INSTITUTO TECNOLÓGICO SUPERIOR DE SANTIAGO PAPASQUIARO

ING. SISTEMAS COMPUTACIONALES

FUNDAMENTOS DE INVESTIGACIÓN

Blockchain, la Tecnología que Revolucionará la Forma en la que Gestionamos la Información

Autor:

Hendrik Alberto Villarreal Sarmiento

Mentor:

M.A.T.S.I. Juan Manuel Gallegos Herrera

Santiago Papasquiaro, Dgo. Noviembre 2019

Prólogo

El presente informe de investigación es el resultado de la indagación, recopilación y análisis de datos relacionados al tema de Blockchain, realizado en el semestre agosto - diciembre del 2019.

Este proyecto está dividido en diferentes partes con el fin de ayudar al lector a conocer los conceptos y terminologías básicas para entender la tecnología Blockchain, teniendo como base preguntas que el autor se planteó y dieron una guía en la investigación final. Dentro del contenido de este informe se encuentran diagramas e imágenes que ayudan a explicar los conceptos de la tecnología Blockchain,

Cabe mencionar que la tecnología Blockchain tiene poco tiempo en la industria y sus usos no han sido explotados del todo, permitiendo con este trabajo dar un panorama a nuevos profesionistas sobre sus posibles usos y posiblemente plantearse nuevos proyectos y soluciones en las industrias.

Contenido

Índice de ilustraciones

Índice de gráficas

Abstract

En el siguiente documento se presentará información acerca de una tecnología aparentemente “reciente”, y está escrito entre comillas, ya que la idea de esta tecnología data de principios de los 90, pero no fue hasta 2009 que se utilizó al ser aplicada en un proyecto de criptomoneda.

Se trata de Blockchain, un sistema de almacenamiento de información que se basa en una seguridad criptográfica a base de cadena de bloques. Aquí se hablará sobre esta tecnología enfocándose en las cosas básicas o más destacables de una forma entendible para que todo aquel que lea este informe pueda entender mejor esta tecnología.

Aquí se verán algunos aspectos como lo es algo de historia, de cómo empezó como una idea que no se supo en que aspectos se podría utilizar hasta ser la base de la red de criptomoneda más grande hasta el momento. También se verá su funcionamiento, así como las partes principales que lo componen.

También se verán algunos conceptos que ayudarán al lector a no perderse el informe y continúe a un ritmo en el que se le facilite el entendimiento de esta tecnología, además de estar ordenado de forma que sea cómodo visualmente para seguir la lectura.

Resumen

Blockchain en español significa Cadena de Bloques, es un sistema de almacenamiento de información que podría revolucionar la manera en la que se almacenan los datos. Hoy en día este almacenaje la hacen humanos, esos seres perezosos, lentos, corruptibles y *hedonistas*. Blockchain trata de asignarle la tarea a otro tipo de seres más confiables, más sacrificables y cada día más veloces…los ordenadores.

Pero hay una debilidad que tiene todo sistema informático, que es hackeable. Pero ¿Cómo evita esto Blockchain? Blockchain se autoprotege gracias a su propia arquitectura que está conformada por tres partes principales:

La **Información,** que son los datos que están dentro del bloque. El **Hash**, que es el número del identificador del bloque, único e irrepetible. Tiene la peculiaridad de que éste varía según la información que tenga dentro. Y finalmente el **Hash del bloque anterior**, haciendo que los bloques estén unidos como si se tratasen de piezas de un puzle.

Hay dos cosas que lo hace inhackeable, una de ellas es el hash que, como ya se mencionó anteriormente, si se cambia la información cambiará el Hash, haciendo que deje de encajar con su bloque predecesor, rompiendo la cadena y lanzando una alerta. Y la otra es que hay muchos ojos mirando todo el rato, así que básicamente la seguridad del Blockchain se lo dan los propios usuarios.

Blockchain es más que solo una simple base de datos, es un sistema de almacenamiento de información que podría crear una sociedad más equitativa, más transparente y más veraz.

Introducción

En este documento se podrá observar acerca de un sistema informático que, a pesar de crearse hace ya varios años, podría llegar a cambiar la forma no solo en la que almacenamos o gestionamos la información, sino también en la forma en la que vivimos día a día.

Anteriormente y durante muchos años han sido personas quienes han realizado la tarea de manipular la información de los demás y a pesar que se ha hecho de esta manera desde hace siglos sigue siendo una forma que tal vez aun no es demasiado confiable, debido a que se han presentado en múltiples ocasiones problemáticas ocasionadas por tener suficiente “libertad” para ingresar a la información.

La información, aunque no lo parezca es incluso más valioso que el dinero, quien tenga control sobre ésta se puede volver alguien peligros, puesto que puede hace con ella lo que desee. La información vale tanto que incluso puede llegarle a costar la vida a alguien.

Ha habido muchos conflictos por la inseguridad que tiene el sistema de gestión de la información, ya que hay ocasiones en las que se pueden filtrar datos, manipularlos o hacer con ellos lo que sea que pueda perjudicar a la víctima.

Pero no hay que tomar siempre que el poder consultar la información de forma libre es algo malo, dado que instituciones de investigación o centros que rigen las leyes, como por ejemplo la FBI o la SIN en el caso de México, si es necesario acceden a la información que sea necesaria para poder realizar investigaciones y así poder hacer acciones que contribuyan con el bien de la sociedad.

Pero el sistema que se maneja para gestionar y almacenar la información puede que en algunas ocasiones no sea del todo seguro, es por eso que en las paginas siguientes se hablará de un sistema de almacenamiento de información que puede llegar a cambiar la forma en la que se maneja, gestiona y administra la información de una forma más rápida y más segura que el sistema tradicional, se trata de **Blockchain.**

El caso más popular en la que se ha utilizado Blockchain es en la criptomoneda más famosa que es el Bitcoin, la moneda que permite hacer transacciones monetarias de forma anónima.

Justificación

El propósito de esta investigación es la de informar o dar a conocer el sistema de Blockchain y las posibles aplicaciones que podría tener en beneficio a la sociedad, pues este sistema es más que solo criptomonedas, se puede llegar a utilizar para más sectores, haciendo que nuestra vida cambie con respecto a la forma en la que manejamos la información.

Preguntas de investigación

¿Qué es Blockchain?, ¿Cómo está compuesto el Blockchain?, ¿Quién creó el Blockchain?, ¿Cuándo se creó el Blockchain?, ¿Cuándo se usó Blockchain por primera vez?, ¿Quién usó Blockchain por primera vez?, ¿Para qué se usó el Blockchain?, ¿En qué se usa el Blockchain actualmente?, ¿Qué es la “minería”?, ¿Qué son los “mineros”?, ¿Ha habido problemas o errores al usar Blockchain?, ¿Cómo se puede ser parte de Blockchain?, ¿Qué beneficios tiene Blockchain?, ¿Blockchain de verdad es tan seguro?

Pregunta principal de investigación

¿Qué es Blockchain?

