seguridad de los datos. A pesar de que los sistemas de almacenamiento en la nube están diseñados para ser una fuente de referencia para la custodia de datos, no son inmunes a los piratas informáticos, ni siquiera a los problemas de infraestructura. [7]

8. Mantenimiento de registros médicos

Blockchain ofrece aún más seguridad y conveniencia en el ámbito de los registros de salud que el tradicional que usa papel y se archiva. Además de almacenar registros de pacientes, el paciente, que posee la clave para acceder a estos registros digitales, tendría el control de quién accede a esos datos. Sería un medio para fortalecer las leyes HIPAA que están diseñadas para proteger la privacidad del paciente. [7]

9. Seguimiento de armas

Uno de los temas candentes en cualquier red de noticias en este momento es el control de armas y / o la responsabilidad de las armas. Blockchain podría crear una red de registro transparente e invariable que permita a las fuerzas del orden público y al gobierno federal rastrear la propiedad de armas o armas, así como llevar un registro de las armas vendidas en privado. [7]

10. Testamentos o herencias

Blockchain también puede poner sus preocupaciones al final de la vida en reposo. En lugar de crear un documento de voluntad, las personas pueden tener la opción de crear y almacenar su voluntad digital en una red de Blockchain. Cuando se utiliza con contratos inteligentes, que pueden dividir las herencias en función de cuándo se cumplen ciertos criterios (como cuando un nieto alcanza cierta edad), los testamentos deberían ser claros y jurídicamente vinculantes, sin dejar preguntas sobre quién debería recibir qué activos cuando tu mueres. [7]

11. Comercio de acciones

En algún momento, Blockchain podría rivalizar o reemplazar las plataformas actuales de negociación de acciones para comprar o vender acciones. Debido a que las redes Blockchain validan y liquidan las transacciones tan rápidamente, podrían eliminar el tiempo de espera de varios días que los inversionistas encuentran al vender acciones y buscar acceso a sus fondos con el propósito de reinvertir o retirar dinero. [7]

12. Gestión de redes de Internet de las cosas

El gigante de redes Cisco Systems podría estar detrás de una aplicación basada en Blockchain que monitorearía las redes de Internet de las cosas (IoT). El IoT describe dispositivos conectados de forma inalámbrica que pueden enviar y recibir datos. Dicha aplicación podría determinar la confiabilidad de los dispositivos en una red y continuamente hacerlo para los dispositivos que ingresan y salen de la red, como autos inteligentes o teléfonos inteligentes. [7]

13. Acelerar el comercio de futuros de energía y el cumplimiento

Incluso la industria de la energía se está involucrando en el acto. De forma similar a los beneficios que podría brindar a los operadores de renta variable anteriores, Blockchain ofrece la capacidad de ayudar a las empresas de energía a liquidar operaciones de futuros considerablemente más rápido de lo que lo hacen actualmente. También vale la pena señalar que Blockchain podría ayudar a las compañías de energía a registrar sus recursos y mantener el cumplimiento normativo. [7]

14. Asegurar el acceso a sus pertenencias

Los contratos inteligentes dentro de las redes Blockchain también tienen la capacidad de personalizarse para las necesidades de las empresas o los consumidores. Como consumidor, puede usar Blockchain como un medio para otorgarles acceso a su casa a los técnicos de servicio, o permitir que su mecánico acceda a su automóvil para realizar reparaciones. Pero sin esta llave digital, que solo usted posee, estos técnicos de servicio no podrían obtener acceso a sus pertenencias. [7]

15. Seguimiento de medicamentos recetados

Finalmente, Blockchain podría ser un medio de rastrear de manera transparente los medicamentos recetados. En un mundo en el que se producen devoluciones de recetas, y los medicamentos falsificados son una realidad, Blockchain ofrece a los fabricantes de medicamentos la capacidad de rastrear sus productos en función de números seriales y / o por lotes para asegurarse de que los consumidores obtienen el verdadero beneficio cuando recogen los medicamentos. farmacia. Merck actualmente está probando dicho sistema para los retornos de medicamentos recetados. [7]

2.4 ¿Cómo funciona la tecnología Blockchain?

Blockchain está construido con 3 tecnologías		
Criptografía de clave privada	**Red peer-to-peer**	**Programa (protocolo de Blockchain)**
Identidad	**Sistema de registro**	**Plataforma**

[8]

La tecnología Blockchain es probablemente la mejor invención desde Internet. Permite el intercambio de valores sin la necesidad de confianza o de una autoridad central. Es un sistema donde le permite escribir datos con la capacidad de guardar permanentemente los datos en la Blockchain. También hay formas de reescribir los datos, pero se requiere la necesidad de que todas las necesidades de otros clientes observados en el sistema acepten el cambio, que es casi imposible en este caso debido a la cantidad de clientes en el sistema. [9]

