

1-1-2017

Análisis de los principales elementos del bitcoin como criptomoneda y producto commodity en el comercio nacional

John Alexander Lara Lara
Universidad de La Salle, Bogotá

Manuel Alejandro Muñoz Agudelo
Universidad de La Salle, Bogotá

Follow this and additional works at: https://ciencia.lasalle.edu.co/administracion_de_empresas

Citación recomendada

Lara Lara, J. A., & Muñoz Agudelo, M. A. (2017). Análisis de los principales elementos del bitcoin como criptomoneda y producto commodity en el comercio nacional. Retrieved from https://ciencia.lasalle.edu.co/administracion_de_empresas/1427

This Trabajo de grado - Pregrado is brought to you for free and open access by the Facultad de Ciencias Administrativas y Contables at Ciencia Unisalle. It has been accepted for inclusion in Administración de Empresas by an authorized administrator of Ciencia Unisalle. For more information, please contact ciencia@lasalle.edu.co.

Análisis de los Principales Elementos del Bitcoin como Criptomoneda y Producto Commodity en el Comercio Nacional

JOHN ALEXANDER LARA LARA.

MANUEL ALEJANDRO MUÑOZ AGUDELO.

Resumen:

Al momento de realizar un diagnóstico de la situación actual del bitcoin como producto commodity en el comercio mundial, resulta evidente encontrar tres grandes posiciones frente a la legalización y regulación de monedas virtuales como ésta; hay países que la aprueban y por lo tanto las propuestas de regulación buscan la mejor forma para su adaptación; los que se mantienen imparciales tanto en su permisión como en su regulación; y los que definitivamente buscan su prohibición y guían su regulación en tal propósito; como es el caso de Colombia, en donde una de sus más grandes desventajas radica en la poca acogida que un sistema de transacción descentralizado y libre de tributación pueda generar entre el gobierno a través de la Superintendencia Financiera y el sector bancario con el Banco de la República, que mediante comunicado deslegitiman la legalidad de ésta y cualquier otra moneda virtual. En este sentido, propender por una investigación académica que aporte a contextualizar en nuestra economía temas de actualidad mundial que representen maneras diferentes de desarrollar los negocios en los mercados globalizados, cuyas nuevas tecnologías obligatoriamente generan y generarán cambios, compromete a los graduandos y entes de formación profesional a liderar juntos, labores en la búsqueda de procesos más eficientes e igualitarios. A continuación, el lector encontrará argumentos de carácter contextual acerca del bitcoin desde su origen y como ha sido su desarrollo en el país, como elementos clave para el análisis de las ventajas y desventajas de su implementación en el comercio nacional.

Palabras Clave: Dinero, Bitcoin, Criptografía, Globalización, Sistema Financiero, Descentralización.

Analysis of the Main Elements of the Bitcoin as Cryptomonedas and Product Commodity in the National Trade

JHON ALEXANDER LARA LARA.

MANUEL ALEJANDRO MUÑOZ AGUDELO.

Summary:

At the moment of making a diagnosis of the current situation of bitcoin as a commodity product in world trade, it is evident to find three great positions against the legalization and regulation of virtual currencies like this one; There are countries that approve it, so the proposals for the regulation look for the best way to adapt it. The ones that maintains unbiased between the regulation and the prohibition and who definitely are against the bitcoin and other virtual currencies and guide their regulation in this particular direction as is the case of our country, in which one of its greatest disadvantages lies in the little welcome that a system of decentralized and tax-free transaction can generate in the government Through the Financial Superintendence of Colombia and the banking sector with the Banco de la Republica, throughout an announcement de-legitimize the legality of this and any other virtual currency. In this sense, to promote an academic research that contributes to contextualize in our economy current issues worldwide and represent different ways of developing businesses in globalized markets, whose new technology generate and will generate even more changes ; engages undergraduate and universities to work together in the search for more efficient and egalitarian processes. The reader will then find contextual arguments about bitcoin from its origin and how it has been developed in the country, as key elements for the analysis of the advantages and disadvantages of its implementation.

Key Words: Money, Bitcoin, Cryptography, Globalization, Financial System, Decentralization.

1. Introducción

Debido a la importancia e impacto positivo que representa para la economía mundial atender a los cambios producidos a partir de las nuevas tecnologías tras el fenómeno de la globalización y sus actuales deficiencias y desigualdades, debe ser una prioridad académica e investigativa para las disciplinas asociadas al contexto económico, político y social; los temas relacionados con el bitcoin como moneda de intercambio y preservación de valor y su propuesta de un sistema monetario a prueba de monopolios. Datos estadísticos hacen referencia a que las bitcoin ganan cada día más adeptos y se han apreciado tanto que en marzo de 2017, superaron por primera vez el valor del oro, el activo refugio por excelencia. La cotización de la moneda virtual supero a comienzos del mes los 1.280 dólares (CoinDesk, 2017) , frente a los 1.230 que rondó el metal dorado para la misma fecha. Conviene tener en cuenta que este comportamiento se debe tanto a la apreciación del dinero virtual, que tres meses después se cotiza a 1.781, como a la depreciación del metal. La incertidumbre política por la indefinición de los planes de Donal Trump, las elecciones en varios países de la Unión Europea, el alza del dólar y la volatilidad del oro, han contribuido a que los inversionistas adquieran nuevos riesgos (Hernández, 2017).

Gráfica 1. Cotización del bitcoin Junio 2016- mayo 2017.



Fuente: (Bitcoin.Org, 2017)

Jorge López, analista de la firma XTB, asegura que no veremos a grandes inversionistas ni a grandes gestoras interesadas en ellos, sino a pequeños jugadores que se lo toman como una apuesta. Sin embargo, los Bitcoin superan actualmente los 2,3 millones de carteras de consumo, lo que lo convierte en uno de los servicios de cartera más populares del mundo. También, ha desarrollado un motor de búsqueda que permite a los usuarios verificar las transacciones rápidamente en el libro de contabilidad

público de la moneda, conocido como la cadena de bloqueo de bitcoin. En los países desarrollados, el dinero virtual sigue siendo en gran medida el juguete de los entusiastas de la tecnología y los especuladores. En los mercados emergentes, donde algunos ven un enorme potencial para los Bitcoin, la infraestructura para procesar transacciones simplemente no existe. Entonces, para que Bitcoin sea adoptado más ampliamente, los partidarios dicen que la moneda virtual debe encontrar una aplicación única que lo llevará más allá del ámbito de la especulación. Y para que eso suceda, se debe primero construir una plataforma robusta; que es lo que Bitcoin está tratando de hacer, a través del Blockchain, hacer más fácil para las personas en todo el mundo utilizar Bitcoin (López, 2015).