Hipótesis

El Blockchain al ser un sistema que puede proteger datos e información, actualmente se usa más en la criptomoneda, tal es el caso de bitcoin. Pero Blockchain es más que solo eso, al ser un sistema que asegura la información que ingresa en él, haría más sencillo algunos aspectos de la vida cotidiana, por ejemplo, podría dificultar o evitar por completo la falsificación de información y documentos importantes.

Actualmente se utiliza para la transacción de dinero de forma anónima y segura, varios bancos están implementando ya este sistema para la gestión de sus cuentas. El gobierno al enterarse de Blockchain iniciaron investigaciones para sacarle provecho a este sistema para beneficiarse ellos y a la ciudadanía, supuestamente más a la ciudadanía.

Blockchain podría lograr eliminar el robo de datos, su modificación o simplemente su manipulación, ya que la información esta no solo guardada, sino también vigilada en cada momento por los demás usuarios de Blockchain.

Blockchain es un sistema revolucionario que podría hacer que muchas de las cosas más fastidiosas de la vida desaparezcan, protegiendo todo tipo de información y creando una sociedad más transparente que es lo que buscan las personas.

Objetivo

Concientizar y dar a conocer a todo aquel que lea este informe sobre Blockchain de una forma entendible para que así pueda comprender esta tecnología.

Objetivos Específicos

- Formular preguntas de investigación.
- Formular hipótesis.
- Buscar información de Blockchain.
- Recopilar información importante.
- Redactar la información de una forma entendible para la mayoría de las personas.

Alcances y limitaciones

Lo que se podría llegar al investigar más sobre estos sistemas de seguridad criptográfica se podría llegar a tal nivel de poder meterse más profundo en el tema. Investigar más a fondo el funcionamiento, normas e incluso como llegar a mejorar la seguridad, tal vez incluso llegar a crear una nueva red de este tipo.

También se podría llegar a investigar cómo evolucionar este sistema de seguridad criptográfica, ya que con la llegada de la supercomputadora cuántica de Google se podría llegar a crear un Blockchain cuántico, un nivel de seguridad realmente superior comparado con los más avanzados hasta ahora.

Aunque los principales obstáculos son el factor tiempo, puesto que estas investigaciones requieren de mucha dedicación, dado que al ser un tema tan profundo y en ciertos aspectos tan joven hace que haya mucho camino por recorrer, por lo que se necesitarían muchos recursos para hacerlo, y ese sería otro factor.

Por ejemplo, en el aspecto económico, pues se tendrían que realizar cursos sobre estos temas y, si así se requiere, viajar a otros lugares para conocer a otros expertos en el tema, crear un equipo de trabajo y todos trabajar en conjunto para realizar una investigación más completa y más versátil.

1. Historia del arte

La aplicación de Blockchain recientemente solo va enfocado en al ámbito financiero, ya varios bancos están implementando este sistema para transferencias bancarias y mantener un buen margen de seguridad.

Y algo que está ganando mucho auge que se basa en Blockchain, que son las famosas y recientes criptomonedas, puesto que se están implementando en varios países, varios en América Latina, donde se destacan Colombia, Brasil, Argentina, México, entre otros. Y fuera del continente americano están España, China, Indonesia, entre otros. Hay muchos otros lugares donde ya están empleando este sistema de transacción. (Mario, 2019)

Cabe mencionar, que recientemente China busca acelerar la creación de su propia criptomoneda para cambiar el efectivo por el dinero digital.

Aunque hay algo que preocupó a muchos, y es que hubo errores de seguridad alrededor de esta tecnología. Conforme evoluciona Blockchain también va haciendo que los problemas a resolver se fueran complejizando, dando a esto que aumente el margen de error. Así el caso de Zcash, que es una criptomoneda que utiliza un proceso matemático complejo para permitir a los usuarios realizar transacciones privadas, hizo publicó que tuvieron que arreglar una falla criptográfica en el protocolo, y que si un atacante hubiera abusado de este error pudo haber tenido la posibilidad de crear monedas Zcash falsas de forma ilimitada (Harán, 2019).

Pero los cibercriminales no se van a por las principales potencias de criptomonedas como bitcoin, pues sería muy costoso para ellos en términos de poder computacional y consumo energético, esto por el protocolo *HashCash,* ya que el resolver un problema matemático requiere de poder de procesamiento, *Nicholas Weaver, profesor de UC Berkeley ISCI y escéptico de Bitcoin* (Brandom, 2019), estima que la red de Bitcoin gasta alrededor de $300,000 de electricidad cada hora.

Es por eso que los atacantes opten por realizar ataques a criptomonedas de menor nivel, ya que al ser más pequeñas son más fáciles y rápidas de minar al exigir menos poder de computo para conseguirlas, logrando así robar alrededor de 120 millones de dólares en total según la plataforma de *Criptonoticias.* Pero recientemente se supo del primer ataque a una de las principales 20 criptomonedas más populares.

Esto tiene de que hablar sobre la seguridad de esta red informática. A principios de este año (2019) se dio a conocer un ataque a la red de Etheorum Classic llamado *ataque del 51%*, en el que los cibercriminales lograron robar más de un millón de dólares (Harán, 2019).

¿Esto quiere decir que Blockchain no es seguro? No necesariamente, hasta ahora Blockchain es uno de los sistemas de seguridad criptográficos más seguros y será así por el momento hasta que se demuestre lo contrario, así como los cibercriminales pueden evolucionar en sus estrategias de ataque Blockchain también seguirá evolucionando sus medidas de seguridad.

Ahora con la llegada de la supercomputadora de Google que puede resolver en 200 segundos un problema matemático que a una computadora normal le tomaría más de 1000 años parece que puede llegar a ser un obstáculo para Blockchain debido a que éste funciona principalmente por la valoración de problemas matemáticos complejos que deberían ser difíciles de resolver, pero… ¿y qué tal suena la encriptación cuántica?

2. Marco Histórico

(Binance Academy, 2019) La idea de Blockchain se describió en 1991 cuando los científicos de investigación *Stuart Haber* y *W. Scott Stornetta* propusieron una solución computacionalmente práctica para que los documentos digitales no fueran modificados o manipulados. El sistema usó una cadena de bloques con seguridad criptográfica para almacenar los documentos temporalmente sellados y en 1992 se añadieron *árboles Merkle* al diseño permitiendo que se pudiera reunir diversos documentos en un único bloque. Sin embargo, esta tecnología no se utilizó y la patente caducó en 2004.

Ese mismo año un informático llamado *Hal Finney* introdujo un sistema llamado *RPoW*. El sistema funcionó al recibir un *token* no intercambiable basado en *HashCash* y a cambio creó un token por *RSA* que luego podría transferirse de una persona a otra. Se podría decir que este era un prototipo temprano en la historia de las criptomonedas.