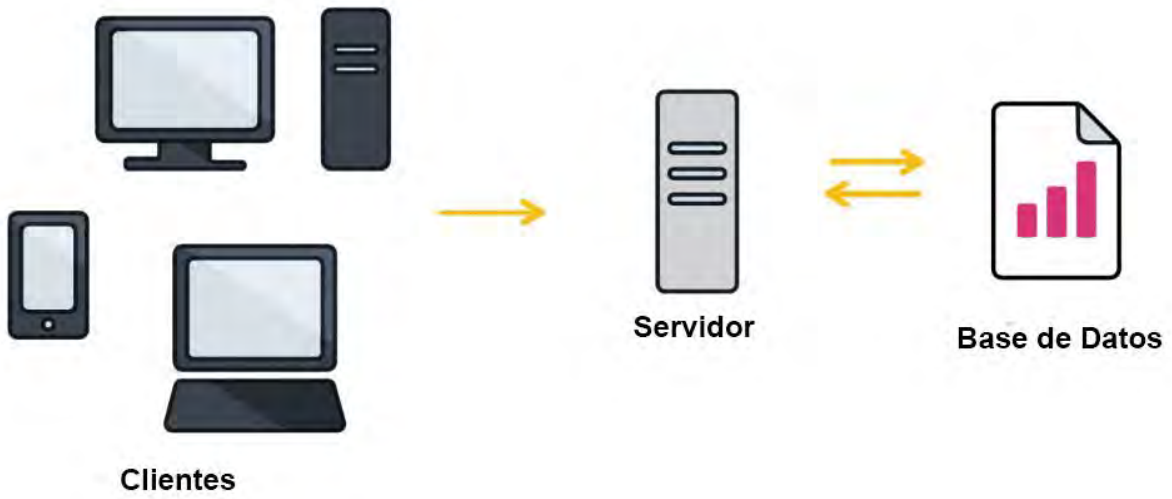

figura 4 Blockchain Proceso 1 (https://media.coindesk.com/uploads/2017/03/landing_pages__image-1-e1489089004344.png)

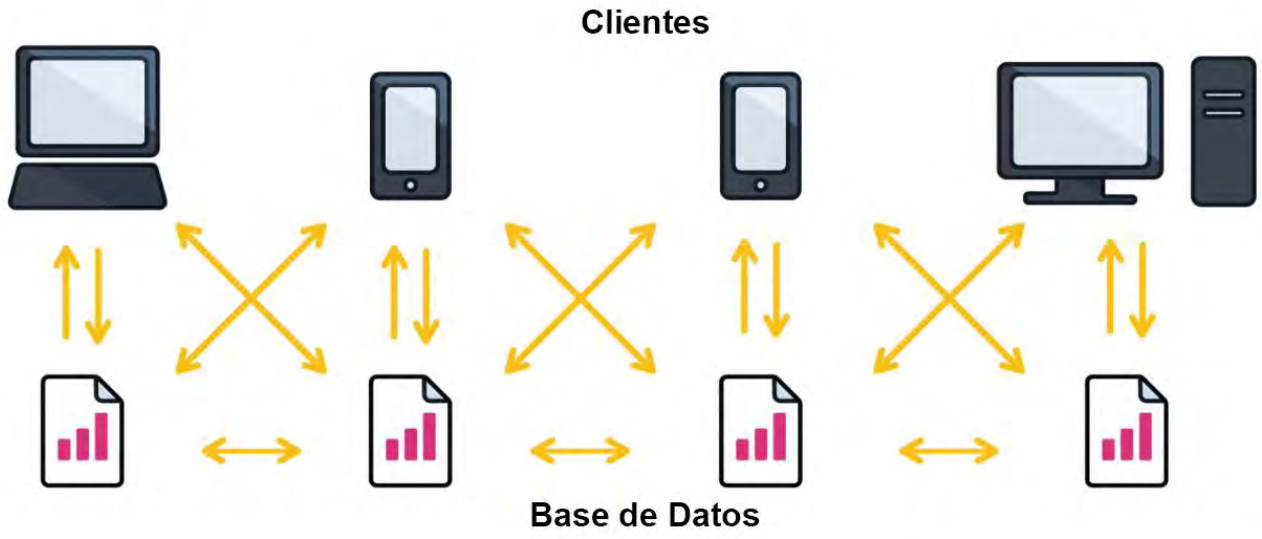

figura 5 Blockchain proceso 2 (https://media.coindesk.com/uploads/2017/03/landing_pages_image_2_horizontal-image_2-e1489089150298.png)

¿Cómo funciona exactamente la Blockchain?

Técnicamente, un Blockchain es una cadena de bloques ordenados en una red de pares no confiables. Cada bloque hace referencia al anterior y contiene datos, su propio hash y el hash del bloque anterior. [10]

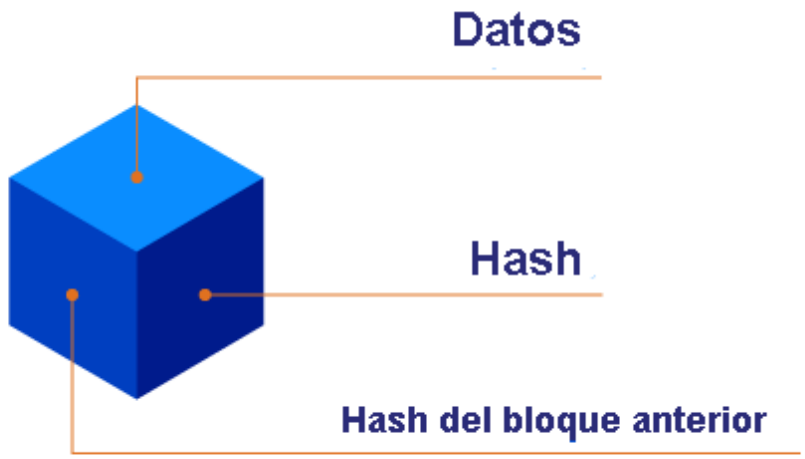

figura 6 Blockchain con hash (https://rubygarage.s3.amazonaws.com/uploads/article_image/file/1078/hash-example.png)

Bloque

Una unidad de datos almacenada dentro de un bloque se puede representar por cualquier valor dependiendo del tipo de Blockchain. Un bloque puede almacenar una cantidad de dinero, una participación en una empresa, un certificado digital de propiedad, un voto durante una elección o cualquier otro valor.

Un bloque almacena detalles encriptados sobre las partes cuya interacción resultó en los datos almacenados en el bloque. Un bloque de criptomonedas también contiene los identificadores encriptados del remitente y el receptor. Un bloque para una transacción de comercio electrónico contendrá los identificadores del minorista y el consumidor. [10]

¿Qué es la función hash (hashing)?

