CENTRO DE ESTUDIOS INTERNACIONALES
GILBERTO BOSQUES
ANÁLISIS E INVESTIGACIÓN

LOS DEBATES DEL BITCOIN: EL PAPEL DE LAS CRIPTOMONEDAS EN UN CAMBIANTE MUNDO FINANCIERO (1)

31 DE ENERO DE 2018

NOTA INFORMATIVA

Imagen: Quartz.

El acelerado crecimiento del Bitcoin en 2017, causó que la moneda virtual pasara de ser una herramienta poco conocida y utilizada a generar un debate altamente polarizado que se plasmó en muchos encabezados de prensa internacional a finales de año. No obstante los miles de artículos escritos a favor o en contra de la misma, muchos aún siguen sin entender realmente lo que representa Bitcoin, cómo funciona la tecnología de blockchain, para qué sirven las criptomonedas y cómo es que se estima su valor. De igual manera, el debate sobre la permanencia de dichas tecnologías y su idoneidad han despertado una batalla entre los servicios financieros tradicionales y los innovadores tecnológicos en un contexto donde pocas personas entienden sus implicaciones reales y cómo podrían cambiar radicalmente el mundo financiero. La presente Nota de Coyuntura, es una introducción a los temas antes mencionados que será seguida por un análisis, a publicarse en seguimiento a ésta, sobre distintos esfuerzos de regulación de estos nuevos activos financieros alrededor del mundo.

Bitcoin debates: the role of cryptocurrencies in a changing financial landscape (1)

Bitcoin's rapid ascent in 2017 led the virtual coin to go from a relatively unknown technology used by few to a hotly contested advancement that took over headlines all over the world. Regardless of the thousands of articles written in support of or against it, many remain in the dark as regards to what Bitcoin actually represents, how blockchain technology works, the use of cryptocurrencies as a whole and how their value is calculated. People representing traditional financial services and technological innovators have become entrenched in a fierce battle about the new technology's staying power as well as its effectiveness, and yet most people lack understanding of blockchain and cryptocurrencies' real implications and how they could radically alter financial systems. This report is an introduction to the aforementioned themes, and it will be followed by an analysis to be published at a later date, about the different efforts around the world to regulate these new assets.

Introducción

En 2008, un autor bajo el pseudónimo de Satoshi Nakamoto publicó “Bitcoin: un sistema de efectivo electrónico de persona-a-persona” (*Bitcoin*[1]*: A Peer-to-Peer Electronic Cash System*) donde por primera vez se exploró la posibilidad de que se estableciera un sistema electrónico de pago que evitara toda institución de intermediación financiera. El objetivo de eliminar intermediarios lograría reducir el costo de las transacciones, así como hacerlas irreversibles. Asimismo, si el sistema es adoptado por completo, se eliminaría la inflación ya que ningún banco o Estado podría introducir más dinero al mercado y se eliminaría la necesidad de otorgar más información de la absolutamente necesaria para realizar transacciones.

Bajo el sistema de Nakamoto, cada usuario participaría en una red donde estaría localizada toda la información de todas las transacciones existentes. La red sería pública y no tendría control central: muchas computadoras tendrían fragmentos o totales del historial de las transacciones, pero para asegurar la veracidad de la información, ésta debería ser la misma en todas las máquinas. Esencialmente, las computadoras contribuirían para generar códigos encriptados complejos que validaran todos los intercambios entre usuarios y éstos se guardarían en una creciente cadena de bloques (*blockchain)*.

Al validar todas las transacciones en un espacio único, será evidente qué capacidad financiera tiene realmente cada usuario/a por lo cual, hipotéticamente, no sería necesaria la existencia de terceros a fin de validar dicha información. En el sistema de Nakamoto, la moneda a intercambiar es la denominada genéricamente como *bitcoin*, moneda que sería introducida al mundo mediante la validación de bloques de transacciones. Este sistema imitaría la manera en la cual se introdujo el oro a la circulación y valoración mundial: cada pedazo de oro que se minaba se introducía al mercado. Hoy, existen mineros de *bitcoin* que se dedican a “descubrir” nuevas monedas a través de complejos sistemas informáticos.

La siguiente Nota Informativa tiene como objeto explicar el funcionamiento del sistema detrás de *bitcoin*, la tecnología de *blockchain* y sus aplicaciones actuales.

[1] *Bitcoin* con mayúscula se refiere a todo el sistema, más *bitcoin* con minúscula indica únicamente la moneda. En esta Nota, se usa *bitcoin* dado que se habla por separado el sistema diseñado por Nakamoto.

Bitcoin y blockchain: el *White Paper* de Satoshi Nakamoto[2]

Satoshi Nakamoto identificó que los sistemas de pagos electrónicos contaban con varios fallos, quizás el más importante de éstos siendo la necesidad de mediación de terceros confiables como instituciones financieras y gobiernos. Nakamoto argumenta que, aunque el sistema funciona bien para la mayoría de las transacciones, el sistema de confianza cuenta con debilidades inherentes. El sistema de confianza se refiere a la certeza que debemos tener sobre los bancos y las instituciones regulatorias – los mediadores entre las personas y toda interacción financiera. Las fallas inherentes según Nakamoto son: 1) el costo de las transacciones, las cuales son más elevadas por el servicio de mediación que deben operar los bancos y otros actores financieros; 2) el primero "elimina la posibilidad de hacer transacciones casuales pequeñas"; y 3) asimismo se dificulta la posibilidad de que se ejerzan pagos completamente irreversibles para servicios igualmente irreversibles.

Dado que en el sistema financiero tradicional debe ser posible revertir ciertos cargos los usuarios debemos de confiar ampliamente en el sistema. Parte de participar en dicho sistema implica otorgarles a instituciones intermediaras más información de la absolutamente necesaria para realizar cualquier transacción. Además de estas consideraciones, el autor formula que el sistema tolera como inevitable cierto margen de fraude, o bien, de error.