El sector financiero genera un doble gasto al servir como tercero “confiable” para el procesamiento de pagos electrónicos puesto que el costo de la mediación incrementa los costos de transacción, limitando el tamaño mínimo práctico por transacción y eliminando la posibilidad de pequeñas transacciones casuales, debilidades inherentes a un modelo basado en confianza. Por el contrario, el bitcoin surge en 2009, justo después de la crisis y propone una solución basada en redes entre pares (per-to-per) como un sistema descentralizado de moneda digital que, a través del uso de un programa público, permite la transmisión de fondos de una moneda inexistente en un formato físico entre usuarios anónimos; algo así como un E-mail, eliminando la necesidad de la presencia de instituciones financieras en las transacciones. Adicionalmente, mantiene registros que no pueden ser alterados sin tener que realizar complicados cálculos matemáticos, la seguridad es bastante alta puesto que se basa en primitivas criptográficas de seguridad demostrada, la escalabilidad del sistema, por diseño e implementación, hace que su desempeño en el mediano y largo plazo esté garantizado. De ahí, que pese a que reúne todas las características potenciales para ser considerado una moneda, encuentra en los gobiernos y el sector financiero sus principales detractores.

Por lo anterior, actualmente políticos, inversionistas y el resto de la sociedad están tratando de comprender la naturaleza de ésta forma de dinero y las implicaciones que tendrá en la sociedad (Gutiérrez, 2015). Este documento recoge una investigación descriptiva de los principales elementos del Bitcoin como Criptomoneda. Para ello, se parte de un análisis histórico del dinero, posteriormente se ubicará el origen del Bitcoin como moneda virtual en 2009, para hacer un seguimiento a su desarrollo en el panorama mundial y como ha sido su llegada al país, puesto que Colombia no ha sido ajena al fenómeno. Finalmente, el documento busca servir como referente a futuras investigaciones y contribuir a la sociedad otorgándole a las propuestas modernas el carácter de necesidad que se demanda, para poder responder a los retos actuales de la humanidad en un nuevo

orden mundial, pues da la sensación de estar ante un fenómeno de consecuencias económicas y sociales muy profundas.

A esta altura, el colapso del sistema financiero tal y como lo conocemos es algo inevitable. No hace falta un posgrado en economía para entender que nadie puede vivir indefinidamente por encima de sus ingresos. Esto, que es válido para cualquier individuo, también lo es para familias, ciudades, países y continentes. Lamentablemente, muy pocos están tomando las medidas necesarias para protegerse en la gran depresión que se avecina. Los adoctrinados, los apáticos y los interesados en mantener el statu quo integran la inmensa mayoría de la población. Los demás están demasiado ocupados intentando sobrevivir a la expansión del aparato estatal (Bitcoin.Org, 2017). En el momento de escribir estas líneas, el mundo occidental sufre una profunda crisis económica: Estados Unidos tiene dificultades para consolidar su techo de endeudamiento y la unión Europea se bambolea al son de los mercados que "atacan" las emisiones de deuda de los países periféricos, con Grecia es una situación de práctica quiebra, Portugal, Irlanda y Chipre en situaciones críticas, y España e Italia a punto de entrar en un punto económico de no retorno (Olier, 2012) .

2. Antecedentes

En 1947, en la selva central de Brasil una expedición a cargo del sabio italiano Metarosso logró establecer un trueque mudo con la tribu indígena de los xavantes, excepcionales guerreros que aún a mediados del siglo XX y con armas primitivas habían logrado oponer tenaz resistencia a la tarea "civilizadora" y el empuje colonizador de los europeos. De ahí, que a ésta tribu le cupo la suerte de conservar sus antiguas costumbres y su organización tribal, conservando casi en estado virgen las relaciones propias de la sociedad humana primitiva. Los xavantes, son el arquetipo de las relaciones comunales primitivas pues sus armas y medios de producción; la flecha, la lanza, el cuchillo, el hacha, la canoa, etc., son primitivos y rudimentarios. Por esta circunstancia, precisamente, el trabajo colectivo para ellos es una necesidad imperiosa. Por consiguiente, trabajan conjuntamente, y los medios de producción son, naturalmente, de propiedad común. Lo obtenido con el trabajo colectivo se distribuye equitativamente entre los miembros de la tribu, es decir, trabajan para conseguir los bienes indispensables, que les aseguren la subsistencia a los miembros de la comunidad (Robert, 2006).

En consecuencia, el intercambio de mercancías comienza allí, donde termina la comunidad: en los puntos de contacto con otras comunidades y en la mayoría de los casos se produce como consecuencia de los rasgos específicos del medio natural en que habita cada una de las diferentes comunidades. Las materias que tienen igual importancia para todos, se encuentran sólo disponibles en los territorios de unos u otros, de tal manera que las restantes ordas solo podían obtenerlas a través del trueque. De ahí entonces, que los terrenos fértiles, la vecindad de los ríos, el acceso al mar, los accidentes montañosos de interés y el control de las rutas comerciales se convierten en objeto de la política de Estado primitivo y por supuesto también de los Estados contemporáneos (Rosales, 2005).

No obstante, para que el trueque fuera posible, era necesario que algunas comunidades produjeran ciertas cosas a cambio de las cuales y en vista de su utilidad, otras comunidades estuviesen dispuestas a dar una parte del excedente de lo producido por ellas. De esta manera, tuvo comienzo la producción destinada al trueque sistemático. En este proceso, la comunidad adquirió gran pericia en la fabricación de ciertos productos, la producción se desarrolló, se perfeccionaron los instrumentos de trabajo, el hombre se enriqueció con nuevas experiencias, y la colectividad fue elevando consecuentemente su nivel de vida. Con el tiempo, algunas tribus se destacaron en el laboreo de la tierra y otras en el pastoreo de ganados. Esta fue la primera gran división social del trabajo. Más tarde, comenzaron a desarrollarse los oficios: tejeduría, herrería, alfarería, etc. Gradualmente, las personas que practicaban algún oficio, "oficiales" se fueron separando de la comunidad. Es entonces cuando tiene ocurrencia la segunda gran división social del trabajo: los oficios se desarticulan de la actividad rural. De esta manera, la esfera del intercambio de mercancías se amplió considerablemente (Robert, 2006).