Una función hash toma un grupo de caracteres (llamado clave) y lo mapea a un valor de cierta longitud (llamado valor hash o hash). El valor de hash es representativo de la cadena de caracteres original, pero normalmente es más pequeño que el original. Hashing se hace para indexar y ubicar elementos en bases de datos porque es más fácil encontrar el valor hash más corto que la cadena más larga. Hashing también se usa en encriptación. [11]

Hash

Cada bloque también tiene un hash. Este hash es un valor generado a partir de una cadena de texto que utiliza una función matemática. Un hash se puede comparar con una huella dactilar, ya que cada hash es único. Su función es identificar un bloque y los contenidos del bloque. [10]

figura 7 Hash 1 (https://rubygarage.s3.amazonaws.com/uploads/article_image/file/1088/hash_as_a_fingertip.png)

Una vez que se crea un bloque, se calcula un hash. Al cambiar algo dentro del bloque, cambia el hash. Entonces, un hash también indica cambios en un bloque. [10]

figura 8 Hash 2 (https://rubygarage.s3.amazonaws.com/uploads/article_image/file/1089/hash_changes.png)

Además, cada bloque contiene un hash del bloque anterior. Por ejemplo, si hay tres bloques en una Blockchain, el bloque 3 contendrá el hash del bloque 2, y el bloque 2 contendrá el hash del bloque 1. [10]

figura 9 Cambios en bloque (https://rubygarage.s3.amazonaws.com/uploads/article_image/file/1080/changes-in-block.png)

Si alguien cambia los datos en un solo bloque, el hash de ese bloque en particular cambia, pero también hace que toda la cadena sea inválida.

figura 10 Hash Invalido (https://rubygarage.s3.amazonaws.com/uploads/article_image/file/1081/invalid-hash.png)

Un hash es una gran herramienta para identificar intentos de cambiar datos en bloques. Sin embargo, un algoritmo hash por sí solo no es suficiente para garantizar la seguridad de una Blockchain. Para mitigar los intentos de corromperla y garantizar la seguridad, la tecnología también usa un proceso llamado prueba de trabajo(Proof-of-Work). [10]

Proof-of-Work / Prueba de Trabajo(PoW)

En Blockchain, este algoritmo se usa para confirmar transacciones y producir nuevos bloques en la cadena. Con PoW, los mineros compiten entre ellos para completar los trámites en la red y obtener recompensas. [12]

La prueba de trabajo es un proceso de producción de datos que es difícil de obtener, pero fácil de verificar. En el contexto de una Blockchain, la prueba de trabajo consiste en resolver problemas matemáticos. Si se resuelve un problema con éxito, se puede agregar un nuevo bloque a la Blockchain. En promedio, realizar cálculos de prueba de trabajo y agregar un nuevo bloque a la cadena demora aproximadamente 10 minutos. [10]

¿Qué hay detrás del proceso de prueba de trabajo?

Este mecanismo se puede comparar con un juego de dados. Digamos que hay un número específico, nueve en este caso, que un jugador necesita para rodar. Lo más probable es que el jugador necesite varios intentos. Pero tarde o temprano, obtendrá nueve. Ahora agreguemos más jugadores al juego. El que tira el número correcto primero gana. [10]

figura 11 juego de dados en PoW
(https://rubygarage.s3.amazonaws.com/uploads/article_image/file/1082/Blockchain-dice-game.png)

Las computadoras que forman la red de Blockchain se utilizan para resolver un problema matemático, para recibir una recompensa y ser el primero en agregar el siguiente bloque a la cadena. Los problemas matemáticos en Blockchain tienen que ser difíciles de resolver, pero fáciles de controlar para evitar trampas. Juntos, el hash y el mecanismo de prueba de trabajo aseguran la seguridad de toda la red Blockchain. [10]

Cadena más larga

La cadena de bloques consiste en una enorme cantidad de nodos (los dispositivos conectados), cada uno de ellos está realizando simultáneamente una prueba de trabajo. Por lo tanto, una situación en la que varios nodos logran completar la prueba de trabajo con un resultado válido es bastante común. Cuando esto sucede se llama *hard fork*. [10] (Es una bifurcación de la cadena).

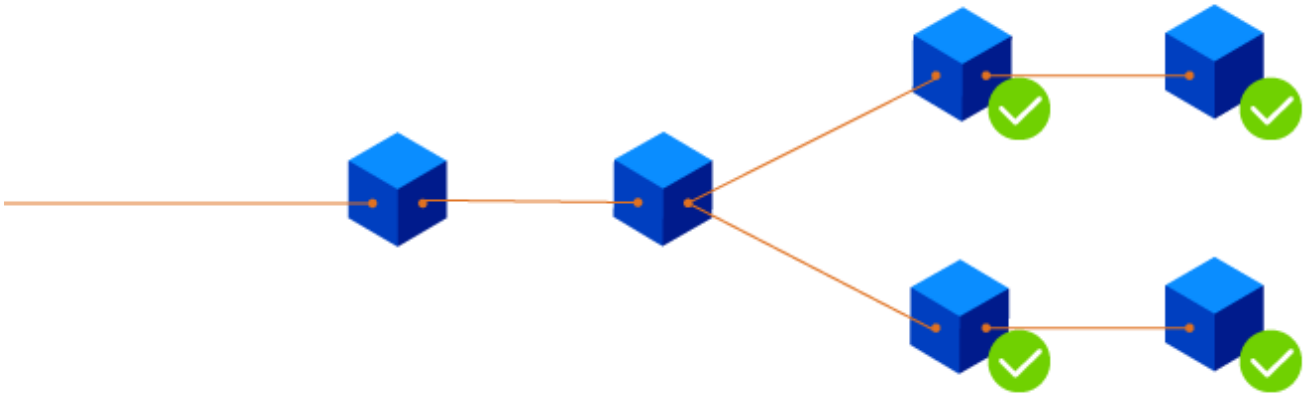

figura 12 tenedor duro (https://rubygarage.s3.amazonaws.com/uploads/article_image/file/1084/Blockchain-fork.png)