Cabe destacar que desde la crisis financiera del 2007-2008, una falta de confianza en los sistemas de banca mundiales y el manejo del capital por parte de los gobiernos ha puesto bajo alerta a los sistemas convencionales. Un artículo de la revista estadounidense *The New Yorker* de 2013, subraya que durante la crisis de Chipre de ese mismo año, casi se duplicó el precio de un *bitcoin (*paso de 60 dólares -USD- a 103USD) y crecieron sus usuarios en Europa, lo cual puede interpretarse como indicio de una mayor confianza en la moneda electrónica (la cual era en ese momento aún más marginal y poco conocida), sobre los sistemas tradicionales.[3] Aunque sin duda esta confianza la reflejó únicamente un sector pequeño de la población, "el hecho de que un número de europeos asustados consideró que el pequeñísimo, volátil y vulnerable mercado del *bitcoin* era una alternativa preferible a su sistema bancario [...] ilustra el colapso mayor de confianza que está amenazando el mundo de la banca global".[4]

Un artículo de Nakamoto, posterior a la crisis, pero previa a su desaparición de foros y blogs públicos (2012), señala que "el problema con el dinero convencional es toda la confianza necesaria para su funcionamiento", especialmente cuando la historia está repleta de constantes violaciones de esta confianza de parte de las instituciones bancarias, financieras y gubernamentales. ¿Qué es en lo que confiamos al participar en los sistemas económicos establecidos? Primeramente, en que los bancos centrales no van a devaluar una moneda al deliberadamente imprimir más dinero; segundo, en que los bancos no usarán el dinero de sus usuarios para generar préstamos y, que de ser así, contaran con suficientes reservas para proteger a sus usuarios de cualquier impago

[2] A menos de especificarse lo contrario, esta sección está basada en información de: Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", *Bitcoin.org*, 2008. Consultado el 18 de enero de 2018 en: https://bitcoin.org/bitcoin.pdf
[3] Maria Bustillos, "The Bitcoin Boom", *The New Yorker,* 1 de abril de 2013. Consultado el 30 de enero de 2018 en: https://goo.gl/m8wnJP
[4] *Ídem*

resultado de sus propias decisiones; y finalmente, se debe confiar en que nuestra información confidencial está segura y nuestro dinero protegido.[5]

Durante la crisis financiera de 2007-2008 se comprobó que la confianza que tenían los usuarios en dichos sistemas podía ser gravemente violada, ya que en efecto los bancos centrales imprimieron más dinero cuando los bancos privados otorgaron préstamos excesivos sin contar con reservas adecuadas.[6] Asimismo cuando comenzaron a devaluarse las propiedades en Estados Unidos (en lo que estaban basados un enorme número de préstamos), se identificó una cadena de malos manejos a través de todo el sistema. Las compañías respaldadas por el mercado hipotecario se desplomaron en valor y muchas inversiones y muchas inversiones catalogadas como "altamente seguras" resultaron valer absolutamente nada, sin importar las garantías que les otorgaron distintas agencias supuestamente objetivas.
Fue entonces que comenzó a perderse cierta confianza en los sistemas convencionales ya que durante esta época quedó clara la manera en la cual toda la cadena financiera actual podría vulnerarse ante manipulaciones, errores y malos cálculos humanos. Asimismo, el hecho de que los gobiernos aceptaron "rescatar" a los bancos y por ende permitir la devaluación del efectivo, sirvió para muchos como más evidencia de la manera en la cual el sistema de confianza beneficia a las instituciones sobre el usuario promedio.[7] Finalmente, el tercer punto de confianza se vulnera dado que el mundo financiero opera considerando cierto margen de fraude: al proporcionar toda la información confidencial necesaria para operar una cuenta bancaria o hacer una transacción, los usuarios son vulnerables a robo de identidad y *hackeos* que pueden tener repercusiones mayores que la pérdida de efectivo. Además, la información que obtienen las compañías de tarjetas de crédito como *MasterCard* sobre nuestros patrones de gasto y compra es vendida en paquetes de *Big Data* (una enorme cantidad de datos) a comercios, bancos y gobiernos.[8]

Para evitar todo esto, la solución, según Nakamoto, es basar el sistema de pagos en evidencia criptográfica[9] más que en la confianza al sistema financiero, al permitir que dos partes generen una transacción directa entre ellas, sin la necesidad de un tercero confiable. Cabe señalar, en este punto, que para el autor una moneda electrónica es simplemente "una cadena de firmas digitales".[10] Bajo su sistema, las transferencias ocurren en cuanto las CPUs[11] son capaces de realizar exitosamente ciertas tareas computacionales (también conocidas como pruebas de trabajo) que validen la transacción y puedan entonces adscribir la cantidad a un nuevo usuario. Nakamoto aseguró que, bajo su modelo, existirían únicamente 21 millones de *bitcoins* lo cual ayudaría a determinar su valor -al no ser un recurso infinito- así como a asegurar la validez de las transacciones: en este sentido, no sería posible que estén en circulación más *bitcoins* de los que han sido descubiertos o "minados" y el total absoluto será de 21 millones.

[5] *Ídem*
[6] *The Economist*, "Crash course", 7 de septiembre de 2013. Consultado el 30 de enero de 2018 en: https://goo.gl/p9LRJU
[7] *Ídem*
[8] Emma Thomasson, "MasterCard expects big growth from 'big data' insights", *Reuters,* 11 de junio de 2014. Consultado el 31 de enero de 2018 en: https://goo.gl/CDT8e7
[9] Códigos matemáticos realizados por computadoras.
[10] Firma digital se refiere a un número único, asignado a cada usuario o transacción.
[11] CPU es un acrónimo de "central processing unit" o unidad central de procesamiento y es la parte de toda computadora que comprende los elementos necesarios para procesar datos

Vale la pena explicar el concepto de "prueba de trabajo" (POWs, por sus siglas en inglés): éste se refiere a un 'fragmento' de datos que es difícil de producir pero simple de verificar para las CPUs.[12] Nakamoto no inventó el proceso, más su manera de emplearlo es altamente innovadora.[13] Las POWs pueden entenderse como rompecabezas o retos que deben completar los CPUs de los mineros para que cualquier transacción sea aceptada y aunada a la cadena existente, y por ende continúe creciendo el *blockchain*..[14] Estos procesos son los que requieren de enorme poder computacional y gastan grandes cantidades de energía.[15] ¿Qué incentivaría a alguien a participar en este sistema considerando sus costos? Para los mineros, el incentivo es claro: ganar más *bitcoin*.

La primera transacción en un bloque es "especial" dado que, al crearse, genera *de facto* una nueva moneda, la cual será "pagada" al creador del bloque: el o la creador/a es la persona que logra "cerrarlo" para comenzar uno nuevo. A la fecha, la computadora que logre completar un bloque recibe 12.5 *bitcoins* como pago.[16] Considerando que "cerrar" los bloques requiere de la alineación de ciertos códigos con un *nonce*[17] específico – el proceso inicialmente era atractivo ya que técnicamente cualquier computadora podría resultar exitosa al crear la combinación correcta. Hoy en día, la probabilidad de que una CPU tradicional logre dicha combinación es extremadamente baja.