Al comienzo el intercambio era realizado por los jefes de las tribus o los ancianos del clan y todo aquello que se cambiaba era propiedad de la comunidad; pero, con el ahondamiento llevado a cabo en la división del trabajo y el desarrollo logrado en la producción, gracias al perfeccionamiento de los instrumentos de trabajo, se hizo posible el empleo de un menor número de personas para el cumplimiento de las faenas de la comunidad. Una familia, por ejemplo, podía labrar una parcela, o cuidar y mantener un rebaño, o atender el trabajo de un taller. El trabajo colectivo, cedió el puesto al trabajo individual, la propiedad social comenzó a transformarse en propiedad privada y el intercambio de mercancías pasó gradualmente a manos de los jefes de familia. Es entonces cuando tiene comienzo la descomposición del régimen comunal primitivo. Aquellas familias, cuyos miembros tenían en su poder parcelas más fértiles u ocupaban en la comunidad la dignidad de jefes, militares o sacerdotes, aprovechaban su posición para su enriquecimiento personal. Se apoderaron entonces de una parte considerable de la propiedad social y de los medios de producción, a consecuencia de lo cual la

mayoría de los miembros de la comunidad, quedaron, al fin y a la postre sumidos en la indigencia, pues eliminada la propiedad social, no adquirieron propiedad privada. El enriquecimiento, sin embargo, fue más rápido para aquellos que traían esclavos como producto de las campañas militares. Además, los ricos reducían a la esclavitud no solo a los prisioneros de guerra, sino también a sus paisanos, empobrecidos y endeudados. Como ahora con su trabajo, el hombre podía producir mayor cantidad de bienes que los que necesitaba para su manutención, entonces era posible apropiarse de este sobrante, amén de que prevalidos en los privilegios otorgados por el poder económico los ricos forzaban a los venidos a menos económicamente a trabajar cada vez más. La pasada igualdad, la propiedad del régimen común y el trabajo colectivo habían desaparecido (Robert, 2006).

Los resultados de la investigación de Metarosso vinieron a confirmar de manera brillantísima las posiciones teóricas de la economía científica, acerca de que en los albores de la sociedad humana, en el transcurso de decenas de miles de años, el dinero fue una noción absolutamente desconocida. El hombre de la sociedad comunista primitiva vivió y se desarrolló sin tener la menor idea acerca del dinero. Esto significa, que el dinero no es eterno. Apareció en un periodo determinado de la historia, cuando su intermediación fue necesaria y de la misma manera desaparecerá cuando esta necesidad haya perdido su valor histórico (Robert, 2006). El dinero es un fenómeno social, que solo existe dentro de marcos sociales y económicos particulares, de ahí que pueda ser inexistente en algunas sociedades, mientras que en otras puede asumir diferentes formas (Harris, 1985) .

Debido a las características de producción de cada territorio, diferentes artículos cumplieron el papel del dinero; pieles, hachas, anzuelos, tejidos, cueros, cuchillos, espadas, lanzas, barras metálicas, alambre, etc. Pero, el oro en virtud de determinadas características naturales resulto el más apto para desempeñar este papel. No obstante, el oro tuvo ciertas incomodidades que conllevaron a que los ricos y comerciantes comenzaran a proveerse de barras acuñadas. Esta tarea muy pronto fue acaparada por los gobernantes quienes se apoderaron del poder exclusivo de acuñar dinero (Robert, 2006). Otros autores coinciden en señalar que el dinero ha sido definido por los economistas como cualquier cosa que se acepta en pago de bienes y servicios, o como reembolso de deudas. De tal manera que la moneda circulante en billetes y monedas, no es más que un tipo de dinero que cumple con tres funciones primarias en una economía; el dinero debe servir como: medio de cambio, unidad de cuenta y depósito de valor. Al ser algo, generalmente aceptado, se define por la conducta de los individuos, lo que afirma aún más su fenómeno social (Mishkin, 2008).

Para entender aún más la función del dinero como medio de pago y sus ventajas, conviene pensar en lo siguiente: en una economía de trueque, los bienes y servicios se intercambian de manera directa por otros bienes y servicios, de tal manera que una persona que desee intercambiar un bien por otro, primero debería encontrar a alguien que posea el bien que ella desea y segundo, contar con suerte y esperar que esa persona quiera intercambiar su bien por el que ella le ofrece. En caso negativo sería necesaria una tercera persona que sirva de puente para este intercambio o seguir buscando a alguien que tenga el bien deseado y que esté dispuesto a cambiarlo por el bien que se le ofrece (López, 2015). En cambio que una economía monetaria, un bien particular, el dinero, puede cambiarse por cualquier bien y cualquier bien puede cambiarse por dinero, pero los bienes (distintos del dinero) no pueden cambiarse entre sí (Harris, 1985).

De la misma manera en que se miden las distancias en términos de kilómetros, o los pesos en términos de kilogramos, se puede medir el valor de cualquier bien o servicio en términos de unidades de dinero (Mishkin, 2008). Así, el autor ejemplifica claramente la segunda función del dinero, servir como unidad de cuenta. Por último, como depósito de valor, implica que el dinero debe conservar su poder adquisitivo a través del tiempo, lo que significa que es posible guardarlo y gastarlo en una ocasión posterior. La función del dinero de servir como depósito de valor está estrechamente relacionada con la de ser medio de cambio, pues para que cumpla su función en el intercambio debe mantener su valor a lo largo del tiempo, de tal manera que, un activo cualquiera que se use como medio de cambio, necesariamente debe ser un depósito de valor (Reina & Zuluaga, 2006).

Dado que las personas pueden almacenar sus riquezas ya sea en forma de dinero o de otros activos, el hecho de que tan bueno sea el dinero como depósito de valor depende del nivel de precios. Por ejemplo, durante las etapas inflacionarias, es decir, aquellas en las que el nivel de los precios aumenta con rapidez y por tanto el valor del dinero disminuye, las personas difícilmente desearían usar el dinero como almacén de su riqueza, es más, el uso del dinero para hacer transacciones declinaría (Harris, 1985). Tal fue el caso durante la hiperinflación de Alemania después de la primera guerra mundial, cuando las tasas de inflación superaron el 1000% al mes, inclusive, hay testimonios que muestran que se necesitaba, por ejemplo, una carretilla llena de dinero para comprar una pieza de pan (Mishkin, 2008). Por otra parte, (Harris, 1985), afirma que los cigarrillos fueron un medio de cambio en Alemania cuando la inflación de los años veinte deprecia los billetes.

En el caso de Colombia, desde el mismo descubrimiento de América se introdujeron monedas acuñadas en España a nuestro continente; pero, a medida que incrementaron las necesidades, se

comenzó a acuñar moneda en La Nueva Granada y en 1700 la acuñación de la moneda paso a ser función del virreinato. Sin embargo, es justamente en la época de la independencia, donde se presenta un aumento exponencial en la cantidad de monedas acuñadas para sufragar los gastos que demandó el conflicto. Ya es en 1870 cuando se funda el primer Banco privado en Colombia, el cual tenía la facultad de emisión de billetes, claro está, de naturaleza privada (López, 2015).