No fue hasta 2009 que *Satoshi Nakamoto*, seudónimo en la que hasta la actualidad nadie sabe quién está detrás, utilizo el Blockchain como base para la creación de su famosa criptomoneda *Bitcoin* donde se utilizó un protocolo *peer to peer* (igual a igual) para el seguimiento y verificación de las transacciones.

El 3 de enero de 2009, Bitcoin nació cuando el primer bloque de Bitcoin fue minado por *Satoshi Nakamoto*, quien obtuvo una recompensa de 50 bitcoins. El primer receptor fue *Hal Finney,* quien recibió 10 bitcoins de *Satoshi Nakamoto* haciendo de esta la primera transacción de bitcoin el 12 de enero de 2009 (Binance Academy, 2019).

En 2013, *Vitalik Buterin,* programador y cofundador de la revista Bitcoin, declaró que Bitcoin necesitaba un lenguaje scripting para crear *aplicaciones descentralizadas*, pero al no lograr un acuerdo con la comunidad, *Vitalik* comenzó el desarrollo de una nueva plataforma llamada Ethereum, que es una plataforma open source descentralizada que permite la creación de acuerdos inteligentes, basada en el modelo de Blockchain.

3. Marco Teórico

3.1 ¿Qué es Blockchain?

Blockchain en español significa “Cadena de Bloques”, es un sistema de almacenamiento de información que permite mantener los datos y la información seguros de cualquier intrusión o intento de manipulación (Universidad Politécnica de Catalunya).

Desde hace mucho tiempo la información ha sido administrada por humanos, esos seres lentos, corruptibles, perezosos y hedonistas que siempre habrá la incertidumbre de

si la información está en buenas manos. Blockchain busca asignarle esta tarea a otro tipo de seres más confiables, eficaces, sacrificados y cada día más veloces… los ordenadores.

Pero todos saben la gran debilidad que tiene un sistema informático, que es hackeable. Entonces ¿cómo evita esto Blockchain?

3.1.1 Funcionamiento de Blockchain

Blockchain no funciona con un poderoso antivirus o por un vigoroso firewall, Blockchain se autoprotege gracias a su propia estructura, su propia arquitectura.

Como ya se vio anteriormente, Blockchain significa “Cadena de Bloques”, viéndolo de forma gráfica se puede decir que son cajas que están unidas entre sí y esas cajas se componen de tres partes principales:

3.1.1.1 Partes de Blockchain

Una de las partes que conforman a Blockchain es la **Información** que son los datos que contendrá el bloque, en el caso de Bitcoin puede entrar lo que sería el emisor, receptor, fecha, cantidad, etc.

Otra parte que lo conforma es el **Hash**. El Hash es el número identificador del bloque, es una serie de dígitos que es único e irrepetible y cada bloque tiene el suyo propio.

Y finalmente el **Hash del bloque anterior**, haciendo que cada bloque quede conectado con el bloque que le sigue formando una cadena, he aquí la razón de su nombre. Viéndolo de una forma visual sería como en la *Ilustración 1,* donde dentro del bloque se encuentra la información y a los costados los Hash.

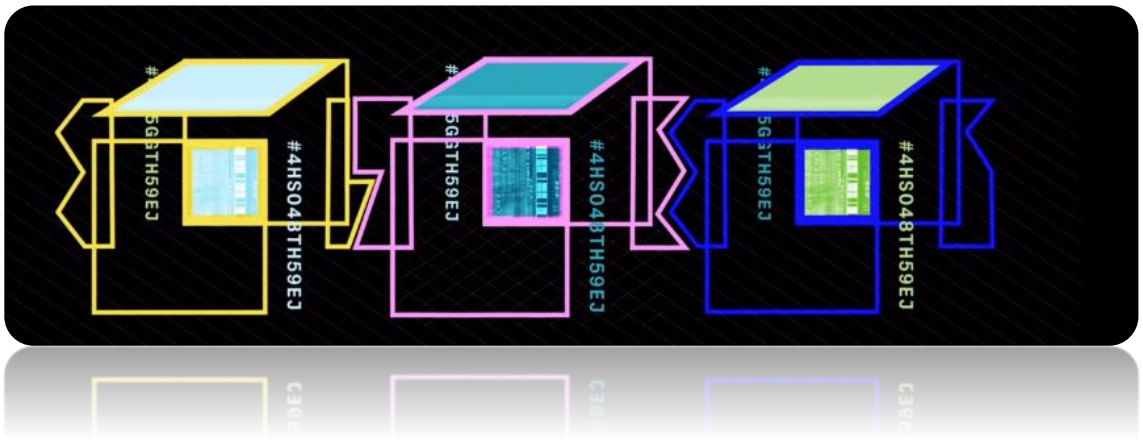


Ilustración 1 Cadena de bloques creado por canal de YouTube "PlayGround"

3.2 ¿Qué hace a Blockchain inhackeable?

Esto es gracias a principalmente 2 cosas, una de ellas es el Hash, y otra es que hay muchos ojos mirando todo el rato. Como ya se vio anteriormente, el Hash es el número irrepetible de cada bloque, pero este tiene la peculiaridad de que cambia según la información que tenga dentro. Esto quiere decir que si alguien trata de cambiar la información automáticamente cambiará también el Hash, lo que hará que ya no quede unido con su predecesor, haciendo que la cadena quede invalidada. *(Ilustración 2)*

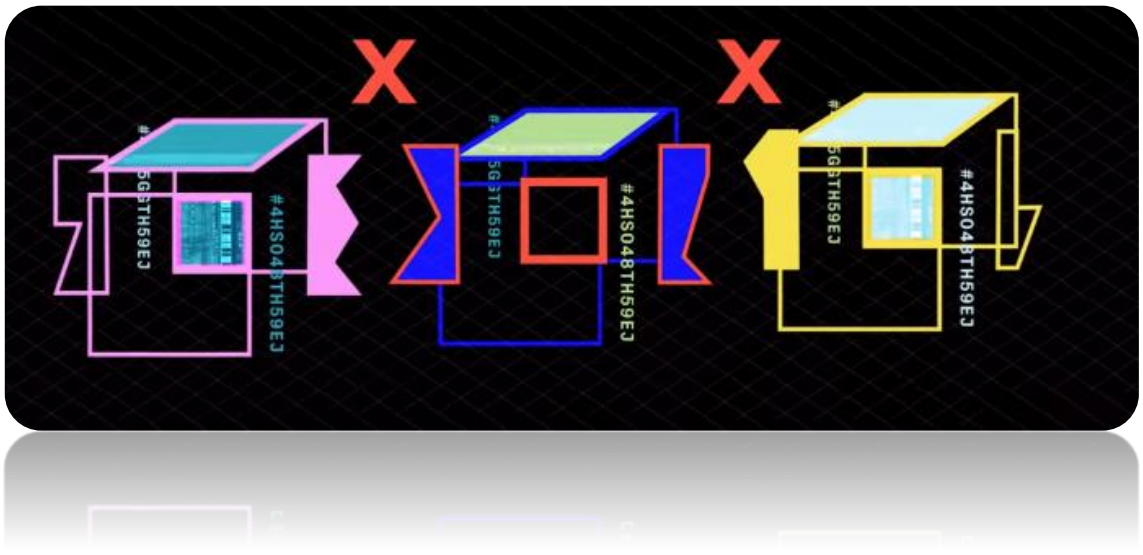


Ilustración 2 Incompatibilidad por modificación de la información.