Cuando se crean y añaden nuevos bloques a una de estas cadenas bifurcadas, se toma como única y válida la más larga. Los bloques de otras cadenas bifurcadas son rechazados por los nodos de Blockchain, y todas las transacciones contenidas en esos bloques se envían para su verificación nuevamente. Hasta el momento, la bifurcación más larga alcanzada no es más de cinco bloques seguidos. [10]

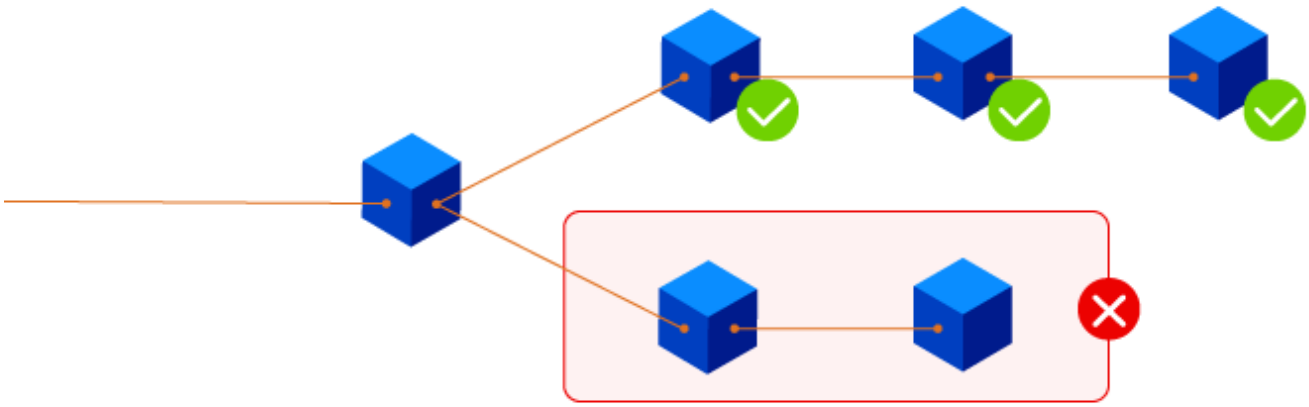

figura 13 Bifurcación 2 (https://rubygarage.s3.amazonaws.com/uploads/article_image/file/1085/Blockchain-verificaiton.png)

Wallet (Billetera)

Junto con el proceso de hashing y prueba de trabajo, una billetera de Blockchain también funciona para garantizar la seguridad de las transacciones y prevenir el fraude. Una billetera genera claves públicas y privadas (emparejadas) que aseguran aún más la seguridad de las transacciones.

Una clave pública se puede comparar con un buzón postal; cualquiera puede poner una letra dentro, pero no pueden recuperar esa carta. Solo un empleado postal que tenga una clave privada puede abrir el buzón y recibir la carta.

Esto es similar a cómo funcionan las llaves dentro de Blockchain. Cualquiera puede enviar una transacción usando una clave pública a la dirección de un receptor. Esto es similar a poner una carta en un buzón. Pero solo el propietario de esa dirección que también tiene la clave privada puede acceder al valor de esa transacción. [10]

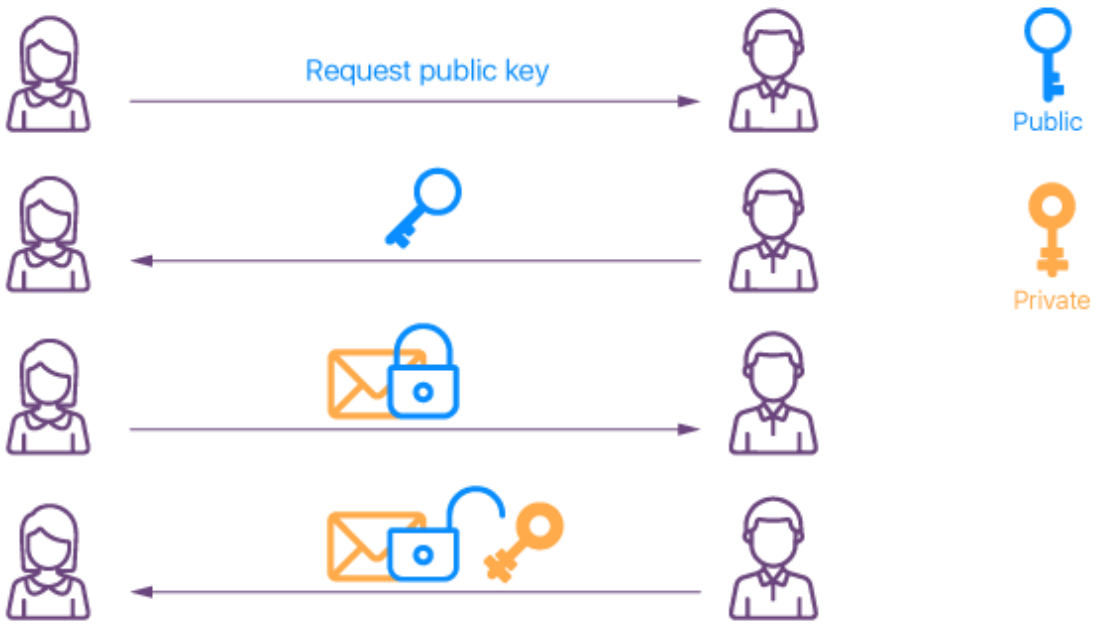

figura 14 Cambio de llaves (https://rubygarage.s3.amazonaws.com/uploads/article_image/file/1086/keys-exchange.png)

Red distribuida

Blockchain es una red distribuida. Cualquier persona puede unirse a una red de peer-to-peer, cuando esto sucede, esta persona obtiene una copia completa de la cadena de bloques. **El almacenamiento distribuido de datos acompañado de mecanismos efectivos de hash y prueba de trabajo ayuda a prevenir casi cualquier fraude.**