Hasta 1886, cuando bajo el mandato de presidente Rafael Núñez se estableció el curso legal o forzoso del billete del Banco Nacional, esta disposición cobro especial fuerza cuando prescribió el carácter de moneda legal de la República a éste billete, su recibo obligatorio en el pago de las rentas y contribuciones públicas, al igual que las transacciones entre particulares y prohibió estipular cualquier otra especie monetaria en los contratos. De esta manera, el estado tomo para sí el monopolio de la emisión monetaria. La implementación del curso forzoso, implica que los billetes no están respaldados por ningún metal, sino en la credibilidad del billete y de quien lo emite. Esto es distinto del patrón oro, donde los billetes impresos estaban respaldados por el metal, y por consiguiente, un billete podía ser convertido en oro (Hernández, 2001).

Desde que se implementó el curso forzoso en 1886, hasta que se inició la guerra de los mil días en 1899, la cantidad de billetes en circulación se multiplicó por diez y cuatro años después se multiplico 21 veces, lo cual devino en una elevación inmoderada de los precios internos, llegando a una tasa de inflación de 389% anual. En el periodo comprendido entre 1905 y 1923, se expidieron cuatro normas que sucesivamente cambiaron las características de la unidad monetaria, cuya finalidad era establecer un sistema financiero basado en el oro, pero no pasaron de ser más que intentos; el modelo continúa vigente hoy en todos los países del mundo (Reina & Zuluaga, 2006). Es entonces, en 1923, cuando se contrata a un grupo de expertos que encabezó el profesor Kemmerer de la Universidad de Princeton, con el fin de recibir asesoría sobre la modernización de las finanzas públicas y del sistema financiero nacional; como resultado de esta misión, se creó el Banco de la República como única autoridad a cargo de la emisión de dinero, también se le atribuyó la función de banco de bancos, regular la moneda y las tasas de cambio (López, 2015).

Desde entonces y hasta 1931, los billetes emitidos por este banco podían ser cambiados por su equivalente en oro a voluntad de los tenedores, lo que llevo a que la moneda nacional se denomine peso oro. Sin embargo, en el año de 1931 fue necesario abandonar el respaldo en oro debido a la gran crisis económica mundial de 1929, lo que significó que el dinero ya no tendría valor por su respaldo en oro y circuló como medio legal de pago, como algo que solo tiene valor porque las leyes y

costumbres lo han investido de poder para actuar como medio de cambio, unidad de cuenta y depósito de valor (López, 2015). Otra de las consecuencias de la gran depresión fue que a partir de ahí, el gobierno aumentó significativamente su injerencia en el funcionamiento del banco, pues desde sus inicios, el Banco de la República bajo la asesoría de Kemmerer, había nacido como un banco independiente del ejecutivo y de los intereses sectoriales (Uribe, 2013).

Con la reforma de 1951, del presidente Laureano Gómez, el énfasis del banco se enfocó principalmente en fomentar el crecimiento económico, debilitando el objetivo de preservar el poder adquisitivo del dinero. No obstante, la controversia sobre el manejo monetario volvió a pasar a un primer plano cuando se adoptó la idea de crear una Junta Monetaria, elegida en su totalidad por el gobierno, para que ejerciera como autoridad monetaria, mientras que la junta directiva del Banco de la República, pasó a ejercer funciones meramente administrativas, situación que siguió operando así hasta la reforma constitucional de 1991 y en virtud de lo dispuesto en el artículo 371 superior, el banco de la República adquirió total independencia del gobierno, sin mencionar que es a partir de aquí con la expedición de la ley 31 de 1992 cuando se establece con claridad que es el banco de la República que ejerce en forma exclusiva e indelegable el atributo estatal de emitir la moneda legal en Colombia, que la unidad monetaria y unidad de cuenta en el país es el peso emitido por el Banco de la República y que es el único medio de pago de curso legal Fiat o forzoso. Recuerden, el dinero fiat o fiduciario son las monedas y billetes que no basan su valor en una contrapartida en oro; sino, en su declaración como dinero por el Estado por medio de una ley y la fe en su futura aceptación. Actualmente, todas las monedas nacionales incluyendo el dólar, el euro y las demás monedas de reserva son monedas fiduciarias o Fiat (Barrera, 2011).

3. El Bitcoin: La Moneda del Futuro

Una vez realizado el análisis de los antecedentes del dinero y su modelo con el fin de analizar las principales características del Bitcoin como Criptomoneda, se considera conveniente ahora, analizar la que ha sido llamada la moneda de la era digital. El Bitcoin es un protocolo de comunicación en línea lanzado en 2009 y una nueva forma de moneda digital, creada con el propósito de brindar mayores ventajas de las que ofrece el sistema financiero tradicional (López, 2015), sobre todo, cuando la confianza en el sector bancario se ha visto afectada por acontecimientos tan graves como la crisis económica mundial de 2008, un crimen sin castigo que costó a millones de personas sus ahorros, sus trabajos, sus hogares, sus sueños; algunos, sus vidas. Cuando, a partir del 2000, gobiernos de diferentes países comenzaron una política de desregulación con desastrosas consecuencias al mismo

tiempo que privatizaban los principales bancos; en solo cinco años, llegaron a estar endeudados por diez veces el valor de la economía de algunos de estos países, crearon fondos de inversión y los banqueros recomendaron poner depósitos en estos fondos, cuando en realidad lo único que buscaban era dinero suficiente para crear una gran estafa que involucra empresas auditoras y agencias calificadoras de riesgos para construir confianza en los ahorradores pero los banqueros y sus amigos se enriquecieron, se creó una enorme burbuja financiera inflada con mentiras que eventualmente generaría grandes ganancias privadas de grandes pérdidas públicas (Ferguson, 2010).

Tal es el caso de Grecia, que se ha visto obligada a solicitar ayuda externa a la Unión Europea, dada su imposibilidad de hacerle frente a la crisis; para resolverla, paradójicamente la prioridad de los gobiernos se ha basado en el restablecimiento de la confianza en el sistema bancario (Serrano, 2008). Bitcoin busca optimizar el sistema de pagos en línea y reducir sustancialmente las validaciones del sistema financiero actual, en el que empresas como Master Card, Visa y American Express pueden cobrar comisiones del 2 al 3% a efectos de administrar una transacción. Entonces, Bitcoin es en sí mismo un protocolo para el intercambio de valor a través de Internet sin un intermediario. Se basa en un sistema de contabilidad pública, donde se registra cada una de las transacciones y se basa en la criptografía para efectos de validación (López, 2015).