Y no es que haya solo una base de datos, cada usuario tiene una copia de ella y dado que hay muchos ojos mirando si un usuario modifica la información la comunidad lo sabe, haciendo que su versión de la base de datos sea anulada. *(Ilustración 3)*

Ilustración 3 Anulación por manipulación de información.

Eso es lo que hace a Blockchain confiable, ya que la seguridad se la dan los mismos usuarios, no una empresa, ni una organización ni un banco, sino usuarios por igual, pero muchos.

Gracias a esta forma de trabajo, los programas o aplicaciones que utilizan como base a Blockchain se les dice que son apps descentralizadas.

4. ¿Cómo hace Blockchain para captar a sus usuarios?

Las personas pueden usar Blockchain por dos cosas, una es simplemente usar el sistema, otra es con un fin un poco más goloso, crear nuevos bloques para la cadena, aquí entran los llamados “Mineros”.

4.1 ¿Qué son los “Mineros” de Bitcoin?

Muchos usuarios de Blockchain no están ahí para usar el sistema, se concentran solamente en crear nuevos bloques. A medida que se va necesitando almacenar más información se requieren de nuevos bloques a la cadena.

4.1.1 ¿Cómo agregar nuevos bloques a la cadena?

Para añadir un nuevo bloque a la cadena se requiere resolver un problema matemático muy complejo que requiere de un gran poder de computación, aquí entra el PoW, así que los mineros ponen a toda máquina sus ordenadores para resolver el problema. Normalmente cada problema es resuelto en 10 min (Universidad de Buenos Aires. Facultades de Ciencias Económicas, Cs. Exactas y Naturales e Ingeniería, 2017). *(Ilustración 4, se puede observar de forma visual el añadir un nuevo bloque a la cadena).*

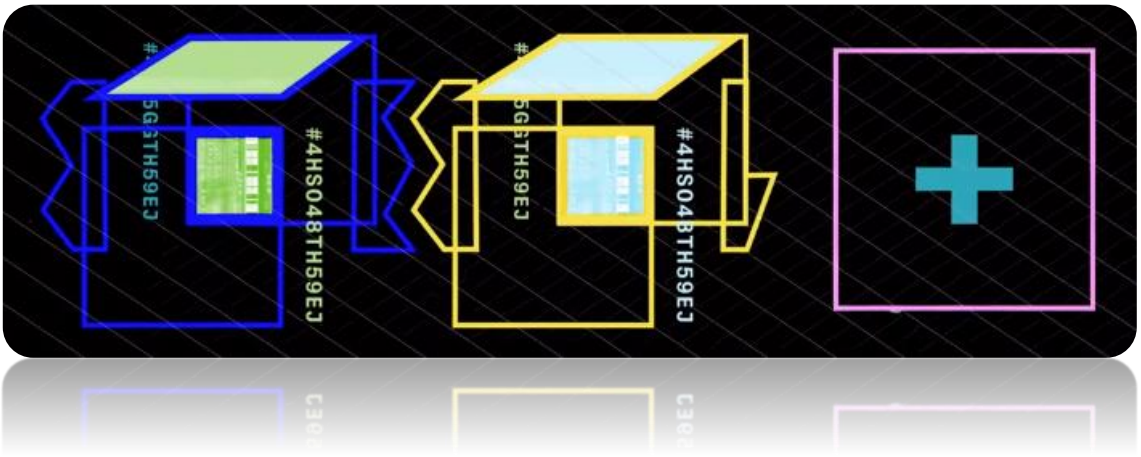


Ilustración 4 Agregar nuevo bloque a la cadena.

Una vez que creen haber resuelto el problema, la comunidad se encarga de revisar el resultado obtenido, si es el correcto el nuevo bloque es agregado a la cadena, la información es consolidada y el acuerdo se lleva a cabo, y lo más importante, el usuario que resolvió el problema recibe una remuneración que es de aproximadamente 12.5 Bitcoins, lo que no está nada mal, dado que en estos días (23/noviembre/2019) un solo bitcoin vale aprox. $140,000 pesos mexicanos o $7,300 dólares estadounidenses (Coinbase, s.f.).

5. Ejemplos de aplicaciones de Blockchain

5.1 Sector médico

Una problemática que se ha presentado desde hace tiempo es en el apartado con respecto a los datos clínicos de las personas que, si bien están catalogadas como

confidenciales, ha habido ciertos conflictos por el acceso y el uso de esta información (Arellano Mejía & Sánchez Morales, 2017).

Solo el personal con una autorización puede obtener acceso a la información clínica de los pacientes, pero también se le puede dar autorización a otras personas para ingresar la información, y nada promete que alguien pueda modificar los datos que se encuentran ahí.

Blockchain puede guardar la información del expediente, que es la prueba de la relación médico-paciente que hay, al ingresar los datos se puede tener la seguridad que éstos ya no serán modificados.

5.2 Documentaciones

Al realizar el guardado de una documentación ya sea importante o no, se quedará seguro con Blockchain. Se podrán realizar respaldos de registros como firmas, registros de tiendas o supermercados, registrar compras realizadas, etc. En el tema del comercio además de que las transacciones o pagos serán seguros también lo será el registro de la compra.

Cualquier información que requiera una documentación será difícil que pueda ser falsificado.

5.3 Votaciones políticas

Después de las elecciones presidenciales de un país, tal vez los ciudadanos no estén satisfechos con la elección que se ha realizado, y no es para más, ya que probablemente la mayoría de las personas duden de sus gobernantes políticos, puesto que el humano es muy tentado por obtener un beneficio extra, aunque no sea de una forma éticamente correcta (Universidad Politécnica de Valéncia, 2017-2018).

Con Blockchain se podrá tener la seguridad de que las votaciones no han sido manipuladas, puesto que se tendrá la información del registro dentro de la cadena por lo tanto una vez ingresado no podrá ser modificado o eliminado, de esa forma el pueblo podrá estar más seguro de que el ganador de la candidatura fue de forma democrática.

5.4 Alimentos

Con Blockchain será difícil por no decir imposible la falsificación de la procedencia de alimentos, pues la información de los mismos estará en constante vigilancia y será fácil mantenerlos rastreados, para de esa forma, evitar el desvió del producto y verificar que todo esté en orden.

5.5 Firmas de contratos

Todos los días se necesitan realizar firmas de contratos, ya sea para contratar un servicio o en el caso de las empresas llegar a un acuerdo con otra organización, pero a veces pueden llegar a ocurrir ciertas situaciones por la falsificación de una firma, el riesgo que pueda haber confusiones o incluso acciones que puedan llegar a perjudicar a la empresa o al individuo que ofrece su firma para documentos.