Por ejemplo, para agregar un bloque que contiene un hash no válido o datos no válidos, duplicar un bloque existente o realizar una transacción fraudulenta, un atacante tendría que piratear la computadora de cada participante de la Blockchain y deslizarse en el bloque no válido. Sin embargo, incluso si esto fuera posible, ninguno de los nodos verificaría dicho bloque. Simplemente sería ignorado, como si nunca hubiera existido en primer lugar. [10]

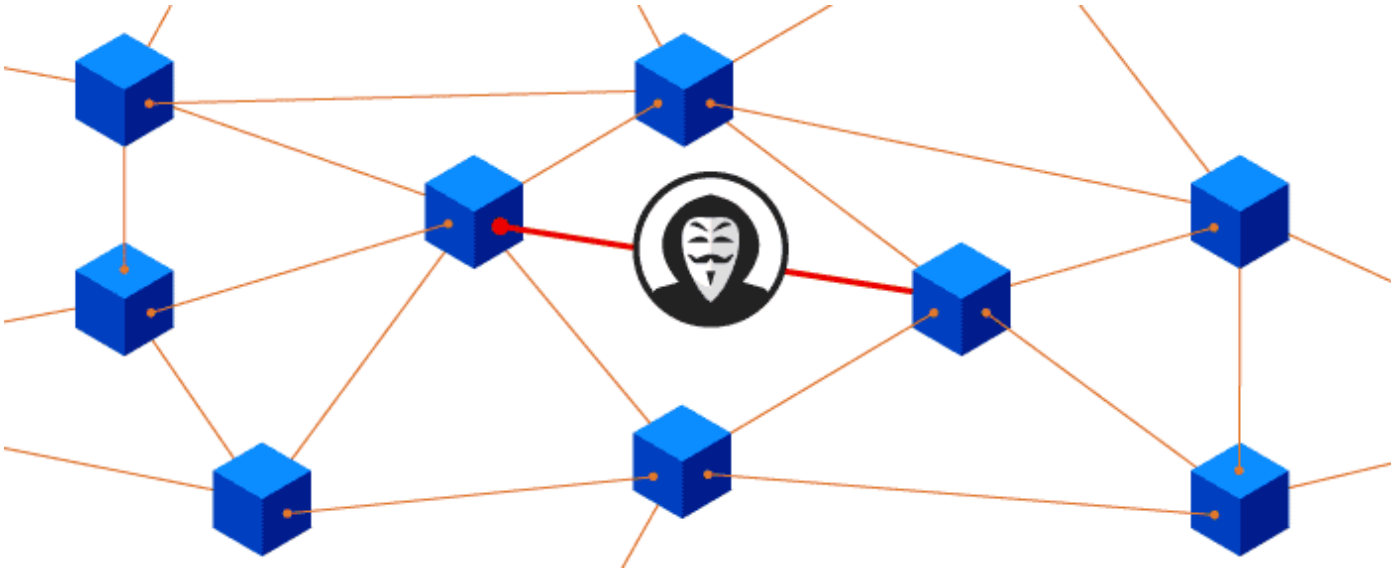

figura 15 hacker intento agregar bloque
(https://rubygarage.s3.amazonaws.com/uploads/article_image/file/1087/fraudless-Blockchain.gif)

Implementación de Blockchain

Uno de los usos más populares de la Blockchain es la criptomoneda. Las criptomonedas como Bitcoin, Litecoin, Ethereum y otras no son emitidas ni controladas por una autoridad central. La descentralización permite que estas monedas de Blockchain den los primeros pasos hacia un modelo financiero alternativo sin intermediarios.

Otra área revolucionada por el Blockchain es comerciar y hacer tratos. Los contratos tradicionales están siendo reemplazados por contratos inteligentes que son irrompibles, eliminando a terceros y trabajando para una amplia gama de aplicaciones: contratos de empleo, compras mayoristas y minoristas, acuerdos para comprar propiedades, acuerdos que garantizan derechos de propiedad intelectual, seguros e incluso contratos matrimoniales.

Blockchain puede ir más allá de las criptomonedas y los contratos inteligentes, además, lo que hace muy bien es almacenar, rastrear y transferir datos sobre bienes inmuebles y terrenos, derechos de propiedad e historial médico, transacciones comerciales e impuestos, y más. [10]

2.5 ¿Qué es criptomoneda?

figura 16 Criptomoneda (https://www.avatrade.es/wp-content/uploads/2018/03/criptomonedas.jpg)

Una criptomoneda (“cryptocurrency en inglés”) es un medio de intercambio, pero diseñado para el propósito de intercambiar información digital a través de un proceso hecho posible por ciertos principios de la criptografía. La criptografía se utiliza para asegurar las transacciones y controlar la creación de nuevas monedas. La primera criptomoneda que se creó fue Bitcoin en 2009. Las criptomonedas se denominan normalmente Altcoins.

Satoshi Nakamoto, el inventor desconocido de Bitcoin, fue el primero en crear con éxito una criptomoneda; aunque su intención no era crear una nueva moneda.

A fines de 2008, Satoshi dijo que desarrolló un sistema de efectivo electrónico punto a punto. Su objetivo era inventar algo y antes del efectivo digital muchos fracasaron en crear uno. La parte más importante de la invención de Satoshi fue que encontró la manera de construir un sistema de dinero digital descentralizado al que denominó sistema electrónico punto a punto. En la década de los noventa, muchas personas intentaron obtener efectivo digital, pero todas fracasaron porque todas tenían la intención de obtener efectivo digital centralizado. El nacimiento de la criptomoneda fue cuando Satoshi intentó construir un sistema de efectivo digital sin una entidad central, como la red de igual a igual para compartir archivos, después de ver que todos los intentos centralizados fallaban. [13]

¿Qué es Bitcoin?

