

BlockChain: un panorama

Johnnathan Steven Navarro Mafla

Monografía como requisito parcial para la obtención del título de Tecnólogo
Informático



UNIVERSIDAD DE
MANIZALES

Universidad de Manizales
Facultad de Ciencias e Ingeniería
Programa Tecnología Informática
Febrero 2018

Introducción

En la siguiente documento se pretende abordar los elementos y características principales que definen la cadena de bloques – blockchain-, de igual manera se espera poder llegar a dar algunas claridades teóricas para definir dicho sistema así como sus aplicaciones, sin embargo se pretende hacer un relación entre las diferentes categorías que serán descritas para llegar así a conclusiones y recomendaciones generales de acuerdo con los acercamientos teóricos, sobre una técnica que es poco conocida en el contexto nacional, específicamente blockchain que es utilizada actualmente en criptomonedas como bitcoin o ethereum que son las más reconocidas mundialmente, sin embargo el bitcoin se ha valorizado tanto que muchas personas compran fracciones de esta o en muchos casos compran varios bitcoin para luego volverlos a vender cuando este se haya valorado más, aún así otros prefieren el minado de criptomonedas que también es un gran negocio, pero se requiere de una buena inversión ya que para poder minar, se necesita gran capacidad de cómputo pero especialmente tarjetas gráficas (GPU) por lo que hoy en día existen GPU solo para minar criptomonedas, aun así se requiere de tiempo y paciencia para que este proceso de minado de su recompensa. En este documento se presentarán los tipos de aplicaciones que actualmente se está utilizando con la cadena de bloques, porque no solo este sistema se utiliza con las criptomonedas, ya que ofrece otros beneficios para otras áreas como por ejemplo el voto electrónico que, si llegase a implementarse en todos los continentes, se evitaría fraudes que actualmente suceden en muchos países.

Actualmente la cadena de bloques se considera una gran oportunidad para crear nuevas ideas de negocio, ya que son sus propiedades las que hacen que este sistema sea lo

suficientemente popular en muchos lugares, por lo que en Colombia tan solo se ha hablado poco de esta tecnología, sin embargo, el bitcoin ya se oye por algunos lugares de este país, como en Pereira que ya existe un lugar donde comprar esta criptomoneda, así pues, más adelante se explicará lo que se conoce del blockchain en Colombia, y se tendrá como conclusión, los posibles beneficios y las desventajas que tiene ésta tecnología en el presente y en su impacto en el futuro.

Contenido

Capítulo 1 La Tecnología Blockchain	1
Definición	1
Pilares de Blockchain.....	3
Capítulo 2 Aplicaciones Blockchain.....	6
Bitcoin.....	6
Ethereum	8
El voto electrónico	9
True Trace.....	10
Capítulo 3 Blockchain en Colombia.....	11
Capítulo 4 Conclusiones y Recomendaciones	14
Referencias.....	17

Lista de Figuras

Figura 1. Cómo funciona el sistema de pago Blockchain.....	3
Figura 2. Gráfica del valor del bitcoin desde el año 2012 hasta la actualidad.....	8

Capítulo 1

La Tecnología Blockchain

Definición

La definición de blockchain o también conocido como cadena de bloques está aludido a la tecnología de la criptomoneda bitcoin, que fue desarrollada por Satoshi Nakamoto, en la cual, implementa algoritmos bastante sofisticados donde ubica el blockchain una parte fundamental para que esta moneda virtual funcione. Ésta tecnología muchos la conocen como cadena de bloques o como el gran libro de contabilidad, donde cada bloque almacena datos y después se une para facilitar la verificación de información que por esta circula.

Adicionalmente, el concepto de blockchain trata de una tecnología de codificación de información, que está oculta detrás de la criptomoneda, por lo cual mantiene en pie el uso constante de esta misma. Actualmente muchas personas en diversos países donde es aceptado el bitcoin opten por usarla más que cualquier otra moneda física, por la multitud de servicios que puede ofrecer, como por ejemplo, las transacciones bancarias, que las utilizan para el cambio continuo de éstas, o por medio del internet de las cosas, por lo tanto, la tecnología blockchain logra complacer a muchos usuarios por su gran capacidad de codificación que lo hace muy seguro.