Una manera de considerar estos procesos es imaginar que cada minero está constantemente intentando adivinar las combinaciones de un candado: acertar tomará cientos o miles de intentos, mientras que verificar la validez de dicho trabajo tomaría mucho menos tiempo (comprobar que el candado abre).[18] No está por más mencionar que al "minar", o resolver estos problemas complejos, los involucrados no tienen forma de saber si están trabajando en validar la transacción que logrará cerrar el bloque. Por ende, entre más POWs generen por hora, incrementan sus posibilidades de que una de éstas logre alinearse con el *nonce* y les permita recibir los 12.5 *bitcoins* prometidos.[19]

De cualquier forma, este 'premio' constituyó un claro incentivo para participar en la red y fungió como una manera inicial de distribuir e introducir las monedas, dada la ausencia de una autoridad central que las emitiera. Según el sistema o protocolo electrónico que los sustenta, existirán 21 millones de *bitcoins*, de los cuales ya han sido "encontrados", o bien, "minados" a través de la solución adecuada de complejos problemas matemáticos casi 17 millones.[20]

Pero, entonces, ¿cómo saber si alguien está gastando doblemente su dinero, o si está generando nuevos *bitcoins* "de la nada"? Estas falsificaciones serían fatídicas para el sistema dado que la

[12] Para más información consúltese Adam Back, "Hascash FAQ", *Hascash.org,* s.f., consultado el 18 de enero de 2018 en: http://www.hashcash.org/faq/
[13] Una aplicación más conocida de este proceso es la que se utiliza para evitar la generación de correos spam: una CPU no tendrá problema generando la prueba de trabajo (tarea computacional) requerida para mandar un correo electrónico, más para quién desea mandar 10,000 correos por minuto, procesar las pruebas de trabajo necesarias sería imposible, dado que su sistema se vería saturado.
[14] Andrew Tar, "Proof-of-work, Explained", *Cointelegraph*, 17 de enero de 2018. Consultado el 31 de enero de 2018 en: https://goo.gl/Q3ZxxB
[15] Esta es una realidad hoy, más nuevos procesos podrían hacer más efectivo el consumo de energía.
[16] *Bitcoin Block Reward Halving Countdown,* 29 de enero de 2018, consultado el mismo día en: http://www.bitcoinblockhalf.com/#
[17] Un digito semi-aleatorio que únicamente se utiliza una vez y debe alinearse con la última prueba de trabajo de un bloque.
[18] 99Bitcoins, "What is Proof of Work/Proof of Stake", *Youtube*, publicado el 1 de agosto de 2015. Consultado el 31 de enero de 2018 en: https://goo.gl/xU8pXz
[19] A fecha de publicación, éstos equivalen a 124,687 dólares.
[20] Bitcoin Block Reward Halving Countdown, *op. cit.*

capacidad de “generar” las monedas arbitrariamente devaluaría por completo al *bitcoin*. He aquí donde tradicionalmente se necesitaría la participación de una autoridad central que verifique las interacciones, más la solución que ofrece Nakamoto para evitar dicha adición es tener una lista de todas las transacciones. Para lograr saber el orden de éstas (y evitar el doble gasto de una moneda electrónica) las transacciones deben ser anunciadas públicamente y se requiere un sistema de participación basado en una historia colectiva para determinar el orden de las transacciones. Esto evitaría el doble gasto sin necesidad de utilizar el modelo de la “confianza”.

Para esto, se generarán sellos de tiempo (*timestamps*) inmediata y electrónicamente los cuales permitirán, en principio, que se eliminen los fraudes dado que existirán siempre pruebas del orden cronológico de toda transacción. Estos sellos serán públicos, al igual que todas las transacciones e interacciones que existan bajo este sistema. El sello temporal sobre cada transacción comprueba que los datos debían haber existido al momento de emitirse y cada nuevo sello incluye todos los pasados, formando una cadena que algunos han equiparado a un gran libro contable. Aquí, se detiene el doble envío al tiempo que se verifica la existencia de la moneda y su transferencia. Asimismo, las pruebas de trabajo emitidas por las transacciones de *bitcoin* están ligadas a todos los sellos temporales creados, por lo cual no existe manera de cambiar las transacciones sin rehacer todo el trabajo lo cual requeriría una enorme cantidad de energía por parte de las CPUs.

Nakamoto expone el funcionamiento de la red de *blockchain* y la manera en la cual esté debiera administrarse:

1. Las nuevas transacciones serán publicadas para todos.
2. Cada nodo[21] aunará las transacciones nuevas a un bloque.
3. Cada computadora trabajará para encontrar pruebas de trabajo complejas para su bloque.
4. Cuando una encuentre una prueba de trabajo, lo comunicará a todas las demás.
5. Las computadoras aceptarán el bloque solamente si todas las transacciones dentro de éste son válidas y no han sido gastadas (evitar doble gasto).
6. Las computadoras expresarán su aceptación del bloque al trabajar en la creación del siguiente bloque en la cadena, partiendo del *hash* del bloque aceptado.

Los nodos parten de la premisa que la cadena más larga es la correcta y continuarán trabajando en su extensión. Sin embargo, si dos computadoras publican versiones distintas del siguiente bloque simultáneamente puede ser que otras reciban una u otra versión primero. Bajo este escenario, los CPUs trabajarán basados en la cadena que han recibido, pero guardarán la segunda versión, en caso de que ésta resulte convertirse en la más larga. La publicación de las nuevas transacciones no necesita alcanzar necesariamente a todos los nodos. Con tal de que llegue a muchos, éstos continuarán la cadena. No se requiere que alguna computadora esté permanentemente activa en el sistema (esto sería equivalente a tener un nodo central o superior) ya que cuando éstas abandonen la red y reingresen, recibirán inmediatamente el último bloque existente. Este mismo evidenciará que faltan otros dentro de su cadena, los cuales también recibirán de otras computadoras.

[21] Las computadoras que tengan guardada en parte o en su totalidad el historial de las cadenas.

Una vez confirmadas las operaciones y gastadas las monedas, las cadenas de bloque que contienen esas transacciones "terminadas" pueden eliminarlas sin romper la cadena mediante una nueva etiquetación. Esto permite conservar el historial sin que se requiera tanta memoria computacional para conservarla toda.[22]

Pero, bajo esa premisa, ¿qué pasaría si alguien tiene una computadora más poderosa y cambia el código de la cadena de *blockchain* para su beneficio? Considerando que las transacciones son públicas y a su vez son verificadas por varias CPUs inmediatamente se necesita que una mayoría sean "honestas" y no busquen pervertir la realidad de los datos para evitar que un ataque con el objetivo de cambiar la información para duplicar monedas o invalidar transacciones resulte exitoso. Dado que cada vez más personas se unen a las redes, es más difícil imaginar un escenario en el cual existan más máquinas "deshonestas" que honestas; asimismo, todas las CPUs deshonestas deberían de replicar el trabajo de las demás para lograr alterar las cadenas. Un incentivo importante para la honestidad de los "mineros" y los usuarios es que, al perderse la confianza en el sistema, sus propias ganancias se devalúan, o de evidenciarse una corrupción total del sistema éstas perderían todo valor.