Bitcoin es una criptomoneda y un sistema de pago mundial. Es la primera moneda digital descentralizada, ya que el sistema funciona sin un banco central o administrador único. La red es de igual a igual y las transacciones tienen lugar entre los usuarios directamente, sin un intermediario. Bitcoin fue inventado por una persona desconocida o grupo de personas bajo el nombre de Satoshi Nakamoto y lanzado como software de código abierto en 2009. [14]

figura 17 Bitcoin (https://en.Bitcoin.it/wiki/File:Bitcoin_euro.png)

¿Qué es Litecoin?

Litecoin es una criptomoneda que ha evolucionado a partir de Bitcoin después de su propia popularidad en la industria, esta alternativa, o 'altcoin', ha surgido para permitir a los inversores diversificar su paquete de moneda digital, según Investopedia. Litecoin es una de las altcoins más prominentes y fue creada por el ex empleado de Google y Director de Ingeniería en Coinbase, Charlie Lee. Litecoin fue el primero en alterar Bitcoin y la diferencia más significativa es que Litecoin demora 2.5 minutos en generar un bloque, o transacción, en comparación con los 10 minutos de Bitcoin. Litecoin fue lanzado como un cliente de código abierto en GitHub el 7 de octubre de 2011 por Charlie Lee, un empleado de Google. [15]

figura 18 Litecoin (https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcTxNC_qagK5UK8ud7RYgIUwu-C68vrgIhnEtWcgOxRFf8698MBI)

¿Qué es Ethereum?

Ethereum es una plataforma de open-source, de código abierto, basada en Blockchain, de fuente abierta, que ofrece funcionalidad de contrato inteligente (scripting). El ether es una criptomoneda cuya Blockchain es generada por la plataforma Ethereum. Ether puede transferirse entre cuentas y usarse para compensar los nodos de minería participantes por los cálculos realizados. Ethereum fue propuesto a finales de 2013 por Vitalik Buterin y el sistema se lanzó el 30 de julio de 2015. [16]

figura 19 Ethereum (https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcTjNs-u0tyxz-IgZXXXnV_GOZXzG8oIas4hpLjbaE9YRvfjso0P)

2.6 Configuración del sistema

¿Cuál es la diferencia entre una red centralizada y una red descentralizada para dinero digital?

Para tener dinero (moneda) digital se necesita una red de pago con cuentas, saldos y transacciones. El principal problema que debe resolver cada red de pago es evitar el gasto doble, lo que significa que debe evitar que la entidad gaste la misma cantidad dos veces, pero además, revisar que hay fondos suficientes, el no repudio (o sea, querer revertir una transacción una vez que fue realizada y completada con éxito). Esto normalmente lo hace un servidor central que registra todas las balanzas y esto se conoce como la red centralizada de efectivo digital. En una red descentralizada no existe una red central, por lo que necesita que cada entidad de la red realice este trabajo. Todos los pares en la red deben tener una lista con todas las transacciones para verificar si las transacciones futuras son válidas o un intento de duplicar el gasto. Todos pensaron que era imposible hasta que Satoshi descubriera cómo hacerlo posible. [17]

¿Cómo funciona?

Una criptomoneda como Bitcoin consiste en una red de pares y cada par tiene un registro del historial completo de todas las transacciones y también el saldo de cada cuenta. Una transacción es un archivo que dice "Persona ***A*** da (transfiere) una cantidad ***X*** de Bitcoin a la persona ***B***" y se registra con la clave privada de la persona ***A*** (una clave básica de criptografía). Después de que se firma, la transacción se transmite en la red, que se envía de par a en par. Esta es la tecnología P2P. [18]