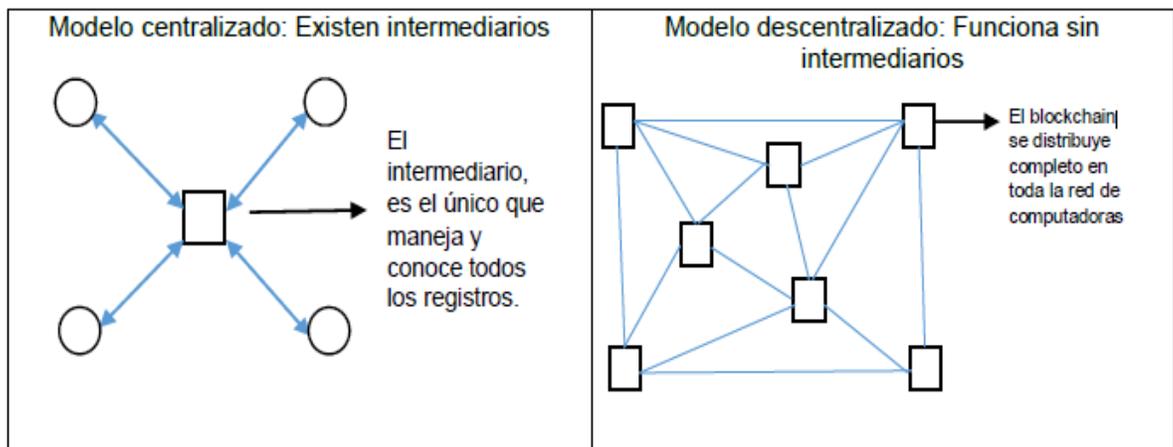
Según Andolfatto, gerente de un banco central de la reserva de Estados Unidos, los bancos centrales bien administrados deben dar la bienvenida a la competencia emergente, refiriéndose al bitcoin. De hecho, el funcionamiento, impacto, crecimiento y expansión del bitcoin, ha generado que gobiernos, empresarios y medios de comunicación de todo el mundo fijen su atención en la que ha sido llamada la moneda de la era digital. Satoshi Nakamoto es el seudónimo utilizado por el o los creadores de bitcoin, todo inició en 2008, cuando fue publicado un documento titulado Bitcoin: A Peer-to-Peer Electronic Cash System, también conocido como el paper Bitcoin; en él, se explica el funcionamiento del protocolo bitcoin y el propósito de la creación de la moneda digital que recibe el mismo nombre. Sin embargo, es en 2009 cuando realmente entra en funcionamiento. A la moneda digital bitcoin también se le conoce como Criptomoneda, debido a que el software creado utiliza la encriptación para controlar la creación o transferencia de los bitcoins. Aún hoy, la identidad del creador de la moneda digital más famosa de internet, sigue siendo un misterio y la obsesión por conocerla crece debido al éxito del bitcoin y a las implicaciones que suponen su adopción frente al sistema financiero tradicional.

3.1 características del bitcoin.

3.1.1 descentralización.

Bitcoin trabaja bajo una aplicación de red P2P, conocida también como Peer-to-Peer o de igual a igual que permite que la comunicación entre los equipos de la red se dé, sin pasar por un servidor dedicado, siendo ésta directa entre parejas de host o máquinas conectadas a la red de tal manera que cada equipo se puede comportar a la vez como cliente y servidor y el sistema puede operar bajo una base de datos distribuida. Esta base de datos es conocida como la cadena de boques o Blockchain que funciona como un libro contable descentralizado donde se registran todas las transacciones de la red. El Blockchain se distribuye completo en todos los nodos de la red, lo que le confiere una de sus principales características, no hay una entidad o banco central que regule este sistema monetario, sino que todo está manejado por una serie de computadoras descentralizadas (López, 2015).

Gráfica 2. Modelo de distribución de la plataforma Blockchain.

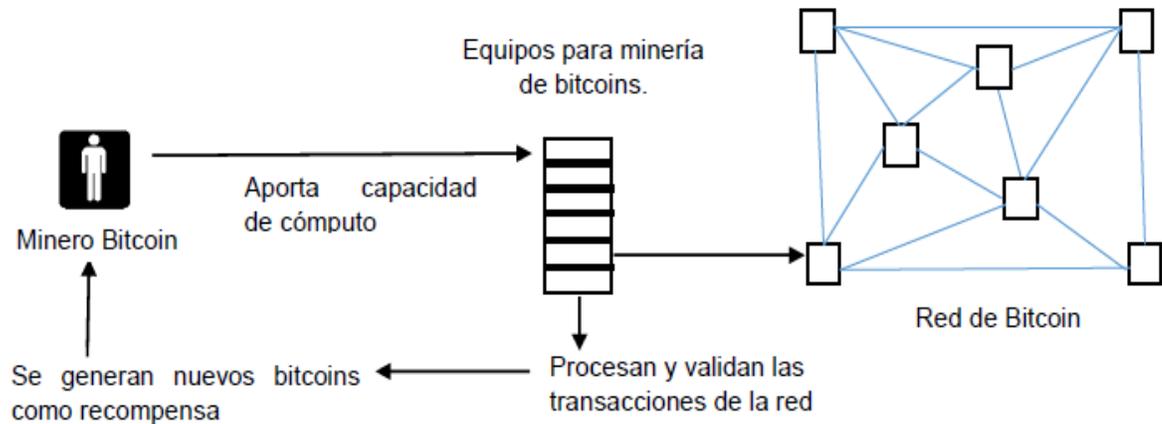


Fuente: (López, 2015).

Adicionalmente, los bitcoin son generados por personas llamados mineros, que ejecutan en sus máquinas software para resolver complejos cálculos matemáticos basados en criptografía con el fin de procesar y validar las transacciones. A medida que estos cálculos van siendo resueltos, se da lugar a la creación de un nuevo bloque de bitcoins, lo que es comunicado y registrado inmediatamente en toda la red. Está programado que el número de bitcoins por bloque disminuya hasta llegar a cero, puesto que el número total de bitcoins nunca podrá ser mayor a 21 millones algo que se calcula sucederá en el año 2140. Cabe anotar que, gracias a que es posible conocer cuántos bitcoins están actualmente en circulación y dado que su emisión está controlada por criterios matemáticos inmodificables que impiden una generación arbitraria de los mismos, el fenómeno de inflación está controlado. No obstante, un bitcoin puede ser dividido en unidades más pequeñas de hasta 8 dígitos

llamados satoshis en honor a su creador. Así las cosas, si en una transacción se transfieren 100 satoshis, eso significa que se ha transferido 0,00000100 bitcoins (López, 2015).

Gráfica 3. Proceso de minería de bitcoins.



Fuente: (López, 2015).