Para entender un poco más la definición de blockchain: Castro Gómez (2017) define:

El Blockchain o cadena de bloques es un registro público de transacciones que se mantiene mediante una red distribuida de computadores, que no requiere respaldo de ninguna autoridad central o una tercera parte y que ofrece un esquema transaccional libre de intermediarios, gracias al uso de algoritmos criptográficos. Sería como el libro de registros de contabilidad de una empresa en donde se registran todas las entradas y salidas de dinero, aunque en este caso hablamos de un libro de acontecimientos digitales que no requiere de un intermediario centralizado que identifique y certifique la información, sino que está distribuida en múltiples nodos independientes entre sí que la registran y la validan sin necesidad de que haya confianza entre ellos.

La cadena de bloques, es como un gran libro de cuentas donde en cada bloque se almacena dicha información por medio de algoritmos, es decir, si una persona le va pasar dos bitcoins a otro usuario esta transacción pasa por la cadena de bloques para validar de que el primer individuo si tenga esa cantidad de bitcoins en su cuenta y retirarlos, para luego transferir los dos bitcoins a la otra persona, y continuar validando que a ese sujeto se le sumaron los bitcoins a su cuenta, así mismo éste proceso se continuará haciendo para cada transferencia, que se haga dentro de este sistema.

Para dar una mayor claridad de cómo funciona la cadena de bloques, a continuación, se expone un breve ejemplo de los pasos a seguir:

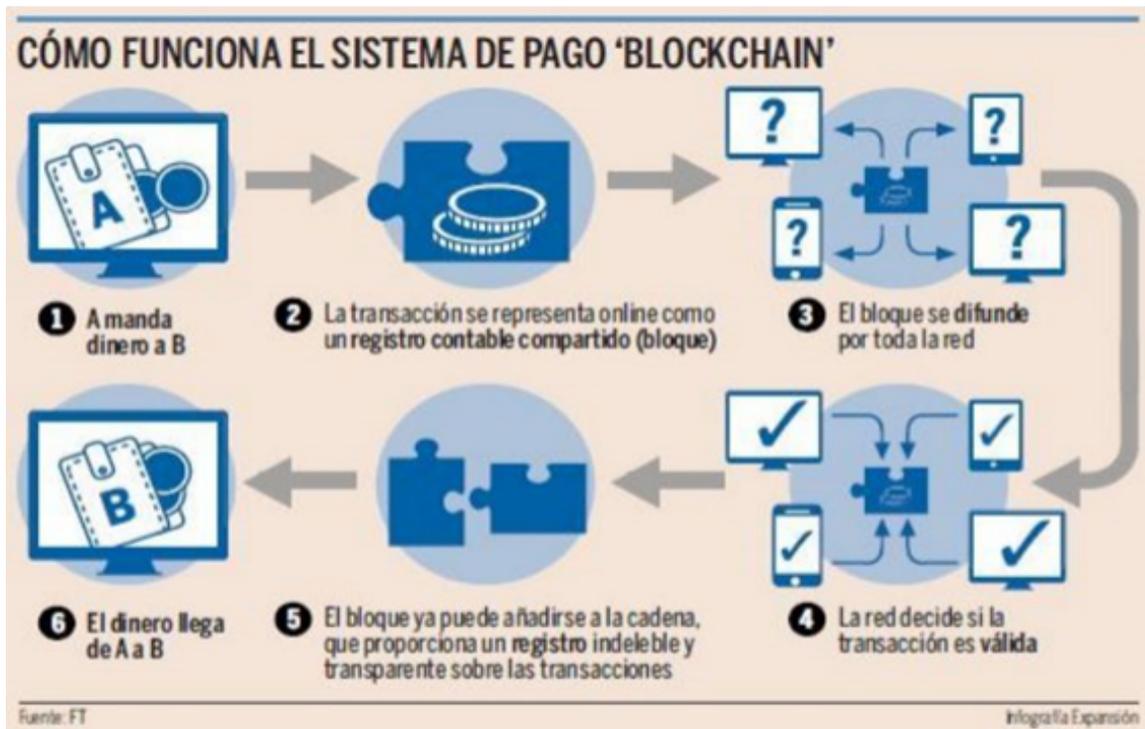


Figura 1. Cómo funciona el sistema de pago Blockchain.