Al aplicar Blockchain a este campo las firmas de contratos estarán seguras. La información resguardada y la seguridad del cliente intacta.

5.6 Educación

Así es, Blockchain también se puede aplicar en el sector educativo, esto gracias a que podría ampliar el historial académico de un alumno. Según Abraham Vázquez del Observatorio de Innovación Educativa del Tecnológico de Monterrey, señala que Blockchain podría romper barreras entre instituciones, esto quiere decir que ahora en lugar de que un título tuviera que ser validado de país en país, ahora simplemente se podría tener un único certificado digital (EDUTEC. Revista Electrónica de Tecnología Educativa., 2017).

6. Marco Conceptual

6.1 ¿Qué es una aplicación descentralizada (DApps)?

Se le llama a la(s) aplicación(es) descentralizada(s) o DApps (Moto, 2018) a todas las aplicaciones que nacen basándose en Blockchain, quiere decir, que remueven la necesidad de un tercero cuando hablamos de intercambios entre una persona y un

proveedor. En la *Ilustración 5* se puede observar la diferencia entre el funcionamiento de una app en la cual se tiene un intermediario y al lado una forma visual de ver una app descentralizada.

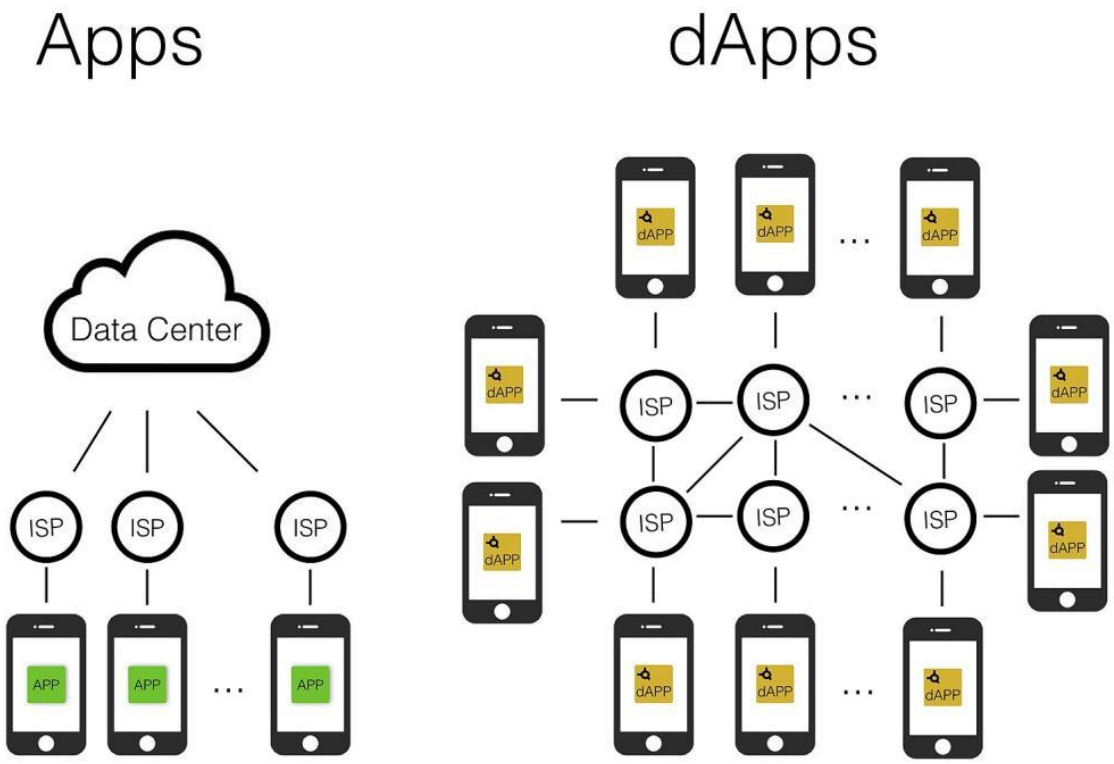


Ilustración 5 Ejemplo Apps Descentralizadas

6.2 ¿Qué es el protocolo Peer to Peer (P2P)?

El protocolo peer to peer (en español se le conoce como **red entre pares** o **red de igual a igual**) es un protocolo de red de comunicación que permite tener una relación directa entre usuario y servidor (Plata, 2019).

Permite una conexión entre nodos (ordenadores) que se comportan como iguales entre sí, esto quiere decir que pueden hacer función de cliente y servidor. Se conectan de forma directa sin la necesidad de intermediarios como servidores o controladores fijos, es decir, que se pueden compartir ficheros entre los demás usuarios que estén dentro de la red de forma directa, un ejemplo de ellos sería el Skype o el BitTorrent. En la *Ilustración 6* se puede observar de forma visual la diferencia que tiene una estructura P2P y una de cliente-servidor que es la que se utiliza normalmente.

Aunque este protocolo no es muy seguro, ya que cada persona o usuario debe encargarse que no entre ningún tipo de virus a la red, puesto que al tener acceso de conectividad con otras computadoras éste puede infectar fácilmente a otra. Además, si otros ordenadores o nodos están conectándose a una para bajar o descargar algún archivo que se haya compartido, pueden bajar el rendimiento de ese ordenador de forma considerable (Sanz Romero, 2019).

Además de que esto ha traído problemas legales con las industrias del entretenimiento por la muy llamada piratería o la violación por derechos de autor, los usuarios pueden compartir el contenido de forma libre. Es el doble filo que tiene esta red, ya que dependiendo el uso que se le dé tendrá cierto efecto a un individuo.

Pero no todo es malo con este protocolo, por ejemplo, Spotify utilizó por un tiempo esta red, pero por el gran crecimiento que tuvo logró hacerse con suficientes servidores para abastecer a todos sus usuarios. Es una ventaja de P2P, si no se cuenta con demasiado dinero como para rentar un servidor ésta es una buena forma de empezar.

De hecho, actualmente las marcas de *Xiaomi, Oppo* y *Vivo* están utilizando este protocolo para crear una aplicación que permita compartir archivos entre dispositivos sin importar de que marca sean.