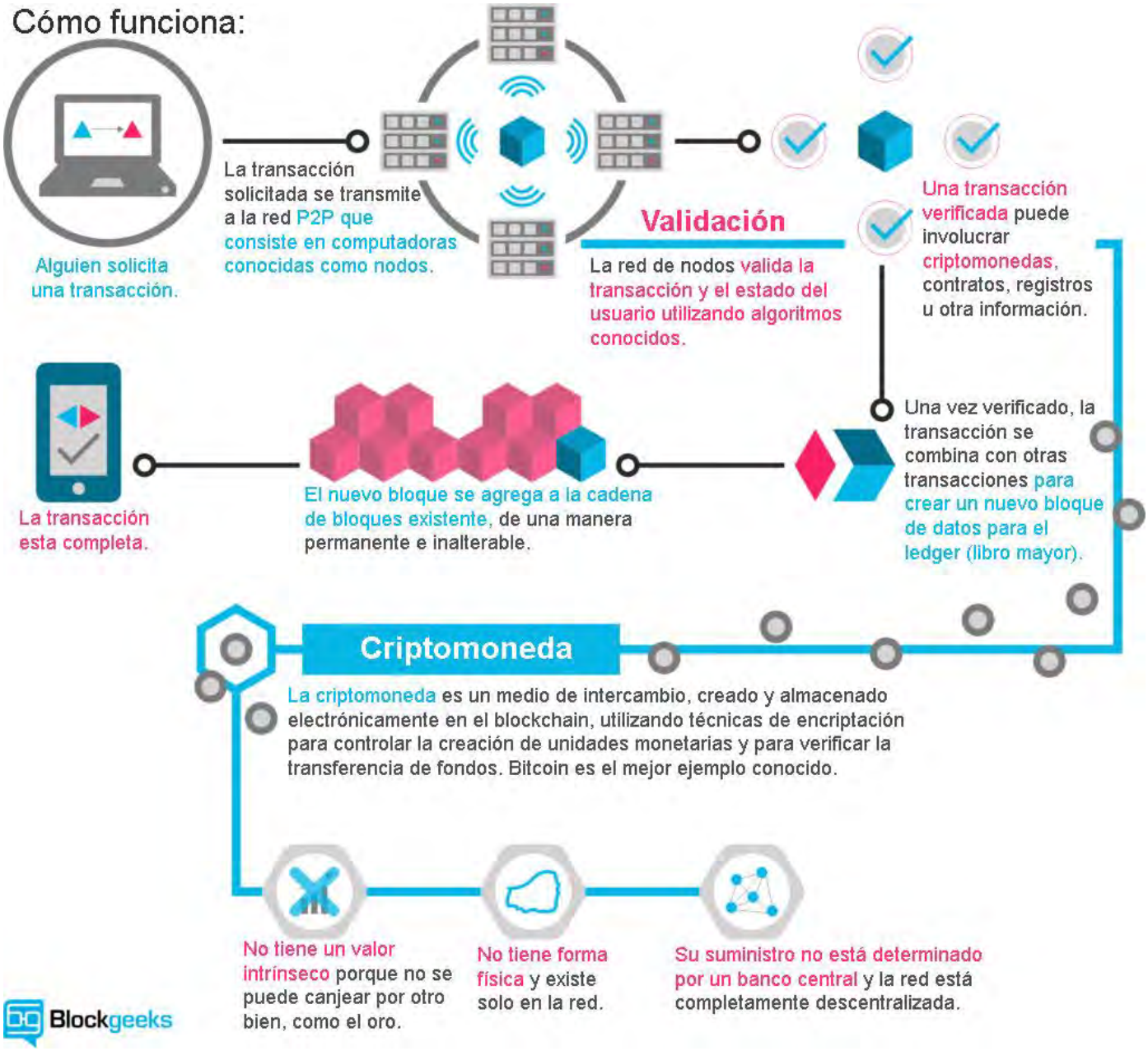

figura 20 Proceso Criptomoneda traducido de (https://blockgeeks.com/wp-content/uploads/2016/11/image-1-1024x936.png)

Una transacción es conocida por toda la red. Ésta sólo puede ser confirmada después de una cantidad específica de “confirmaciones” por parte de los otros nodos de la red (compañeros).

La confirmación es un concepto crítico en las criptomonedas o se puede decir que las criptomonedas son todas confirmaciones. Siempre que una transacción no esté confirmada, está pendiente y puede falsificarse. Cuando se confirma una transacción, ya no se puede falsificar; no puede revertirse y es parte de un registro inmutable de transacciones históricas llamadas Blockchain. En la red de criptomonedas, solo los mineros pueden confirmar las transacciones. Los mineros toman transacciones, las califican como legítimas y las distribuyen en la red. Después de que un minero confirma la transacción, el nodo se agrega a la base de datos y se convierte en parte de la Blockchain. Los mineros normalmente son recompensados con altcoins ya que la actividad del minero es la mayor parte del sistema de criptomonedas. [18]

¿Qué están haciendo los mineros?

Inicialmente cualquiera puede ser un minero. Como una red descentralizada no tiene autoridad para delegar esta tarea, una criptomoneda necesita algún tipo de mecanismo para evitar que un partido gobernante abuse de ella. Imagine que alguien crea miles de pares y propaga transacciones falsificadas. El sistema se rompería inmediatamente. Satoshi estableció la regla de que los mineros necesitan invertir algún trabajo de sus computadoras para calificar para esta tarea. Deben encontrar un hash, producto de una función criptográfica, que conecta el nuevo bloque con sus predecesores. Esto se llama prueba de trabajo. Bitcoin se basa en el algoritmo SHA 256 Hash. No es necesario que entienda los detalles sobre SHA 256. Solo es importante que sepa que puede ser la base de un rompecabezas criptológico que los mineros compiten para resolver. Después de encontrar una solución, un minero puede construir un bloque y agregarlo a la Blockchain. Como incentivo, tiene derecho a agregar una llamada transacción de coinbase que le da un número específico de Bitcoins. Esta es la única forma de crear Bitcoins válidos.

Los Bitcoins solo se pueden crear si los mineros resuelven un desafío criptográfico. Dado que la dificultad de este desafío aumenta, la cantidad de energía computacional que invierte el minero también aumenta, además solo hay una cantidad específica de tokens de criptomoneda que se puede crear en un período determinado. Esto es parte del consenso que ningún participante en la red puede romper. [18]

Capítulo 3 Conclusiones

La tecnología de Blockchain puede ser (y ha demostrado ser) complementaria en un espacio de posibilidades amplio el cual incluye modelos centralizados y descentralizados. Como cualquier nueva tecnología, Blockchain con el tiempo podría promover el desarrollo de un ecosistema más amplio que incluye aspectos ya conocidos y las recientes innovaciones. Con esto me refiero a sectores como el de salud, el financiero, de bienes raíces, políticas (a través de las votaciones) derechos de propiedad intelectual, etc.

Blockchain **no es sólo** una plataforma o una gran base de datos descentralizadas, es todo un nuevo paradigma de trabajo colaborativo, es la base de nuevas formas de monedas virtuales, mecanismos de seguridad y confiabilidad con implementaciones en muy diversos ámbitos de la actividad humana.

El sistema Blockchain ha demostrado ser sólido en seguridad y en mantener todos los datos y transacciones guardados permanentemente en él. Aunque, todavía es posible que los hackers ingresen al sistema, es difícil que logren cambiar algo y, si esto sucede se puede comprobar en el historial (en el cual participan muchos nodos de la red), el cual es diseñado para hacer la información guardada permanentemente.

Blockchain permite almacenar una gran cantidad de información de manera confiable, lo que la convierte en una sustitución menos cara en comparación con múltiples sistemas de software complejos.

Algo que quiero destacar es que durante la investigación que realicé se analizó Blockchain para las criptomonedas, sin embargo, se hizo notorio para mí que la implementación de cadenas de bloques puede ser una muy buena opción para las pequeñas y medianas empresas, es decir, pueden usarlas con éxito del mismo modo que las grandes empresas

Hablando de las criptomonedas que se investigaron en este proyecto, quiero destacar el valor en moneda mexicana actual de Bitcoin la cual se ubica en $ 95, 363.50 MXN, (hubo momentos en que llegó a los casi $400, 000.00 MXN), Litecoin $715.00 MXN, y Ethereum $2,928.01 MXN. Estos valores han cambiado mucho desde que se publicaron las criptomonedas, pero los cambios, no obedecen a la moneda en sí, (específicamente en la tecnología Blockchain), si no, como en cualquier otro sistema de monedas, responde a cuestiones de apreciación de los usuarios, los cuales, entre todos, van determinando su valor frente a otras monedas, particularmente con respecto al dólar.