Nakamoto escribe que la introducción de *bitcoins* al mercado es similar a la manera en la cual se introducía el oro por medio de los mineros: la diferencia es que en vez de la energía y recursos requeridos para minar oro, el *bitcoin* requiere energía y tiempo de las CPUs. Esta medida también ayuda a mantener a los "nodos" honestos, dado que, si algún atacante lograra conseguir más poder computacional que todos los demás participantes juntos, deberá escoger entre usar su energía para generar más *bitcoins* o para corromper el sistema al alterar la información de los bloques – lo cual pone en riesgo su propia fortuna al desestabilizar la validez del sistema. Naturalmente, argumenta Nakamoto, quién tuviera dichas capacidades preferiría invertir en generar más valor y seguir reglas que claramente le benefician.

De acuerdo con el modelo de Nakamoto, no es posible alterar fácilmente al sistema ni generar cambios arbitrarios dentro de éste: no es posible tampoco 'inventar' más monedas sin hacer el trabajo necesario ni puede un usuario acreditar dinero con el que nunca contó. Los nodos, o las computadoras con el historial de las cadenas, no aceptarán transacciones inválidas y los nodos que no sufran manipulación alguna no aceptarán cadenas que contengan transacciones inválidas.

Otra garantía del sistema de prueba de trabajo que por ende generan los intercambios de *bitcoin* es que entre más pruebas se estén generando por hora, se incrementa la dificultad computacional de las mismas. El mecanismo tiene como objetivo generar un nuevo *bitcoin* aproximadamente cada 10 minutos, por lo cual entre más participantes existan, serán más complejas las pruebas de trabajo. Este tipo de consideraciones serán importantes más adelante cuando se discuta el "costo real" del *bitcoin* en el mundo en términos del uso de energía.

Al anunciar todas las transacciones de manera pública, se pierde la privacidad que existe hoy en transacciones comunes donde únicamente los involucrados están al tanto de la operación. Aun así,

[22] En su documento del 2008, Nakamoto cita que las computadoras ya cuentan con 2 GB de memoria, pero que según la Ley de Moore en cuanto al crecimiento tecnológico, este crecería exponencialmente. Como punto de referencia, la memoria de los iPhones pasó de 256 megabytes (MB) en 2009 a 2 gigabytes (GB) en 2017. Dos GB son aproximadamente 2,000 MB, por lo cual la capacidad de memoria aumentó un 900% en menos de 10 años.

la privacidad puede ser retenida al asegurar la anonimidad de las partes involucradas en la transacción: Nakamoto indica que dicho modelo es similar al que se utiliza en la bolsa, donde se sabe la hora y cantidad de los intercambios, pero se desconoce entre quiénes ocurrieron.

Bitcoin: del código al dólar

Como se mencionó previamente, existen actualmente casi 17 millones de *bitcoins* en el mercado (los otros 4 millones restantes aún no se han minado), pero queda claro para pocos la manera en la cual se intercambian, la forma en la que se utilizan y cómo se les adscribe valor. Aunque sin duda uno de los temas más importantes de estos nuevos sistemas es que actualmente existen casi en su totalidad sin regulación, esto está cambiando recientemente. Varios países alrededor del mundo han comenzado a regular la circulación y el intercambio de estas monedas a fin de impedir abusos especulativos. Sin embargo, este tema, así como el del riesgo de asociación con conductas criminales o el posible mal uso de los sistemas financieros inmediatos serán explorados en una segunda parte de ésta nota.

El precio del *bitcoin* se calcula con base en los principios básicos de la economía de oferta y demanda.[23] Considerando que existen solamente un límite de monedas circulando actualmente y que nuevas monedas se insertan al mercado a un nivel predecible y desacelerado, su precio se incrementa al volverse más complejo (en procesos computacionales, así como en disponibilidad) adquirir una. Ya que actualmente es un "mercado relativamente pequeño comparado a su potencial" no toma enormes cantidades de dinero hacer que existan fluctuaciones importantes en sus precios. Las enormes altas y bajas a la moneda en los últimos años han respondido a un sinnúmero de factores, más tienen que ver en gran medida con inversiones que indican el nivel de confianza que tiene el mercado sobre la moneda, su valor (no precio, pero importancia o utilidad) y su durabilidad. Cuando la confianza baja, muchos venden sus monedas a un precio menor al cual las adquirieron, lo cual causa una devaluación, que posteriormente puede revertirse cuando, por ejemplo, muchos más usuarios se unan al sistema o alguna institución financiera reconocida valide los intercambios.[24]

Según los partidarios del *bitcoin*, éste tiene valor porque es una moneda como otras, (cuenta con las características básicas de durabilidad, portabilidad, funcionalidad, escasez, divisibilidad y reconocimiento), pero está basada en las propiedades de las matemáticas más que en propiedades físicas (como el oro o la plata) o en la confianza en autoridades financieras centrales.[25] Su valor se crea al ser adoptado, por lo cual éste incrementa al tiempo que crecen sus usuarios, vendedores y negocios. Como toda otra moneda, su valor se deriva directamente del hecho de que la gente lo acepta como pago. En la actualidad, el *bitcoin* opera como moneda, activo financiero y red social al mismo tiempo, de ahí su enorme complejidad. Opera como activo porque su valor crece al crecer su ecosistema, y como red social porque entre más usuarios tenga es más útil.

[23] *Bitcoin.org, "*FAQ", s.f., consultado el 24 de enero de 2018 en: https://bitcoin.org/en/faq#why-do-bitcoins-have-value
[24] Samantha Bonkamp, "CBOE will be first to trade on bitcoin futures"; *The Chicago Tribune*, 4 de diciembre de 2017. Consultado el 30 de enero de 2018 en: https://goo.gl/PJjMQ8
[25] *Ídem*

Las criptomonedas se guardan en "carteras" cibernéticas que, en vez de tener la moneda en sí misma, tienen acceso a la llave privada[26] que a su vez permite acceso a la dirección pública (llave pública[27]) de cada usuario. Realmente, las carteras son simplemente códigos que dificultan el acceso a la información deseada. Algo comparable sería pensar en tener nuestro NIP guardado en un correo electrónico, y que dicho correo sea privado y únicamente accesible mediante la introducción de una contraseña y que a su vez, dicha información esté en una computadora que, a su vez, requiere claves de acceso.