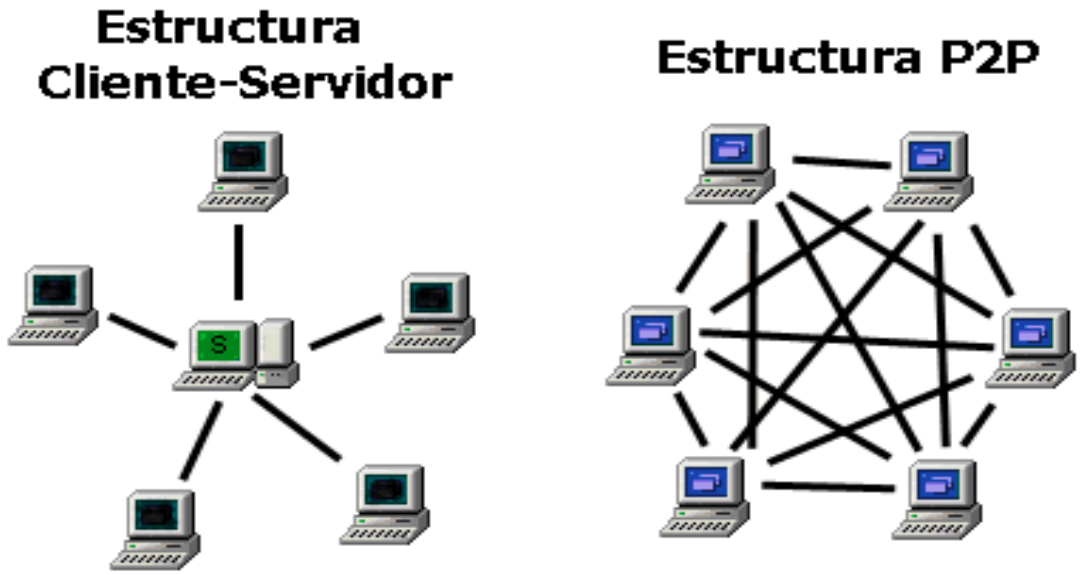


Ilustración 6 Comparación Estructura Cliente-Servidor y Estructura P2P.

Por ejemplo, si una persona tiene un video normalmente para compartirlo lo subiría a YouTube, pero en la red P2P si otra persona quiere tener ese video se lo pediría directamente al creador de ese contenido. Al mismo tiempo, esa persona al ya tener ese video lo puede compartir con otra que se lo pida, y ahora todo aquel que tenga ese video también lo puede compartir con otras personas.

6.3 ¿Qué es el protocolo PoW (Proof of Work)?

El protocolo de prueba de trabajo o PoW por sus siglas en ingles es un protocolo que consiste en que partes de una red realicen de forma exitosa un trabajo que requiera de mucha potencia computacional para poder tener acceso a los recursos de dicha red. *(En la Ilustración 7 se muestra una imagen ilustrativa de PoW).*

Este protocolo funciona a que le asignan una tarea a un usuario que luego es verificado por la red. Normalmente las tareas son problemas matemáticos complejos para que realice la computadora. Podemos poner de ejemplo a la famosa *Captcha,* la cual para poder ingresar al servicio de la red se debe pasar por una serie de pruebas en este caso sencillas para que sean resueltas, de esta manera se evita que un atacante pueda crear millones de registros y de esa manera colapsar la página web (Bit2Me, Academy by Bit2me, s.f.).

Pero cuando es comunicación entre ordenadores el problema no debe ser tan complejo, debe poder resolverse, pero con una dificultad relativa.

Lo peculiar de PoW es que su sistema es asimétrico, es decir, que por la parte del cliente el problema a resolver será algo complicado de realizar, pero la verificación por parte de la red será sencilla. Esto quiere decir que el problema lleva mucho tiempo en resolverse y es costoso hablando de recursos, pero al generarse el problema, también genera una serie de patrones que facilitan la verificación.

Ilustración 7 Imagen ilustrativa de Proof of Work.

6.4 ¿Qué es el HashCash?

El HashCash es una solución que se propuso contra los mensajes basura o también conocidos como Spam. Se basa en el protocolo PoW para verificar si un correo es basura o no (Bit2Me, Academy by Bit2me, s.f.).

El objetivo de HashCash es requerir un trabajo de computación para que este sea verificado, una vez verificado, al usuario se le da luz verde para utilizar dicho servicio. El usuario ingresa un encabezado al correo mediante HashCash, de esta forma se crea como una especie de “sello” que asegura que el correo ha pasado por una prueba de trabajo.

El sello es un identificador que demuestra o comprueba que el procesador ha utilizado el procesador por una pequeña cantidad de tiempo, pues es lo que genera un sello genuino para cada correo que se va a enviar.

Y, ¿cómo ayuda esto a evitar al spammer?

Como se mencionó anteriormente, se necesita un pequeño consumo extra en el procesador para crear el “sello”. Para un usuario que manda unos cuantos correos no será

ningún problema, ya que el consumo energético del procesador no será tan exagerado como para incrementar demasiado la factura de luz.

Pero para el spammer no es así, dado que al enviar tantos correos hace que el procesador tenga que trabajar más para poder enviar esos correos, lo que conlleva a que se necesite de más energía, por lo que la factura del spammer le llegará más elevado por el alto consumo energético del procesador.

Esto es lo que hace que disminuya la probabilidad de que el spammer envíe sus correos basura a las bandejas de entrada de los usuarios.

6.5 ¿Qué es un token?

Un token es un objeto que solo tiene valor dentro de cierto contexto. Por ejemplo, una moneda de casino, esos pedazos de plásticos que fuera del establecimiento no tienen ningún valor aparente, pero dentro del casino representan cierta cantidad de dinero para facilitar el conteo o la manipulación al momento de jugar (Ripio Blog, 2018).

Y esta es la función principal de los tokens, representar algo más. En el mundo de las criptomonedas se intercambia hacen transferencias con tokens que representarían en este caso la moneda de dicho sistema de transacción.

Pero los tokens se pueden usar para otras cosas, ya que además de representar algo económico, también pueden representar alguna recompensa o ser simplemente objetos coleccionables. Las empresas pueden emplear los tokens para representar las acciones que tiene dicha empresa.

6.6 ¿Qué es hedonismo?

El hedonismo o ser hedonista se refiere a que se busca un placer o un bien, enfocado más a uno mismo, es decir, que se busca un beneficio propio (Wikipedia, s.f.).

7. Metodología

Todo lo que se ha realizado hasta ahora en la investigación es el de recabar información y exponerla en el informe, dicha información fue conseguida de distintas fuentes, de esa forma al obtener la suficiente información se comprime o se busca lo más importante y se muestra de una forma teórica con una breve explicación en algunos conceptos para que quede un poco más claro.

Esto se hace así debido a que no todas las personas cuentan con la suficiente experiencia en el ámbito informático, de esta forma se busca hacer que cualquier persona pueda llegar a comprender el funcionamiento de esta tecnología llamada Blockchain para que pueda tener un poco de conocimiento si en algún momento esta tecnología se expande aún más.

Para que la investigación pudiera continuar sería necesario ampliarla ya no solo a investigar cómo funciona esta tecnología, sino que también a que se le podría aplicar, pero ya no generalizándola, ahora planteando bien el problema y recabar información ahora concentrado en esa área, para esto se puede usar el método científico.

Al usar el método científico se tendría que cuestionar o plantear el problema en sí, esto para poder tener un punto de partida y sabir a donde irá dirigida la investigación para poder resolver o buscar una posible solución al problema.

Después sería recabar un poco de información base, información actual donde se puedan observar los aspectos de la problemática y así tener una amplia perspectiva de lo que se necesitaría, para esto sería necesario analizar la información recabada.