Expansión (2017). Recuperado de

<http://www.expansion.com/empresas/banca/2017/09/02/59aad815ca4741f2768b461d.html>

Pilares de Blockchain

La cadena de bloques es considerada hoy en día como una importante tecnología, para el sustento del bitcoin y toda su red, por lo que es importante conocer cómo funciona en todo su entorno práctico en relación a su actividad; el blockchain tiene algunos pilares necesarios para que esta ciencia sea lo que es hoy en día:

Inmutabilidad: El significado de esta palabra proviene del latín *inmutabilis* que significa no se puede cambiar ni tampoco modificar, en cuanto a cómo funciona la inmutabilidad en la cadena de bloques, García. A (2017) dice que: “Permite identificar transacciones, o información en diferentes formatos, identificarlos con un código único, y registrarlos en un registro imborrable, inmodificable y universal” permitiendo que este pilar sea una de las tecnologías más atractivas del blockchain, por otro lado a muchos de los usuarios no les interesa mucho la idea de que las líneas de código sean inmutables porque si en algún momento necesitan verificar la datos de algún usuario si se tiene la sospecha que puede ser falso, en efecto, se pueda recurrir a editar el código para confirmar la información del usuario; ahora bien Iglesias.P (2017) opina que: “Sería el primero en firmar por un blockchain editable si en efecto esto sirviera para proteger a los que de verdad lo merecen frente a documentos y registros que han demostrado ser falsos. Pero me da la impresión de que acabara siendo utilizado por aquellos a los que precisamente menos nos debería interesar proteger”, con esta cita se puede decir que aunque muchas personas quieran que esta tecnología sea mutable en las diferentes implicaciones que puede tener el hacerlo, de igual manera ya no sería una ciencia tan gustativa para los usuarios al saber que su información puede ser editada por terceros y esto demostraría una total caída del uso de la misma.

Red descentralizada: A partir de un punto central donde se pueda almacenar la información de cualquier tipo de contenido en la actualidad, como por ejemplo un servidor, es aquí donde los administradores de alguna red se pueden conectar para acceder a esta información y así tener un control de todo lo que fluye por ella, por el

contrario la red descentralizada del blockchain hace que ningún archivo o dato queda almacenado en un solo lugar y esto hace que toda la información esté viajando por la red donde esta pueda estar conectada, en otras palabras García. A (2017) escribe en uno de sus artículos: “Es una topología de red caracterizada por la ausencia de un servidor central o de referencia. La suma de todos los equipos clientes (denominados nodos) se vinculan unos a otros de modo que ninguno de ellos, ni siquiera un grupo estable de ellos, tiene poder de filtro sobre la información que se transmite en la red”, con esto podemos decir que cualquier persona al entrar en este sistema su información nunca será almacenada en ningún lugar a nivel de cómputo por lo tanto hace que toda su estructura de código sea única. Los dispositivos electrónicos por los cuales se conectan los usuarios ya sea computadoras, celulares, tablets, ipad etc. son las que mantienen esta tecnología operativa y la red cada vez más estable y duradera por lo cual dichos aparatos hacen parte de toda la red descentralizada del blockchain cada día más grande y difícil de hackear, haciendo que el valor del bitcoin y sus usuarios aumente cada año más.

Capítulo 2

Aplicaciones Blockchain

El uso del bitcoin se ha convertido en tendencia a nivel mundial por lo cual muchos usuarios la utilizan para realizar pagos de alguna compra realizada ya sea en un almacén, restaurante o un supermercado como ha sucedido en algunos países donde esta criptomoneda ya es común para el cambio o como medio de pago en estos establecimientos, no obstante el crecimiento del blockchain ha hecho que se implementen nuevas aplicaciones para el uso continuo de la misma en varios sectores del desarrollo mundial entre ellos tenemos:

Bitcoin

Este es una moneda digital (criptomoneda) creada por Satoshi Nakamoto, por la cual no se encuentra controlada por bancos centrales que la distribuyan, esta funciona por medio de los usuarios que la conforman, es decir, que para que esta moneda actúe en su entorno, el bitcoin debe estar de cliente en cliente y de esta manera no es necesario que haya un punto central para almacenarla, a su vez cada usuario tiene una combinación criptográfica con la que accede a identificarse en la red, lo cual permite comprar y descontar bitcoin de su cuenta controlando cada transferencia por medio de su código. Dicho de otra manera, según los creadores del sitio Bitcoin en Español (2012) en un documento llamado bitcoin la moneda del futuro, postulan que:

Bitcoin es una moneda electrónica descentralizada, concebida en 2009 por quien se ha dado a conocer como Satoshi Nakamoto (aunque su verdadera identidad se desconoce). El nombre Bitcoin se aplica también al software libre diseñado por Nakamoto para la gestión de dicha moneda, y a la red P2P (peer to peer, o red de “pares” bajo un mismo protocolo) que le da soporte. A diferencia de la mayoría de las monedas, el funcionamiento de Bitcoin no depende de una institución central, sino de una base de datos distribuida. El software ideado por Nakamoto emplea la criptografía para proveer funciones de seguridad básicas, tales como la garantía de que los bitcoins solo puedan ser gastados por su dueño, y nunca más de una vez. (p. 17,18)

Sin embargo el bitcoin se ha convertido en una confiable moneda de cambio para muchas personas, llegando a utilizarlas para el pago de recuperación de información por causa de un virus llamado wannacry que infectó a muchas computadoras en varias partes del mundo, sucedió en mayo del presente año, esto da a pensar que el bitcoin se ha vuelto importante para muchos de sus usuarios, llevándolo a valorizar cada día más gracias a sus diferentes aplicaciones que tiene y puede llegar a tener con el uso continuo del mismo.

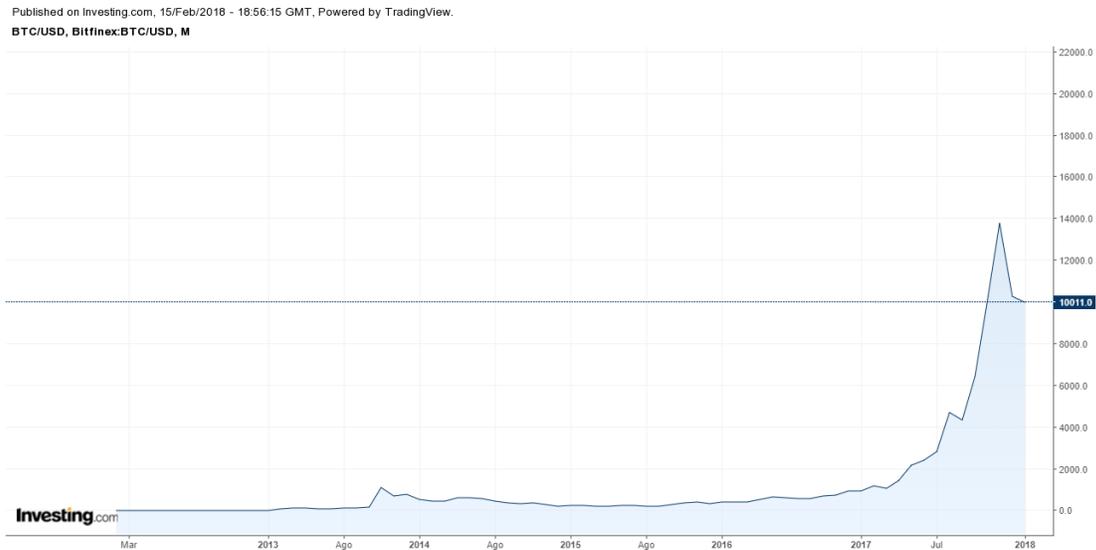


Figura 2. Gráfica del valor del bitcoin desde el año 2012 hasta la actualidad.