Dado que las carteras son solamente códigos, se pueden guardar de distintas maneras: en aplicaciones celulares, en internet (o en la denominada “nube”), en dispositivos USB o se pueden simplemente tener escritos en un papel.[28] El atractivo de las primeras dos opciones es su conveniencia, mientras que sus riesgos son los *hackeos* - en especial la segunda opción es vulnerable a estos robos ya que los códigos están bajo el control de terceros. Finalmente, las segundas dos opciones ofrecen más seguridad ya que al no estar conectadas al internet, deben de ser físicamente ultrajadas y en caso del USB este requiere aún más códigos de acceso. Al igual que en la analogía del NIP bancario y la computadora, en cuanto se tiene información en internet es más fácil sustraerla.

Hoy en día se sigue generando un *bitcoin* cada 10 minutos, más también existe ya un mercado creciente, actualmente valuado en 169 mil millones de dólares.[29] Existen varias plataformas para el intercambio (compra-venta) de criptomonedas, y éstos pueden ser intercambios de persona a persona o por alguna otra moneda, ya sea virtual o física. Es posible, por ejemplo, vender 50% de un *bitcoin* para comprar pesos mexicanos (de la misma manera que opera la compra-venta de monedas extranjeras) y usar el otro 50% para comprar alguna otra moneda virtual. Estas operaciones se realizan a través de transacciones bancarias, dado que el dinero en la cartera virtual debe de ser transferido a una cuenta tradicional para poder usarse.[30]

Asimismo, existen cajeros automáticos de *bitcoins* en 62 países alrededor del mundo, pero únicamente Estados Unidos, Canadá y el Reino Unido cuentan con más de cien unidades.[31] México está entre los 20 países con más cajeros automáticos ya que cuenta con 12 según páginas dedicadas al mapeo de los cajeros.[32] Cabe resaltar que, dado que la moneda se puede vender en fracciones tan pequeñas como 0.000 000 01, el límite de *bitcoins* no tendría que afectar necesariamente su capacidad circulatoria.[33]

[26] Código único de cada usuario para accesar a su capital. Podríamos compararlo con un NIP en la actualidad.
[27] Éste es el código con el cual se identifican a las personas en la red públicamente. Podríamos considerarlo hasta cierto punto como el código CLABE: no revela información personal pero sí liga a una persona con una serie de transacciones previas.
[28] *Coindesk*, "How to store your Bitcoin", 20 de enero de 2018. Consultado el 22 de enero de 2018 en: https://goo.gl/D4SsTH
[29] *Bitcoin Block Reward Halving Countdown, op. cit.*
[30] Es en este paso en el cual es posible que los gobiernos o bancos interfieran en las transacciones.
[31] *Coin ATM Radar, “*Bitcoin ATMs by Country”, s.f., consultado el 30 de enero de 2018 en: https://coinatmradar.com/countries/
[32] *Ídem*
[33] *Coindesk*, "How to sell Bitcoin", 20 de enero de 2018. Consultado el 23 de enero de 2018 en: https://goo.gl/LZDoLg

El *blockchain*: inicios de un cambio revolucionario

La revista *Harvard Business Review* publicó un artículo escrito por los profesores de negocios Marco Iansiti y Karim R. Lakhani, que señalaba que "los contratos, las transacciones y los récords de los mismos son estructuras definitivas de nuestros sistemas legales, económicos y políticos […] y aun así estas herramientas críticas y las burocracias formadas para su manejo no han logrado mantenerse al tanto de la transformación de la economía digital. […] En un mundo digital, la manera en la cual se regula y se mantiene el control administrativo debe cambiar".[34]

El documento señala que el potencial del sistema de bloques en cadena es inmenso ya que este es una respuesta a la imperativa de la evolución del sistema financiero hacia el mundo digital. El sistema permite concebir la idea de un mundo dentro del cual los contratos sean parte de códigos digitales y existan en bases de datos compartidas y transparentes, lejos de manipulaciones o alteraciones. El hecho de que exista evidencia de todas y cada una de las transacciones y los procesos (y que estos deban ser identificados, validados, aceptados y compartidos) implica que podrían desaparecer las necesidades de emplear a abogados, banqueros y otros intermediarios ya que las transacciones existirían en una bitácora común accesible para todos.

Aun así, existen riesgos reales como los colapsos de ciertos sistemas además de los *hackeos*. El documento asegura que una adaptación 'total' del sistema aún está a muchos años de distancia, dado que la tecnología no es "disruptiva" sino "fundacional".[35] Esto implica que es un nuevo comienzo, capaz de establecer nuevas bases para los sistemas económicos y sociales bajo los cuales operamos. Dada la magnitud de los alcances, "serán décadas" antes de que la tecnología permeé realmente nuestra infraestructura social y económica. Los autores aseguran esto basándose en el desarrollo del internet desde sus inicios en 1972 (cuando era conocido como TCP/IP) hasta su forma actual. No fue sino hasta la década de los años noventa del siglo pasado que la infraestructura cibernética y su disponibilidad alcanzaron capacidades suficientes para la substitución de mercados y sistemas existentes. En esta década, fue cuando comercios electrónicos como *Amazon* (venta bienes) o *Expedia* (venta de viajes/experiencias) comenzaron a reemplazar a negocios tradicionales. La siguiente generación de corporaciones fueron las que realmente desarrollaron aplicaciones transformadoras (*Google, Skype*, etc.).

Aunque *bitcoin* es la primera aplicación de la tecnología de bloques de cadenas, no será la última ni la única. Al igual que el correo electrónico permitió la creación de mensajería virtual de usuario a usuario, el *bitcoin* contribuiría a sentar las bases para permitir las transacciones financieras de usuario a usuario. Al igual que el TCP/IP creó la posibilidad de explotar nuevas capacidades económicas al reducir dramáticamente el costo de la conectividad, el nuevo sistema de *blockchain* promete reducir el costo de las transacciones. En particular destaca que tiene "el potencial de convertirse en el sistema que guarda todas las transacciones" – lo cual significaría un cambio radical a la economía mundial.[36]

[34] Marco Iansiti, Karim R. Lakhani, "The Truth about Blockchain", *Harvard Business Review*, enero-febrero 2017, consultado el 20 de enero de 2018 en: https://hbr.org/2017/01/the-truth-about-blockchain
[35] *ídem*
[36] *Ídem*

Hoy en día, todos los negocios tienen un récord de sus transacciones, así como métricas de su desempeño y planes basados en su historial. No obstante, éstos no están centralizados y a menudo están dispersos entre distintas áreas internas del negocio, además de conformar información privada. Esto implica que, aunque muchas transacciones pueden ejecutarse en pocos segundos, la transferencia real de bienes puede tardarse horas o días – consideremos tan solo una transacción bancaria entre bancos distintos o transacciones a otros países. Por un lado, este retraso tiene que ver con que las partes involucradas no tienen acceso a sus respectivas bitácoras y no pueden inmediatamente verificar que los bienes existen y son transferibles. He aquí donde se requiere la intervención de terceros y se emplea el modelo de confianza: las instituciones financieras sirven, desde luego, como garantes.