Actualmente existen diversas variantes de uso de Blockchain, querer nombrarlas todas es complicado. Pienso que cualquier actividad que incluya acuerdos entre más de dos entidades (cadenas de bloques) será una elección perfecta por implementar y creo que cada vez más personas verán cuán útil es el uso de la Blockchain por lo que su uso se irá incrementando y diversificando en el futuro.

Referencias

[1] B. Marr, «Forbes,» 16 Febrero 2018. [En línea]. Available: https://www.forbes.com/sites/bernardmarr/2018/02/16/a-very-brief-history-of-Blockchain-technology-everyone-should-read/#6bf847e77bc4. [Último acceso: 06 Septiembre 2018].

[2] J. Giordani, «Forbes CommunityVoice,» 28 Marzo 2018. [En línea]. Available: https://www.forbes.com/sites/forbestechcouncil/2018/03/28/Blockchain-what-is-it-and-what-is-it-for/#2ec30c371a16. [Último acceso: 14 Julio 2018].

[3] E. d. Paz, «Ibertrónica,» 10 Abril 2018. [En línea]. Available: https://www.ibertronica.es/blog/actualidad/que-es-Blockchain-para-que-sirve/. [Último acceso: 15 Julio 2018].

[4] J. R. Rojas, «Blastingnews,» 28 Marzo 2018. [En línea]. Available: https://mx.blastingnews.com/tecnologia/2018/03/Blockchain-que-es-y-para-que-sirve-002468853.html. [Último acceso: 17 Julio 2018].

[5] B. Parez, «South China Morning Post,» 25 Septiembre 2017. [En línea]. Available: https://www.scmp.com/tech/enterprises/article/2112627/three-key-things-you-need-know-about-Blockchain-technology. [Último acceso: 15 Julio 2018].

[6] N. Bauerle, «coindesk,» 2018. [En línea]. Available: https://www.coindesk.com/information/applications-use-cases-Blockchains/. [Último acceso: 10 Julio 2018].

[7] S. Williams, «My Motley Fool,» 11 Abril 2018. [En línea]. Available: https://www.fool.com/investing/2018/04/11/20-real-world-uses-for-Blockchain-technology.aspx. [Último acceso: 18 Julio 2018].

[8] N. Bauerle, «coindesk,» 2018. [En línea]. Available: https://www.coindesk.com/information/what-is-Blockchain-technology/. [Último acceso: 28 Agosto 2018].

[9] M. D'Aliessi, «A Medium Corperation,» 01 Junio 2016. [En línea]. Available: https://medium.com/@micheledaliessi/how-does-the-Blockchain-work-98c8cd01d2ae. [Último acceso: 28 Agosto 2018].

[10] T. H., «RubyGarage,» 2018. [En línea]. Available: https://rubygarage.org/blog/how-Blockchain-works. [Último acceso: 28 Agosto 2018].

[11] Techopedia, «Techopedia,» 2018. [En línea]. Available: https://www.techopedia.com/definition/19744/hash-function. [Último acceso: 28 Agosto 2018].

[12] A. Tar, «CoinTelegraph,» 17 Enero 2018. [En línea]. Available: https://es.cointelegraph.com/explained/proof-of-work-explained. [Último acceso: 28 Agosto 2018].

[13] C. Graydon, «CCN,» 16 Septiembre 2014. [En línea]. Available: https://www.ccn.com/cryptocurrency/. [Último acceso: 06 Septiembre 2018].

[14] N. Acheson, «coindesk,» 16 Enero 2018. [En línea]. Available: https://www.coindesk.com/information/what-is-Bitcoin/. [Último acceso: 06 Septiembre 2018].

[15] M. Mavadiya, «Forbes,» 12 Deciembre 2017. [En línea]. Available: https://www.forbes.com/sites/madhvimavadiya/2017/12/12/what-is-Litecoin-why-is-ltc-price-going-up/#3670760d6661. [Último acceso: 06 Septiembre 2018].

[16] «Coinbase,» 05 Septiembre 2018. [En línea]. Available: https://www.coinbase.com/what-is-Ethereum?locale=en. [Último acceso: 06 Septiembre 2018].

[17] A. Kumar, «The Windows Club,» 16 Mayo 2016. [En línea]. Available: https://www.thewindowsclub.com/centralized-vs-decentralized-internet. [Último acceso: 06 Septiembre 2018].

[18] Blockgeeks, «Blockgeeks,» 2018. [En línea]. Available: https://blockgeeks.com/guides/what-is-cryptocurrency/. [Último acceso: 06 Septiembre 2018].

[19] S. S. a. T. N. Cadigan, «Business Insider,» 15 Febrero 2018. [En línea]. Available: https://www.businessinsider.com/Blockchain-with-no-cryptocurrency-a-database-innovation-2018-2. [Último acceso: 28 Agosoto 2018].

[20] J. S., «CoinMonks,» 06 Mayo 2018. [En línea]. Available: https://medium.com/coinmonks/Blockchain-for-beginners-what-is-Blockchain-519db8c6677a. [Último acceso: 28 Agosto 2018].

[21] CoinTelegraph, «CoinTelegraph,» 2018. [En línea]. Available: https://cointelegraph.com/Bitcoin-for-beginners/how-Blockchain-technology-works-guide-for-beginners#hash-function. [Último acceso: 28 Agosto 2018].

[22] N. Bauerle, «coindesk,» 2018. [En línea]. Available: https://www.coindesk.com/information/why-use-a-Blockchain/. [Último acceso: 20 09 2018].