Investing. (2018). Recuperado de <https://es.investing.com/currencies/btc-usd-chart>

Ethereum

Es una entidad que desarrolló un programa que realiza contratos en una cadena de bloques, es un poco parecido al funcionamiento del bitcoin, pero como todo tiene sus diferencias, en el artículo que escribe Rodriguez.E (2017) en omicron afirma que:

“los ethers son ‘infinitos’, algo que no ocurre con los Bitcoins (donde hay un número definido), además de que el cálculo y el premio obtenido son diferentes. La recompensa, en concreto, no es variable, como en el BTC (que cada 210.000 bloques minados cambian de valor a

la mitad, lo que se conoce como halving), sino que vale siempre 5 ethers.”.

Es por esta razón que ethereum en los últimos meses ha estado ganando mayor aceptación en el campo de la criptomoneda, no obstante ether también tiene la posibilidad de que pueda ser minado, pero como se decía anteriormente la recompensa es diferente, aun así hay algunas compañías se dedican a diseñar y crear gráficas especiales ya que gracias a ellas se hace más fácil el minado y por ende la tecnología de las tarjetas de video han aumentado su rendimiento al ver su potencial en el minado de criptomonedas.

El voto electrónico

Esta es una tecnología innovadora que ayuda a evitar varios problemas gracias a las características que tiene el blockchain como sería el anonimato, evitar que las personas obtengan el voto más de una vez, impedir que terceros puedan alterar la cantidad de votos para un beneficio, promoviendo la seguridad de cada usuario, comprobando que no tenga la posibilidad de agregar votos ilegales, aún así no se ha implementado a nivel mundial este sistema que ayudaría a muchos gobiernos a librarse de posibles manipulaciones indebidas de los votos, vale la pena decir que esta tecnología abre las puertas a varias posibles aplicaciones que puede llegar a tener el futuro y de lo cual hace que la informática favorezca el crecimiento seguro de las naciones.

True Trace

Es una propuesta realizada por kolokium que se basa en la tecnología del blockchain que permite a los usuarios localizar los objetos que envían a otros lugares utilizando métodos como identificación QR, de esta forma el usuario podrá verificar el movimiento del objeto gracias a una aplicación que escanea el código, para tener una mayor claridad de que es true trece Rodríguez.N (2017) escribe que:

Permite hacer seguimiento de cualquier mercancía que se encuentre en el sistema. Basta con que alguno de los participantes de la cadena logística (operador o usuario) cuente con la identificación del objeto para poder acceder desde cualquier lugar del mundo, sin necesidad de ninguna acreditación al historial de seguimiento del objeto. Este historial es inalterable a pesar de ser público, dadas las características de la tecnología Blockchain. (p. 6)

Capítulo 3

Blockchain en Colombia

Sin duda el mundo ha estado cambiando gracias a la tecnología del bitcoin y a sus diferentes métodos que han de utilizar para el uso de esta moneda virtual, sin embargo en Colombia ya están utilizando esta tipo de cambio por lo que ya sus usuarios lo van aceptando como tendencia y con ello se suman a muchas personas que quieren experimentar cómo es la actividad de ésta, siendo así, en la ciudad de Pereira del municipio de Risaralda, una empresa dispuso a establecer un cajero electrónico que permite comprar bitcoins de manera fácil y segura, hay que hacer notar que esta máquina no es permitido retirar dinero en efectivo, solo es posible comprar algunas criptomonedas. En un artículo hecho por Tamayo. J (2017) en la página xataka, escribe con respecto al uso de este cajero:

Usar el cajero es muy simple, únicamente se debe tener el código QR de la billetera a la que se transferirá el monto. Cuando un cliente ingresa el dinero en efectivo, en la pantalla le muestra a cuánto equivale en la moneda que va a comprar. La empresa encargada de su instalación es CompuDeMano, un distribuidor de productos Apple que también acepta monedas virtuales como método de pago, en sus tiendas ubicadas en varias ciudades del país.