Según Iansiti y Lakhani, la primera fase de la introducción del *blockchain* al mercado masivo será como método de pago.[37] Este primer paso es "fácil" dado que ya existe la infraestructura para hacerlo y las compañías simplemente tienen que decidir aceptar dicha moneda como válida.[38] Esto impulsaría el avance de la tecnología del *blockchain* al tener necesariamente que desarrollarse capacidades para éste en muchas industrias: financiera, contabilidad, ventas y marketing, por mencionar algunas. Asimismo, el sistema podrá ser adaptado para el manejo de datos internos o para la localización de información: hoy en día ya se utiliza la tecnología para rastrear el movimiento de piedras preciosas desde la mina hasta el consumidor. Evidentemente, sus implicaciones son muchas y van más allá del ámbito exclusivo del *bitcoin*.

Según los autores, dos áreas en donde la aplicación de la tecnología podría tener un efecto duradero e importante es en los sistemas de identificación pública (aduanas) y en el uso de decisiones basadas en algoritmos para prevenir el lavado del dinero en transacciones financieras complejas y entre muchas partes.[39] Este tipo de avances serán los que abrirán el camino para la creación de "nuevos ecosistemas", de la misma manera que el primer correo electrónico enviado en 1971 sentó las bases para el mundo en el cual vivimos hoy – dominado por tecnologías y compañías que han logrado transformar la manera en la cual interactuamos con y dentro del internet. Los autores concluyen que "sin importar el contexto, hay una gran posibilidad de que el *blockchain* afecte tu negocio. La gran pregunta es cuándo".[40]

¿Tecnología o ideología?

Sterlin Lujan escribe en la página de noticias de *Bitcoin.com* (no afiliada con Satoshi Nakamoto) que la criptomoneda es un "catalizador para la anarquía pacífica y la libertad" y que se creó posterior a la caída de los mercados en 2007 específicamente para derrocar ese sistema. El autor asegura que la tecnología se promueve como inofensiva para apelar a las masas y a las élites poderosas, pero que sin embargo, su meta real es "acabar con las influencias corruptas y regresar el dinero a las manos de la gente".[41] Según el autor, en su documento de 2008 Nakamoto expresa claramente

[37] *Ídem*
[38] Aunque esto es fácil en términos de sistemas es mucho más complejo en términos de regulación y certidumbre legal, temas que se explorarán en la Parte II de esta serie.
[39] Marco Iansiti, Karim R. Lakhani
[40] *Ídem*
[41] Sterlin Lujan, "Bitcoin was built to incite peaceful anarchy", *Bitcoin.org*, 9 de enero de 2016. Consultado el 24 de enero de 2018 en: https://goo.gl/paZ9cD

un "sentimiento anarquista", por lo cual *bitcoin* no es simplemente una tecnología financiera pero en realidad, su creación obedece al deseo de destruir la centralización del dinero por gobiernos y bancos.

El autor cita que la inflación es otra consecuencia indeseable del control centralizado del dinero, lo cual puede evitarse mediante el uso de *bitcoin* ya que nadie puede interferir en la transacción entre dos usuarios ni puede generar más *bitcoin* para regular el precio del mismo. Sin duda, existe un gran número de artículos que celebran la creación de estos sistemas para dejar atrás los actuales, que muchos ven como corruptos y obsoletos. Esta motivación e interés son de particular atractivo para jóvenes (*millennials*) que hoy viven una enorme desventaja financiera comparada al mundo en el cual crecieron sus padres. La propagación de la información y la creciente transparencia del internet han evidenciado que muchos sistemas políticos y económicos operan de maneras insatisfactorias.

Por ende, según el Profesor Nigel Dodd, director del departamento de Sociología de la *London School of Economics*, el atractivo y, al mismo tiempo, el riesgo de estos avances es la ideología detrás de la tecnología y no las capacidades tecnológicas en sí.[42] Dodd asegura que la paradoja más importante del *bitcoin* es que su éxito ideológico conllevaría a su fracaso como moneda. Esto ocurriría dado que su premisa se basa en considerar al dinero un 'objeto' que debe abstraerse de la vida social para protegerlo de manipulaciones de intermediarios o autoridades. Aunque las criptomonedas se presentan como sistemas mecanizados que operan por encima de las prácticas sociales, en realidad la moneda cuenta con “una comunidad con ideales políticos que depende de un grado de organización social para producirse”, tiene una estructura social y está caracterizada por asimetrías de poder y riqueza típicas de los sistemas tradicionales. Sin embargo, hasta el momento, el *bitcoin* ha tenido un éxito razonable como moneda o valor financiero y no necesariamente como ideología porque ha incitado el crecimiento de una comunidad a su alrededor que confía en sus alcances y en la visión de su creador, por lo cual creer que la moneda ha suplantado las relaciones sociales (basados estrictamente en la confianza) por códigos es falaz.[43]

Generalmente, las propuestas de reforma del sistema monetario buscan la desregulación del dinero por el Estado o por los bancos. El *bitcoin* es un modelo que promueve, en teoría, las dos, y Dodd está de acuerdo en que parte del atractivo nace de la crisis bancaria del 2008. *Bitcoin* resuelve el problema actual del sistema financiero que ata la producción de efectivo sistemáticamente a la producción de deuda (los sistemas bancarios permiten que los bancos generen dinero al extender préstamos). Por lo tanto, muchos admiradores de la criptomoneda son de índole anarquista o libertaria (*libertarian*) y su atracción al sistema nace de un sentimiento de protesta lo cual hace que sea un movimiento social tanto como una moneda. Un gran atractivo no es solamente que *bitcoin* elimina el control central, sino que busca "eliminar la política de la producción y el manejo del dinero en su totalidad".[44]

Bitcoin no es diferente a ninguna otra divisa, dado que todo el dinero es virtual en el sentido de que depende de una serie de obligaciones y condiciones a las cuales está vinculado. La diferencia es

[42] Nigel Dodd, “The social life of Bitcoin”, *LSE Research* Online, febrero de 2017. Consultado el 22 de enero de 2018 en: https://goo.gl/SkjkCy
[43] *Ídem*
[44] *Ídem*

que la moneda efectivamente imita las propiedades del oro en un sistema virtual. Muchos argumentan el uso del oro como divisa dado que no se puede crear más; bajo esta óptica el dinero, o los valores que lo respaldan, es un objeto que debe mantenerse escaso para proteger su valor. En el caso del *bitcoin*, es conocimiento público que únicamente existen o se podrán introducir al mercado 21 millones.