Todas las personas que desean utilizar bitcoins, necesitan una bitcoin wallet o billetera bitcoin, que es el medio que permite enviar y recibir bitcoins, inmediatamente se crea una billetera, también se crea una pareja de claves; una pública que corresponde a la dirección pública del usuario y como una cuenta bancaria es la que el usuario da, para que le realicen los pagos y consignaciones, y una clave privada generalmente asociada a un código de seguridad. Las billeteras se pueden crear accediendo a sitios de Internet que ofrecen éste servicio tales como blokchain.info donde crear una billetera y acceder a ella es tan fácil como crear una cuenta de correo electrónico. Una vez tiene acceso a la billetera, el usuario conocerá su dirección pública y podrá comenzar a hacer transacciones en bitcoins, los sitios de internet no requieren descargar ningún programa en el ordenador y algunos de ellos, poseen aplicaciones para iPhone y Android, que permiten realizar transacciones desde el dispositivo móvil con solo escanear un código QR que aparece al lado de la dirección pública como se muestra en la gráfica 4.

Gráfica 4. Código QR y dirección pública.



Fuente. (López, 2015).

A continuación, La gráfica 5, contiene un ejemplo completo de uso de una billetera bitcoin; incluyendo la dirección pública, la clave privada y el registro en la cadena Blockchain de una transacción entre Juan y María.

Gráfica5. Ejemplo de uso de una billetera bitcoin, dirección pública, clave privada y registro en el Blockchain.

<p>Juan tiene una billetera bitcoin.</p> <p>La dirección publica de Juan es: 1P99KRKcw...</p>	<p>Maria tiene una billetera bitcoin.</p> <p>La dirección publica de Maria es: 1ABYb9BT7...</p>						
<p>Juan consulta su billetera, y le enseña su dirección pública a Maria para que Maria le transfiera 1 BTC:</p> <p>Hola María, mi dirección es: 1P99KRKcw... (Dirección que siempre aparece con su código QR)</p>							
<p>En su billetera, Maria busca la opcion enviar, y escanea con su celular el código QR que le pasó Juan, digita el monto y firma la transacción con su clave privada que esta sociada a un código de seguridad que solo ella conoce.</p> <p>Desde: 1ABYb9BT7... Dirección de Maria → 1 BTC Hacia: 1P99KRKcw... Dirección de Juan</p>							
<p>La red confirma la transacción y la transacción se registra en el blockchain. Ahora, 1 BTC aparece registrado a la dirección pública de Juan y Juan podrá gastarlo o transferirlo otra vez.</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <thead> <tr> <th>Origen</th> <th>Destino</th> <th>Monto</th> </tr> </thead> <tbody> <tr> <td>1ABYb9BT7...</td> <td>1P99KRKcw...</td> <td>1 BTC</td> </tr> </tbody> </table>		Origen	Destino	Monto	1ABYb9BT7...	1P99KRKcw...	1 BTC
Origen	Destino	Monto					
1ABYb9BT7...	1P99KRKcw...	1 BTC					

Fuente: (López, 2015).

Nótese, la facilidad de la operación. En éste caso, lo que sucedió es que en la cadena de bloques, se registró 1 bitcoin, previa autorización de María que firma con su clave privada, a la dirección pública que entrego Juan para que se le realice el pago; a su vez Juan, solo podrá disponer de los bitcoins que se registraron a su dirección pública mediante su clave privada. De tal manera, que si Juan llegara a perder su clave, ya no podría disponer de esos bitcoins. Es decir, el nuevo propietario del bitcoin es

Juan, cuya dirección se registró en el Blockchain y quien puede disponer de ellos pues es el único que conoce la clave privada.

3.1.2 modelo de software libre.

La expresión software libre hace referencia a cuatro tipos de libertad, de las que son titulares sus usuarios; la libertad para ejecutar el programa, la libertad para estudiar el funcionamiento del programa y adaptarlo a nuevas necesidades, lo que implica poder acceder al código fuente del programa, la libertad para distribuir copias gratuitas o cobrando por su distribución y la libertad para mejorar el programa y publicarlo en beneficio de la comunidad, lo que implica entregar el código fuente del programa (Stallman, 2004) . Lo anterior significa que, Bitcoin es un código abierto; su diseño es público, nadie es dueño o controla Bitcoin y todo el mundo puede participar. Por medio de sus muchas propiedades únicas, Bitcoin permite usos interesantes no contemplados por ningún sistema de pagos anterior (Bitcoin.Org, 2017).

A diferencia de lo que podría ocurrir con las decisiones de las autoridades monetarias de algunos países, el funcionamiento del bitcoin es totalmente transparente y puede ser adaptado y mejorado a nuevas circunstancias, lo que ha permitido la creación de múltiples compañías que ofrecen mejores opciones de seguridad y servicios dentro del ecosistema bitcoin (López, 2015).

3.1.3 criptomoneda.

Al bitcoin también se le conoce como criptomoneda, debido a que el software creado por Satoshi Nakamoto utiliza la encriptación para controlar la creación o transferencia de los bitcoins, lo que le da un valor agregado en seguridad. Como se dijo anteriormente, los mineros ejecutan en sus máquinas un software encargado de resolver complejos cálculos matemáticos basados en criptografía para procesar y validar las transacciones. A medida que estos cálculos van siendo resueltos, se da lugar a la creación de un nuevo bloque de bitcoins, resultado que es registrado y comunicado inmediatamente en toda la red. Actualmente, se utiliza un hardware especializado conocido como ASIC. Además, los mineros se han unido en lo que se conoce como pools (piscinas), para minar bitcoins en grupo y repartirse las utilidades (López, 2015).

3.1.4 mining.

Dicho en otras palabras, el mining o minería de bitcoins es el proceso mediante el cual se procesan y validan las transacciones en la red, y como recompensa por este servicio y acorde con las reglas

establecidas en el protocolo bitcoins, se generan nuevos bitcoins que serán distribuidos entre los mineros.

3.1.5 anonimato.

Las transferencias de bitcoins se hacen de una dirección pública a otra de manera potencialmente anónima, dado que los saldos están ligados a estas direcciones y no a los usuarios y únicamente pueden realizarlas quien tenga acceso a la clave privada; en virtud de que la base de datos es descentralizada, el sistema debe identificar y ordenar secuencialmente todas las transacciones en la red. Esta base de datos es la denominada Blockchain o cadena de bloques y funciona como una especie de registro contable descentralizado y público que lleva un historial de la propiedad de todas las monedas desde la dirección creadora, hasta la dirección del último dueño, lo que hace imposible que sean gastados más de una vez por la misma persona. De hecho, una vez realizada la transacción, los nodos de la red verifican la cantidad de bitcoins involucrados y la autenticidad de las firmas criptográficas con base en la clave privada y emiten una serie de confirmaciones que la hacen prácticamente irreversible (López, 2015).

3.1.6 seguridad.