Como se sabe, para comprar bitcoins es necesario que cada transacción pase por la cadena de bloques, con ello se puede decir que ya se está utilizando el blockchain en Colombia y con ello se da a conocer el funcionamiento de sistema no solo en las demás ciudades del mundo, sino en nuestro país, por lo que implica que Colombia no está fuera de las diferentes tendencias que surgen cada día en todo el mundo, de igual manera la tecnología que se emplea detrás de la compra del bitcoin, también es utilizada de otras formas en Colombia, ahora bien surge la idea de nuevos métodos para utilizarla como lo expone Aguilar (2017) en una entrevista hecha para cripto noticias, por medio del Ministerio de Tecnologías de la Información y las Comunicaciones, en donde escribe que:

Blockchain ha mostrado un potencial teórico en la creación de confianza en un entorno descentralizado y por ende reduciendo los costos de transacción. De igual forma se ha hecho evidente su utilidad en soluciones que requieren autenticación y trazabilidad. En ese orden de ideas, dos campos potenciales de aplicación de la tecnología blockchain son el sector salud y el sector comercio. En salud, en lo que tiene que ver con autorizaciones y pagos en el sistema y en comercio en lo relacionado con trazabilidad y lucha contra el contrabando y adulteración de bienes.

En relación a lo dicho en la cita, Colombia tiene una buena visión para el uso de la cadena de bloques en varias empresas que pueden ayudar a impulsar la economía del país

y aumentar el uso de nuevas técnicas avanzadas, aún así este sistema puede incentivar a universidades a enseñar este tipo de tipologías de redes en sus diferentes programas de tecnología para que los estudiantes diseñen nuevas formas de utilizarla, no obstante la maestría en derecho internacional ofreció una conferencia sobre el impacto del blockchain en Colombia.

Capítulo 4

Conclusiones y Recomendaciones

Como resultado de la revisión bibliográfica realizada sobre el blockchain y teniendo en cuenta las comparaciones realizadas con otras investigaciones se concluye que la evolución de la tecnología de la cadena de bloques ha hecho que varias empresas opten por aplicar este concepto en sus nuevos proyectos, haciendo que esta ciencia aumente su crecimiento y se favorezca el uso de las nuevas tecnologías, otro punto es de aceptar que la confiabilidad que aporta a sus muchos beneficios, hace que sus usuarios expresen el gran aporte que hace esta técnica a las diferentes aplicaciones que puede tener, sin embargo para tener la tecnología es necesario tener un buen conocimiento sobre ella, ya que se puede implementar en diferentes áreas de negocio, por lo que exige que las personas tengan un grandes competencias en programación y la inversión que se hace para implementarla es de un costo elevado para tener excelentes resultados sobre ella.

Lo interesante de esta tecnología, es la confiabilidad que ofrece al hacer una transacción, ya que es prácticamente imposible de hackear su red por sus numerosos algoritmos que la preceden, otro punto es el ahorro que tiempo y papel al momento de hacer las transacciones, evitando así alteraciones que podrían hacerse si se hicieran en un papel, por otro lado esto mismo puede usarse en elecciones para votar electrónicamente evitando las falsificaciones de los votos y haciendo mucho más seguro votar.

Vale la pena decir que la cadena de bloques podría ofrecer grandes beneficios a las diferentes áreas de trabajo que existen actualmente, que no solo sea del sector privado sino también para el sector público, como puede ser en hospitales, colegios, universidades, entidades gubernamentales, entre otros, esto porque al no poder falsificar documentos ya estando dentro de la red, eliminando intermediarios que puedan alterarlos; no obstante es de tener en cuenta que se debe pensar bien la manera de cómo se va utilizar y que tipos de datos se van a tener en este sistema ya que una de las características que tiene el blockchain es ser imborrable e inmutable, por lo que sería imposible poder cambiar un dato que pueda afectar alguna persona.

Por otro lado, son pocos los desarrolladores en el mundo que tienen las suficientes capacidades para entender y construir un proyecto con blockchain, ya que como hay poca documentación de este sistema, se hace difícil entenderlo completamente, aun así, es de planificar bien si se pretende tener esta tecnología para un negocio a futuro por la cantidad de tiempo y recurso que cuesta implementarlo, en definitiva, se requiere de tiempo y paciencia para obtener una recompensa.

Ahora bien, esta ciencia aunque lleva varios años en servicio aún le falta mucho por desarrollarse para que pueda ser lo bastante segura y aceptable para las diversas áreas de trabajo que existen, ya que aún no se conocen las implicaciones que puede causar en el futuro, porque son pocos los estudios que se han hecho para que esta tecnología sea lo bastante viable, por lo que aún falta mucho por descubrir, sin embargo es de valorar el

gran camino que lleva hasta el momento y aun si llegará el día en que las criptomonedas se terminaran, blockchain podrá continuar mostrándose como una gran tecnología para explotarla de manera correcta y que pueda ayudar a muchas personas a entender más a fondo el funcionamiento y los beneficios que puede ofrecer.