Sin embargo, es falso que no podría eliminarse el límite establecido y se podrían generar más. La noción de que nunca se puede alterar el total "es una ficción necesaria que mantiene a la red unida". De levantar dicho límite, se perdería la confianza en el sistema. Esta ficción es similar a la creencia que “las políticas monetarias son técnicas y no políticas y que los bancos centrales operan más allá de las consideraciones comunes a los gobiernos”, asegura Dodd. [45]

En realidad, la producción de *bitcoin* está dominada por un número pequeño de mineros, y el sistema de hecho favorece a los productores más poderosos e incentiva la creación de monopolios. Si uno quisiera minar *bitcoin*, quizás la única posibilidad sería unirse a alguna *mining pool*[46], o rentar un espacio en una operación minera mayor. Esto implica que es matemáticamente posible que un minero o grupo de mineros con enorme poder computacional monopolicen la creación de nuevas monedas.[47] Asimismo, quienes más capital poseen son más capaces de adquirir mejores máquinas para minar y también asumir los costos de energía que conllevan los procesos computacionales.

El riesgo de la especulación

Para muchos economistas, las nuevas monedas representan una burbuja de especulación peligrosa ya que su inflación tiene que ver simplemente con la consideración de que seguirán creciendo y no en algún valor intrínseco. El regulador financiero del estado de Massachusetts en EEUU publicó varias recomendaciones para advertir a posibles inversionistas acerca de los peligros de estas monedas: 1) no son realmente dinero como cualquier otro ya que no los valida ningún gobierno o autoridad central; 2) las pérdidas causadas por *hackeos* o robos de cualquier tipo son irreparables; 3) el bloque de cadenas es un sistema nuevo y experimental que es susceptible a cambios, errores o actividad criminal.[48]

Steve H. Hanke del *CATO Institute* considera que, aunque existe un suministro limitado del *bitcoin*, la demanda ha resultado ser muy variable, lo cual ha causado cambios importantes en su precio y creado un ciclo de burbuja especulativa y desilusión en el mercado (*bubble-bust*).[49] Dicha volatilidad es su debilidad más grande ya que para Hanke esta es evidencia de que la moneda no es realmente dinero, pero más bien un activo sobre el cual se especula. Dada la volatilidad, el *bitcoin* no puede usarse confiablemente para contar – por ende, no puede usarse para comparar los valores de bienes y servicios, lo cual es un atributo clave del dinero. A su consideración, el *bitcoin* será

[45] *Ídem*
[46] Grupos de mineros organizados que juntan sus recursos y capacidades para lograr minar *bitcoins*, de ser exitosos, reparten las ganancias de manera equitativa.
[47] El autor señala que esto es parte del diseño de *bitcoin* y bien podría ser que otras monedas lo eviten.
[48] Thomas Franck, “Massachusetts regulator lists 7 dangers with bitcoin, calls it potentially ´worthless´”, *CNBC*, 13 de diciembre de 2017. Consultado el 31 de enero de 2018 en: https://goo.gl/spxgQC
[49] Steve H. Hanke, “Bitcoin might not be money, but cryptocurrencies are the way of the future”, *CATO Institute*, 11 de diciembre de 2014. Consultado el 31 de enero de 2018 en: https://goo.gl/Bswiyh

reemplazado por monedas mejor desarrolladas, lo cual podría conllevar a una devaluación considerable.[50]

Las herramientas convencionales para medir el valor o la efectividad de alguna inversión no son aplicables al sistema de *bitcoin* ya que la única ganancia directa para el usuario vendría a través de un incremento en su precio, no de bonos o intereses.[51] Ya que es difícil establecer un valor sobre el mismo, no es posible concluir que su precio incrementará en un mes, un año o mañana. Un *bitcoin* no tiene un valor absoluto (al no contar con respaldos tradicionales) y su suministro limitado es necesario para que se le adscriba valor, más no es suficiente para considerarlo valioso.[52] Por ende, es importante considerar los riesgos que corren hoy en día los negocios que deciden aceptarlos como pago (su volatilidad implica que de un día para otro, puedan perder enormes cantidades de dinero) así como el efecto que tendría en el mundo de devaluarse a cero.

De ser una burbuja como muchos consideran, se prevé que pueda perder hasta 80% de su valor actual, ya que históricamente este ha sido el resultado en otras situaciones similares.[53] Aun así, varios economistas consideran que la devaluación de la moneda no tendría un impacto devastador en el mundo financiero. Esto, dado que el valor que aporta *bitcoin* al mercado es muy pequeño comparado al que aporta el oro, los bonos u otros activos.[54] Pocas instituciones grandes han invertido en la moneda y aquellas que lo han hecho, definitivamente no le destinaron grandes partes de su portafolio, por lo cual se estima que de caer a un precio de 0 dólares, el impacto en los precios de la bolsa estadounidense serían de -0.5%. Asimismo, existen mucho menos inversionistas comunes en esta posible burbuja de los que había en las burbujas de activos de tecnología en el año 2000 o en la burbuja inmobiliaria del 2007.[55] Por ende, el riesgo más grande es a los inversionistas individuales, muchos de los cuales han apostado grandes sumas de sus ahorros al éxito y permanencia de esta tecnología.

Consideraciones finales: cambios irreversibles

El economista ganador del Premio Nobel, Paul Krugman, publicó en 2013, un artículo en el que aseguraba que una de las características con las cuales no cuenta *bitcoin* pero sí cuenta el dinero tradicional es el concepto de "guardar" algún valor.[56] El valor que respalda al oro es su utilidad o apreciación estética y el valor que respalda al dólar es el reconocimiento del Estado (se pueden pagar impuestos con él) además de que la Reserva Federal promete comprarlos en caso de que su valor se contraiga más allá de cierto punto. En efecto, la mayor (y muy válida) crítica hacia estos nuevos sistemas es que son esencialmente juegos de especulación ya que al final del día no existe

[50] *ídem*
[51] *The Economist,* "Bitcoin is a speculative asset but not yet a systemic risk", 16 de diciembre de 2017. Consultado el 30 de enero de 2018 en: https://goo.gl/TMQAni
[52] Que existan pocos o sean difíciles de conseguir no los hace por naturaleza valiosos: esto solo importa dentro de un sistema en el cual se les adscribe un precio.
[53] Adam Shell, "Bitcoin: if currency crashed, plunge would hurt investors but not economy", USAToday, 23 de enero de 2018. Consultado el 31 de enero de 2018 en: https://goo.gl/NDnBxb; y, *The Economist,* "Bitcoin is a speculative...", op. cit.
[54] *Ídem*
[55] *Ídem*
[56] Paul Krugman, "Bitcoin is evil", *The New York Times*, 28 de diciembre de 2013. Consultado el 22 de enero de 2018 en: https://krugman.blogs.nytimes.com/2013/12/28/bitcoin-is-evil/

nada que garantice que una moneda cibernética se puede traducir a miles, cientos o si quiera decenas de dólares.