Lo anterior, hace imposible la falsificación y además permite, que cualquier transacción, que se hace con la misma facilidad con la que se envía un correo electrónico, pueda ser monitoreada en tiempo real, que se acceda a la cadena de bloques para obtener información acerca del historial de determinada transacción y hasta conocer cuántos bitcoins están vinculados a una dirección determinada. No obstante, en febrero de 2014 Mt. Gox, una firma japonesa y uno de los mayores operadores de transacciones en Bitcoins, se declaró en quiebra después de informar que hackers les habían robado el control de 850.000 Bitcoins de su sitio web, algo así como 480 millones de dólares y que representaban casi el 7% de todos los bitcoins en circulación en el mundo (Méndez, 2014). Como reacción a éste acontecimiento, una declaración conjunta de la comunidad Bitcoin, firmada por los directores ejecutivos de las compañías más representativas dentro del ecosistema Bitcoin, se dijo que esta trágica violación de la confianza de los usuarios de Mt. Gox, fue el resultado de las acciones de la compañía y no refleja la resistencia y valor del bitcoin y la industria de la moneda digital. Según Gavi Andresen, científico jefe de la fundación Bitcoin, los problemas que Mt Gox ha experimentado se deben a una desafortunada interacción entre su software de cartera altamente personalizado, su procedimiento de atención al cliente y su falta de preparación para la maleabilidad de las

transacciones, un detalle técnico que permite cambiar la forma en que las transacciones son identificadas.

Según Andresen, la maleabilidad de las transacciones ha sido conocida desde 2011 y en términos sencillos, es una pequeña ventana donde el identificador de la transacción puede ser renombrado, antes de ser confirmado en el Blockchain; dicho en otras palabras, es la posibilidad de renombrar el identificador de una transacción en el espacio de tiempo en que una ventana se abre para confirmar la transacción y lo que tarda en cerrarse al ser confirmada en el Blockchain. Lo sucedido, es un recordatorio de que Bitcoin es aún joven y experimental, algo que es entendible, en razón de que esta nueva invención explora ideas que jamás habían sido exploradas con anterioridad. Aunque no exenta de polémica, esta idea de pagos descentralizados entre usuarios, eliminando la presencia de instituciones financieras ha demostrado en la práctica que es funcional y válida para la realización de transacciones y su adopción está creciendo en todo el mundo (Díaz, 2015). Con solo digitar en howtobuybitcoin.info, se obtiene una lista de los bitcoins exchanges disponibles en cada país.

3.1.7 disponibilidad.

Si bien la billetera está alojada en el sitio web, algunos de ellos ofrecen la posibilidad de hacer una copia de seguridad de este archivo digital, también es posible crear billeteras offline o sin conexión a internet con solo ejecutar un programa en el ordenador personal, tal como Electrum, Bitcoin Core- también conocido como el cliente Bitcoin- o Armory; aunque éstos últimos sólo se recomiendan para usuarios avanzados; o mediante aplicaciones para dispositivos móviles como Mycelium o Bitcoin Wallet; o crearlas en un dispositivo de hardware especialmente diseñado para funcionar como billetera como: Trezor, el cual ofrece prácticas y eficientes funciones de seguridad; también existe la Paper Wallet o billetera de papel. Por éste método, accediendo a una página como Bitaddress.org, que también puede ejecutarse offline o sin conexión a internet, se imprime en medio físico por una parte la dirección pública y su correspondiente código QR, y por otra, la clave privada, acompañada también de un código QR y puesto que la clave privada está impresa en papel, esta puede ser guardada en una caja de seguridad de un banco. En la siguiente tabla podrá encontrar el listado de billeteras Bitcoin ordenados de acuerdo a su disponibilidad.

Tabla 1. Lista de Billeteras Bitcoin de acuerdo a su disponibilidad.

	Billeteras para Movil			Billeteras de Escritorio			Billeteras de Hardware	Billeteras en la Web
	Android	iOS	Blackberry	Windows	Mac	Linux		
Bitcoin Wallet	Si		Si					
KnC Wallet	Si							
Mycellium	Si	Si						
Breadwallet		Si						
Green Address	Si	Si		Si	Si			Si
Hive	Si	Si			Si			Si
Bitcoin Core				Si	Si	Si		
Electrum				Si	Si	Si		
mSIGNA				Si	Si	Si		
Multibit				Si	Si	Si		
Armory				Si	Si	Si		
Trezor							Si	
HW.1							Si	
Coinbase	Si	Si						Si
Coinapult								
Xapo	Si	Si						Si
BitGo								Si
Coinkite								Si
Blockchain.info	Si	Si						Si

Fuente (López, 2015).

En 2013 se instaló el primer cajero bitcoins a la entrada de un café en Vancouver (Canadá) y posteriormente se implementarían en E.U, Israel, España, Reino Unido y Emiratos Árabes Unidos; algunos de estos cajeros son bidireccionales y pueden cambiar moneda local en bitcoins y bitcoins en moneda local; otros, inclusive permiten comprarlos con tarjeta de crédito (BBC Mundo, 2013). A medida que el bitcoin se ha popularizado, se ha usado para pagar todo tipo de productos y servicios tal como se haría con los pesos o los dólares (Méndez, 2014). Según lo señalan varios medios de comunicación, esta moneda se puede usar para comprar una cerveza en Berlín, pedir una pizza en Ámsterdam y tomar un taxi en Edimburgo, hacerse un chequeo dental en Liubliana, estudiar en Nicosia o comprar medias de alpaca en Massachusetts o hasta ir al espacio con Virgin Galactic, inclusive empleados canadienses han comenzado a cobrar parte o la totalidad de sus salarios en bitcoins (Hayward, 2014) . En la Tabla No podrá encontrar un listado de las principales empresas que usan bitcoins en sus pagos y donaciones.

Tabla 2. Lista de algunas de las empresas que usan bitcoins.

Microsoft	Virgin Galactic	Google
Dell	Newegg	Bing
Expedia	Reeds jewelers	Time Inc.
Dish	Paypal	Greenpeace
Overstock.com	Mozilla	Cruz roja Americana

Fuente (López, 2015).

Desde diciembre de 2014, Microsoft permite el uso del bitcoin para la compra de música, videos, aplicaciones y juegos para su consola Xbox 360 o para sus sistemas operativos Windows o Windows Phone. De la misma manera, en marzo de 2014, los gemelos Winklevoss, famosos por demandar a Mark Zuckerberg por haberles robado la idea de crear la red social Facebook, se sumaron a la lista de personas que utilizando bitcoins, compraron billetes para un viaje espacial comercial con la empresa Virgin Galactic, propiedad del multimillonario Richard Branson (Reuters, 2014). También en julio de 2014 la compañía Dell, la tercera mayor fabricante de equipos informáticos, anunció la posibilidad de realizar compras en su portal utilizando bitcoins. El sitio de viajes más grande de Internet: Expedia, en junio de 2014 comenzó a recibir bitcoins para reservas de hotel y no descarta la posibilidad de incorporarlo a sus otras líneas de servicios.