Referencias

- Aguilar, D. (2017). Gobierno colombiano considera blockchain para planes de desarrollo del país. *Criptonoticias*.
- Bitcoin en Español (2012). La moneda del futuro, que es cómo funciona y por qué cambiará el mundo. En BITCOIN (págs. 1-197). elBitcoin.org.
- Banca 2.0 (2016). Blockchain: El futuro ya. (págs. 38-39).
- BBVA Innovation Center (2016). El avance de bitcoin y de los pagos virtuales TECNOLOGIA BLOCKCHAIN (págs. 1-25) *Serie fintech*.
- Berenguer, J. (2017). Blockchain la tecnología que está en boca de todos (págs. 1-3). *ANDBANK/private Bankers*
- Economía (2017) Blockchain y sus aplicaciones prácticas.
- Brakeville, S., & Perepa, B. (2016). Fundamentos básicos de blockchain: Introducción al control de negocio.
- Cano M, Jeimy J. (2017). Blockchain: “Cadena de bloques”. Reflexiones sobre seguridad y control. *Revista sistemas*.
- Canos, F. (2017). Las aplicaciones del blockchain. *Diarioabierto*.
- Castro Gómez, S. (2017). Blockchain: mirando más allá del Bitcoin. *Semana Económica*, 1-10.
- Criptonoticias (2018) ¿Qué es bitcoin?
- Criptonoticias (s.f.) ¿Qué es ethereum?
- Dave. (2017). Los 7 principios de la tecnología blockchain. *Visión crítica, economía, tecnología*.
- Delgado Von Eitzen, C. (2017). ¿Qué es blockchain y que usos tiene? Lo puede cambiar todo. *Blog de ChiristianDvE (Beta)*.
- Digital, C. C. (2017). Tecnología blockchain disponible en Colombia. *Colombia Digital*.

Iglesias, P. (s.f.). Algunos puntos a considerar sobre la inmutabilidad del blockchain. *PabloYglesias*.

Fintech Observatorio. (2017). Aplicaciones de la tecnología blockchain más allá del bitcoin. (págs. 1-17). *Equipo Fintech*.

Fintech. (2017). Patentan un sistema de votación basado en blockchain. *Observatorio finanzas y tecnología*.

Galván, P. (s.f). Blockchain y sus aplicaciones. *Sg software guru*.

García, A., & Valencia, L. (2017). Los cinco grandes pilares del Blockchain. *Blog Post*.

Georges, J. (2017) La cadena de bloques (blockchain) Una cadena disruptiva con el poder de evolucionar el sector financiero. *Equisoft*

Guggiari, J. (2015). Blockchain: La tecnología que descentraliza al mundo. (págs. 1-6) *JoséGuggiari*.

Lage Serrano, O. (2017). ¿Es 'blockchain' realmente inmutable? *BBVA Revolución Blockchain*.

Moreno, C. (2017). El mito de la inmutabilidad de Blockchain. *Tu asesor bitcoin*.

Muñoz de Frutos, A. (2017). ¿Qué es blockchain? *Computerhoy*.

Ortiz, F. (2017). Usos del blockchain más allá del bitcoin. *Mcpro muycomputer*

Padilla, S. (2017). Una evolución efectiva. *El espectador, Economía*.

Rodriguez Garcia, E. (2017). Todo sobre ethereum, la moneda virtual de moda que está eclipsando a bitcoin. *Omicrono. Bitcoin criptomonedas*.

Rodriguez, M. (2016). 15 aplicaciones de la tecnología blockchain más allá de bitcoin. *Fintech, Observatorio finanzas y tecnología*.

Tamayo, J. (2017). Colombia ya tiene su primer cajero electrónico de bitcoin.

Tapscott, A. Tapscott, D. (2016). La revolución blockchain, Descubre cómo esta tecnología transformará la economía mundial. (págs. 1-20).