Al hacer eso ya se tendría la manera de formular una serie de hipótesis donde se propondrían soluciones o percepciones sobre la situación con los datos o información ya recabada.

Una vez teniendo las posibles soluciones sería hora de ponerlas en práctica, se empezaría a experimentar para ver cual hipótesis fue la que se acercó más a una posible

solución y de ahí seguir haciendo modificaciones y seguir experimentando hasta llegar al resultado deseado.

Luego por último sería recabar los datos o resultados obtenidos para analizarlos y sacar las conclusiones sobre si es factible o no utilizar la tecnología Blockchain en el campo o la problemática que se planteó al principio, de esa forma se podrán buscar nuevas aplicaciones del Blockchain a distintos campos que puedan beneficiar a la sociedad, y no solo eso, sino que también se puede buscar una forma de evolucionar.

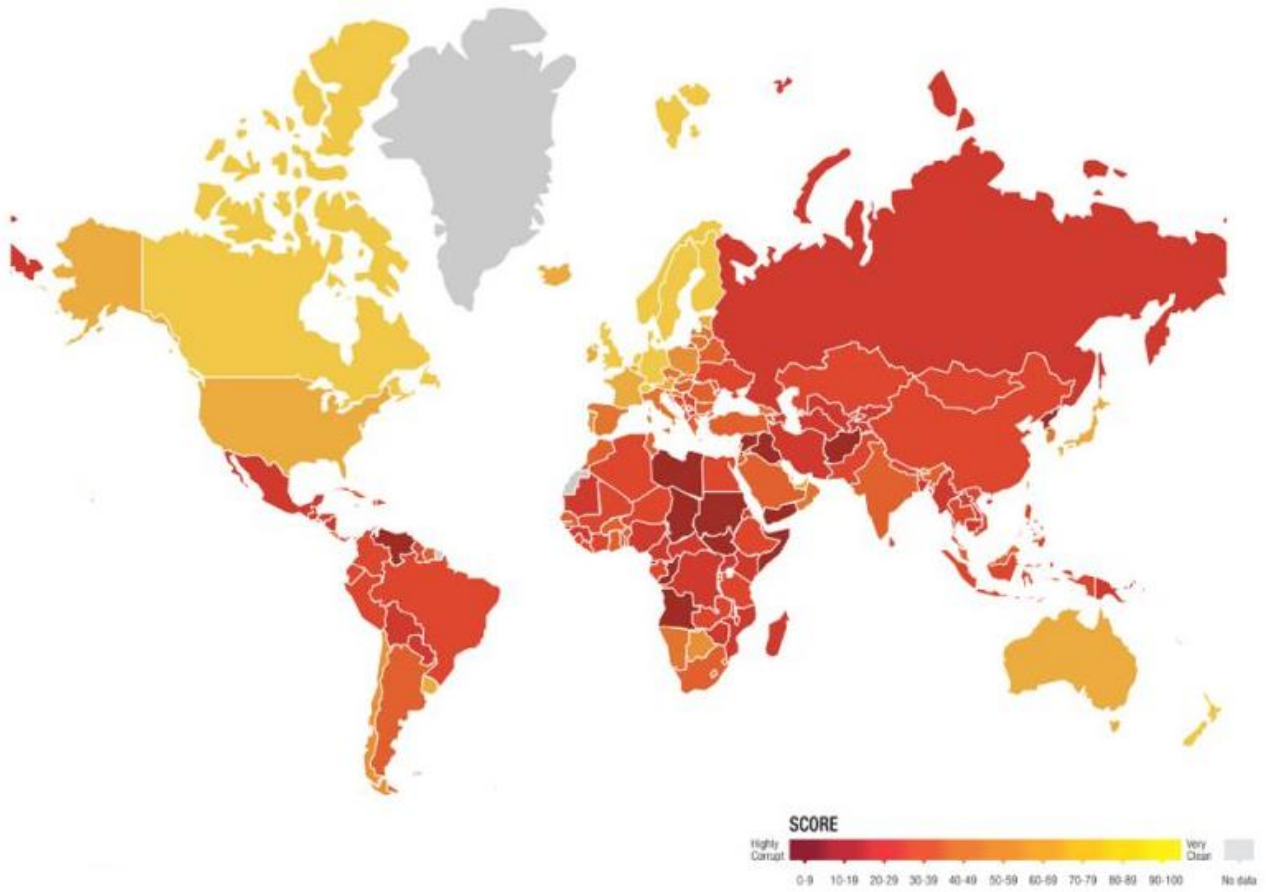
Resultados

Al ir recopilando información descubrí que esta tecnología es la que utilizan las criptomonedas, principalmente la de Bitcoin, pero también descubrí que existe una gran cantidad de criptomonedas de diferente tipo, algunas no tan valiosas como Bitcoin, pero utilizan una estructura o sistema similar.

La investigación puede seguir adelante, pero en este momento el factor principal que limita su continuación es la falta de tiempo, dado que existen más niveles de detalle que exploran algunos conceptos o funciones más detalladas, ya que blockchain, como se ha visto anteriormente, es más utilizado en el sector financiero (Bitcoin), donde en la *Gráfica 1* se puede observar la evolución de su valor.

Gráfica 1 Evolución del valor de Bitcoin, proporcionada por Coinbase

Un problema que afecta a muchos países es el índice de la percepción a la corrupción, que como lo podemos ver en la *Gráfica 2* hay muy poca transparencia entre ellos mismos, pero esto no tiene que ver solo con el gobierno, sino también con sus ciudadanos, dado que ellos son una pieza fundamental para el desarrollo de un buen gobierno democrático.



Gráfica 2 Índice de Percepción de la Corrupción 2018. (Cuentas, 2019)

Y algo que está muy ligado a la participación de la ciudadanía es la tecnología y los nuevos desarrollos que se están implementando para mejorar las vías democráticas. De esta forma, se pretende desarrollar sistemas con la ayuda de las nuevas tecnologías que mejoren la participación de los ciudadanos, y al mismo tiempo mejorar la comunicación entre ellos y la tecnología. Una forma para incentivar la participación ciudadana es con el ya mencionado Blockchain, por medio de un sistema de votaciones electrónicas (Universidad Politécnica de Valéncia, 2017-2018).

A pesar de que Blockchain no es una tecnología reciente (inició en 1991), no se ha aplicado en otras áreas mas que en el sector financiero con las criptomonedas.

Pero Blockchain es más que criptomonedas, como lo dijo Verónica Tan, directora de Infocomm Media Development Authority *"Más allá de las criptomonedas, la tecnología blockchain se trata de colaboración. Es una tecnología colaborativa que permite que diferentes actores trabajen juntos compartiendo y consumiendo datos. Eso es asombroso para los gobiernos, las instituciones privadas y cómo la sociedad puede crear cosas nuevas"* (Gusson, 2019).

Conclusiones

Después de haber realizado esta investigación pude darme cuenta que la tecnología evoluciona de todas las maneras buscando facilitar o ayudar a nuestras tareas diarias o a facilitar algunos aspectos de nuestra vida como lo es el caso de Blockchain.