Sitios como overstock.com, un minorista en línea que ofrece una amplia gama de bienes y servicios, alrededor de un millón de productos en el sitio, permite pagar con bitcoins cuando se realiza un pedido internacional, algo que fácilmente podría hacerse desde Colombia. También existen portales como BitcoinShop.us, donde únicamente se puede pagar usando moneda digital y otros como BitDazzle y CryptoThrift, donde se puede pagar con ellas, esto sin mencionar que Paypal, el sistema utilizado para realizar transacciones en línea también ha permitido el uso de bitcoins en su plataforma de pagos. Recientemente, las Naciones Unidas apoyan un proyecto para promocionar la identificación personal legal de más de 1100 millones de personas en todo el mundo a través de una red digital de identificación, utilizando la tecnología Blockchain. A propósito de esto, Diego Espítia, embajador de seguridad de Eleven Paths Telefónica Cyber Security Unit explicó en entrevista para NTN24 el objetivo de ésta propuesta, como el desarrollo de la tecnología existente que es el Blockchain el cuál brinda un soporte de trazabilidad tan confiable que permite a través de tecnología biométrica garantizar la identificación legal sin papeles; más que un pasaporte es como una hoja de vida digital

global de fácil acceso que permitiría solucionar la problemática de los refugiados e inmigrantes en todo el mundo para validar su identidad.

Adicionalmente, Espitia aclara que el principal reto es que la gente confíe en esta plataforma y que para eso está el Blockchain, para generar ese grado de confianza; pero que eso no va a ser tan fácil de entender para las personas del común debido a que es una base de datos con información sensible de muchísimas personas. Pero, que brinda la seguridad por ser una base de datos distribuida en la cual se puede escribir pero no borrar y generar registros que debes ser validados matemáticamente y de manera casi inalterable o demasiado costoso para poder generar un ataque de esas magnitud. Ahora, no todo con Blockchain es mágico, pero ésta es una aplicación que ubica la investigación en terrenos de futurología; ésta es una tecnología que al igual que el comercio electrónico al comienzo le va a parecer a las personas algo un poco soñador pero que va a ser la forma en que se maneje todo, Blockchain permite dar esa capacidad de seguridad y un soporte que va a permitir muchísimo manejo y gestión de la información.

4. Conclusiones.

El dinero no es eterno. Apareció en un periodo determinado de la historia, cuando su intermediación fue necesaria para el desarrollo de la sociedad, y de la misma manera desaparecerá cuando esta necesidad haya perdido su valor histórico (Robert, 2006). Actualmente, los adelantos tecnológicos permiten plantearse nuevas alternativas de negociación a nivel global y con altos niveles de seguridad; es el bitcoin un fenómeno tecnológico, económico y social de aplicabilidad y cambios profundos, que se presenta como consecuencia de las nuevas tecnologías. Esto, puede generar fuertes resistencias como es normal por parte de los históricos protagonistas de la escena económica mundial y su modelo. Pese a esto, es claro que la tecnología que fundamenta la aplicabilidad y el seguimiento a esta moneda virtual como es el Blockchain, ya está cobrando un papel protagónico en los nuevos modelos de manejo de la información y cuenta con el respaldo de organizaciones mundiales como la ONU y una gran comunidad que lo cataloga como el modelo económico que dominará el futuro del mundo.

Ataques cibernéticos como los presentados durante el mes de mayo en los cuales secuestran la información de empresas y organizaciones en todo el mundo para después pedir rescate por esta en Bitcoins llama mucho la atención teniendo en cuenta que se desconoce el origen de los mismos. Pero, lo que si dejan muy claro es que fenómenos económicos de consecuencias trascendentales alrededor del Bitcoin se tejen en todo el mundo.

Referencias.

- Barrera, J. (2011). *Importancia de la necesidad de la coerción mutua en la globalización o la descivilización progresiva*. Pensamiento crítico.
- BBC Mundo. (2013). Instalan el primer cajero de bitcoins en el mundo. *Instalan el primer cajero de bitcoins en el mundo*. Vancouver : Mundo Noticias.
- Bitcoin.Org. (2017). *Blockchain.info*. Obtenido de Blockchain.info:
<https://blockchain.info/es/charts/market-price>
- CoinDesk. (2017). *CoinDesk*,. Obtenido de CoinDesk,.
- Díaz, J. (2015). *Bitcoin. Una Moneda Criptográfica*. España: Instituto Nacional de Siberseguridad.
- Ferguson, C. (Dirección). (2010). *Inside Job* [Película].
- Gutiérrez, P. (2015). El Bitcoin, ¿Presente y futuro del dinero? Sus características e implicaciones. *El Bitcoin, ¿Presente y futuro del dinero? Sus características e implicaciones*. Madrid., Madrid, España: Universidad Pontificia ICAI.
- Harris, L. (1985). *Teoría Monetaria*. México: Fondo de cultura económica.
- Hayward, J. (2014). Salaries paid in bitcoin a growing trend in Canada. *Salaries paid in bitcoin a growing trend in Canada*. Canada: CBC News.
- Hernández, M. (2017). El valor del bitcoin supera por primera vez a la onza de oro. *El Mundo*.
- López, A. (2015). *Implicaciones jurídicas del uso del bitcoin en Colombia. Validez del contrato de compraventa comercial con bitcoins*. Pasto: Universidad de Nariño.
- Méndez, J. (2014). *Para todo lo demás está bitcoin*. Enter.co.
- Mishkin, F. (2008). *Moneda Banca y Mercados Financieros. 8. Ed* . México: Pearson Educación.
- Olier, E. (2012). *Geoconomía Las claves de la economía global*. Madrid : Paerson.
- Reina, M., & Zuluaga, S. y. (2006). *El Dinero y la Política Monetaria*. Bogotá: Reina, M; Zuluaga, S. y Rozo, M. (2006).Departamento de Comunicación Institucional Banco de la República.
- Reuters. (2014). Los gemelos Winklevoss se irán al espacio con un viaje pagado con bitcoins. . *Los gemelos Winklevoss se irán al espacio con un viaje pagado con bitcoins*. . Reuters.
- Robert, J. (2006). *Historia del Dinero*. Bogota: Ediciones Universales.

Rosales, G. (2005). *Geopolítica y Geoestrategia Liderazgo y Poder*. Bogotá: Universidad Militar Nueva Granada.

Serrano, J. (2008). Crisis Financiera de 2008: La visión un año despues. *Revista Soluciones de Posgrado*.

Stallman, R. (2004). *Software libre para una sociedad libe*. Madrid: Traficantes de sueños.

Uribe, J. (2013). La Independencia de la Banca Central en Colombia. *La Independencia de la Banca Central en Colombia*. Bogotá, Colombia: Banco de la República.