Blockchain se utiliza principalmente en el sector financiero en la actualidad con las famosas criptomonedas, pero hay algo en esta tecnología que va más allá de dinero digital. Blockchain puede ayudarnos en distintos aspectos de nuestra vida cotidiana.

Y así como la tecnología evoluciona nosotros también debemos actualizarnos en la información de ésta, en mi carrera que es Ing. En Sistemas Computacionales es un aspecto importante, ya que llegará nueva tecnología la cual se debe estudiar.

También es importante realizar investigaciones para la difusión de esta información, debido a que muchas personas desconocen estos temas y no se pueden dar cuenta de las soluciones que se pueden obtener al utilizar de distinta forma la tecnología que tenemos actualmente y la que vaya llegando.

Y no solo eso, sino que también las escuelas o instituciones capacitoras actualicen sus matrículas y especialidades para que de esa forma los alumnos se capaciten también

con la información más reciente y actualizada ampliando más sus competencias en el campo laboral.

La gestión de información por medio de cadena de bloques puede ayudarnos bastante en varios aspectos de nuestra vida, ya que podemos confiar que nuestra información estará segura, hay muchas cosas en las que se puede usar Blockchain, pero aún no han sabido como aplicarla.

De hecho, los mismos creadores no sabían en que aplicarlo hasta que se les venció la patente, pero una persona o grupo de personas lo usaron como base para la famosa criptomoneda de Bitcoin. Pero se ha estado observando que Blockchain tiene más campos de aplicación, solo se deben buscar, hay que explorar hasta donde se puede llegar con esta tecnología.

Pero si bien es cierto, todos sabemos que puede haber errores, "*todo lo que es creado por el hombre tiene fallas",* pero esto no quiere decir que todo es malo o que todo está mal hecho, simplemente las cosas se crean como una base y después debe evolucionar con el paso del tiempo, los errores darán información de lo que está mal para poder solucionarlo, y la experiencia se encargará de evitar ese error en un futuro.

Y Blockchain no se salva de ello, todo el entorno evoluciona, y las amenazas también, pero Blockchain también se adapta a estas situaciones. Con la llegada de nueva tecnología, nueva información, nuevos conocimientos, se puede hacer que la red sea aún más segura y que pueda ser aplicada en más campos o sectores que nos faciliten mas aspectos de nuestra vida cotidiana.

Ya que Blockchain es más que solo Bitcoin o que una simple base de datos, Blockchain es un sistema de almacenamiento de información que podría crear una sociedad más equitativa, más transparente y más veraz.

Bibliografía

Arellano Mejía, J., & Sánchez Morales, C. A. (Abril-Junio de 2017). *SciElo*. Obtenido de ¿El expediente clínico debe ser clasificado como confidencial y reservado?: http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0028-37462017000200111

Binance Academy. (18 de Noviembre de 2019). *Binance Academy*. Obtenido de La Historia de Blockchain: https://www.binance.vision/es/blockchain/history-of-blockchain

Bit2Me. (s.f.). *Academy by Bit2me*. Obtenido de Qué es Prueba de trabajo / Proof of Work (PoW): https://academy.bit2me.com/que-es-proof-of-work-pow/

Bit2Me. (s.f.). *Academy by Bit2me*. Obtenido de Qué es el HashChash: https://academy.bit2me.com/que-es-hashcash/

Brandom, R. (9 de Enero de 2019). *The Verge*. Obtenido de Why the Ethereum Classic hack is a bad omen for the blockchain: https://www.theverge.com/2019/1/9/18174407/ethereum-classic-hack-51-percent-attack-double-spend-crypto

Coinbase. (s.f.). *Coinbase*. Obtenido de Precio Bitcoin: https://www.coinbase.com/price/bitcoin

Cuentas, R. (2019). *Rendir Cuentas*. Obtenido de ÍNDICE DE PERCEPCIÓN DE LA CORRUPCIÓN 2019: http://www.rendircuentas.org/noticia/indice-percepcion-la-corrupcion-2019/

EDUTEC. Revista Electrónica de Tecnología Educativa. (2017). En *BLOCKCHAIN EN EDUCACIÓN* (pág. 4).

Gusson, C. (14 de Noviembre de 2019). *Cointelegraph*. Obtenido de ¿Por qué los gobiernos y las corporaciones necesitan blockchain?: https://es.cointelegraph.com/news/why-do-governments-and-corporations-need-blockchain

Harán, J. M. (Abril de 2019). *Welive Security*. Obtenido de Blockchain: problemas de seguridad que giran alrededor de esta tecnología: https://www.welivesecurity.com/la-es/2019/04/02/blockchain-problemas-seguridad-alrededor-tecnologia/

Mario. (6 de Octubre de 2019). *Dirigentes Digital*. Obtenido de Los diez países que más usan criptomonedas: https://dirigentesdigital.com/economia/los-diez-paises-que-mas-usan-criptomonedas-GA1233686

Moto, E. (20 de Junio de 2018). *Qore*. Obtenido de ¿Qué es una aplicación descentralizada?: https://www.qore.com/noticias/65116/Que-es-una-aplicacion-descentralizada

Plata, U. N. (2019). Facultad de Informática. En I. M. Gallardo Urbini, *Certificados Digitales: de una arquitectura jerárquica y centralizada a una distribuida y descentralizada* (pág. 101). La Plata, Argentina.

Ripio Blog. (19 de Julio de 2018). Obtenido de ¿Qué es un token y cómo funciona: https://www.ripio.com/ar/blog/que-es-un-token-y-como-funciona/

Sanz Romero, M. (14 de Septiembre de 2019). *Computer Hoy*. Obtenido de ¿Qué es P2P y en qué consiste?: https://computerhoy.com/reportajes/tecnologia/p2p-que-es-489221

Universidad de Buenos Aires. Facultades de Ciencias Económicas, Cs. Exactas y Naturales e Ingeniería. (2017). Carrera de Esepecialización en Seguridad Informática. En J. A. Aguirre Regato, *Cadena de bloques: potencial aplicación a Historias Clínicas Electrónicas* (pág. 16). Buenos Aires.

Universidad Politécnica de Catalunya. (s.f.). En C. Dolader Retamal, J. Bel Roig, & J. L. Muñoz Tapia, *LA BLOCKCHAIN: FUNDAMENTOS, APLICACIONES Y RELACIÓN CON OTRAS TECNOLOGÍAS DISRUPTIVAS* (pág. 34). Cataluña.

Universidad Politécnica de Valéncia. (2017-2018). En P. García Mateo, *Blockchain aplicado al sector púnlico* (pág. 59). Valéncia.

Universidad Politécnica de Valéncia. (2017-2018). En P. García Mateo, *Blockchain aplicado al sector público* (pág. 26). Valéncia.

Wikipedia. (s.f.). Obtenido de Hedonismo: https://es.wikipedia.org/wiki/Hedonismo