Es por esto que las fluctuaciones en el valor de la moneda han sido tan vertiginosas y radicales. Aunque el precio de una moneda subió de 800 dólares en enero de 2017 a casi 20,000 dólares en diciembre del mismo año, para posteriormente bajar a alrededor de 11,000 dólares (su valoración actual), continúan existiendo las posibilidades de que llegue a valer absolutamente cero. De suceder esto, se eliminarían miles de millones de dólares del mundo, y miles de personas perderían una porción de sus ahorros – generando crisis que el mismo sistema quiere evitar.

Visto desde esta óptica el *bitcoin* realmente no tiene valor alguno. No obstante, sí tiene un costo real más allá del valor o precio que le adscriba la sociedad o el mercado: su consumo de energía. Morgan Stanley publicó recientemente una proyección que revela que la demanda de energía de la moneda llegaría a oscilar entre los 120 y 140 terawatts por hora, equivalente al nivel de consumo de Argentina.[57] Como punto de comparación, los sistemas de pago VISA utilizan la energía equivalente a la de 50,000 hogares estadounidenses para completar 350 millones de transacciones, mientras que *bitcoin* usa la energía de 2.8 millones de hogares para lograr 350 mil transacciones.[58] De manera similar, la energía para minar y reciclar oro gasta 138KWh al año, e imprimir dinero y crear monedas otros 11KWh, mientras tanto, minar *bitcoin* requiere entre 0.8KWh a 4.4KWh anualmente. El costo del *bitcoin* es real y su impacto también: más allá de un futuro lejano o cercano hoy tiene implicaciones legales, financieras y medioambientales que no son simples de ignorar. Sin embargo, la tecnología continúa evolucionando y sus fallas (así como algunos de sus atractivos) están sujetas a cambiar.

En parte, los riesgos más grandes a la expansión en el uso de este activo financiero son las regulaciones gubernamentales. Los Estados han buscado más formas de controlar, regular y hasta prohibir las interacciones financieras entre usuarios ya que en el peor de los casos podrían suponer transacciones nefarias de lavado de dinero o que contribuyen a industrias criminales y en el mejor de los casos generarían incentivos para efectuar operaciones susceptibles de evadir impuestos. La regulación sería, para muchos, la muerte de los mejores aspectos del sistema. Quienes creen en la importancia de eliminar la intervención bancaria o gubernamental sin duda considerarán esta imposición como un enorme fracaso. Irónicamente una de las "libertades" que ofrece *bitcoin* es no participar en la creación del *Big Data* de consumidores, bajo el cual todos estamos actualmente sujetos dado que las transacciones son monitoreadas y analizadas por las compañías bancarias, de tarjetas de crédito, comercios, etc.[59] Al permitir cierta regulación, se perderían dichas ventajas, al menos desde una perspectiva general.

Sin embargo, para la gran mayoría de las personas la regulación podría implicar no solamente un incremento notable de la confianza en el sistema (lo cual podría acelerar su popularidad, pero desacelerar sus precios) sino también certeza y seguridad legal ante controversias y emergencias de toda índole. Asimismo, existen un sinfín de aplicaciones importantes para las criptomonedas. En

[57] The Canadian Press, “Energy hunters: Bitcoin miners search for cheap, innovative energy sources”, *Global News Canada*, 28 de enero de 2018. Consultado el 29 de enero de 2018 en: https://goo.gl/b6Htpa
[58] Nicole Kobie, "How much energy does bitcoin mining really use? It's complicated", *Wired*, 2 de diciembre de 2017. Consultado el 25 de enero de 2018 en: https://goo.gl/4mZ4Dy
[59] *Ídem*

México se ha destacado el potencial de su uso para evitar los altos costos de las transferencias de remesas, así como la inversión a pequeña escala y la posibilidad de utilizar servicios financieros simplemente con acceso al internet, sin necesitar de instituciones físicas y papeleo. Lo que está por verse es la manera en la cual puedan coexistir ciertas regulaciones dentro del sistema sin eliminar todas las ventajas actuales. Como bien mencionó el artículo del *Harvard Business Review,* partes de la tecnología (*blockchain*) pueden y ya están siendo adaptadas a los sistemas actuales.

Finalmente, una consideración importante es que el *blockchain* limita y hace posible la idea de singularidad: desde la idea de que el dinero es una cosa, cuya producción puede regularse y controlarse hasta la noción de que cada una de nuestras acciones y transacciones son eventos verificables. La memoria del *blockchain* promete ser infalible, y dibuja un mundo de certezas sin control centralizado que es atractivo a primera vista.[60] El *bitcoin* podrá o no tener éxito (ya existen cientos de otras monedas con procesos distintos y aplicaciones más específicas)[61] pero lo que es incuestionable es que su impacto ya está teniendo efecto. Sea o no una burbuja financiera y se convierta o no en una tecnología paralela de intercambios financieros, su creación ha desatado una nueva etapa en el avance tecnológico con múltiples implicaciones, algunas aún por determinarse, para la manera en que opera la economía mundial.

[60] Nigel Dodd, op. cit.

[61] Entre éstas, destacan: 1) *Litecoin*: una alternativa que requiere menos poder de procesamiento para generar los algoritmos y por ende es más veloz, además de que permite que usuarios comunes participen en su red. Mientras *bitcoin* es el "oro", el creador de *litecoin* lo fundó para ser la "plata"; 2) *Ripple*: es considerablemente diferente a *Bitcoin* ya que funge como un sistema de pagos e intercambios internacionales, más para dichas transacciones se debe pagar una cuota la cual únicamente es aceptada en sus propias monedas, XRP. No involucra "minar" y además está respaldada por muchas instituciones financieras que están experimentando con esta nueva tecnología para transacciones globales; 3) *Dash*: busca mejorar el sistema de *Bitcoin* al mejorar el tiempo de procesamiento y resguardar aún más la anonimidad de sus usuarios; 4) *Ethereum*: es una plataforma abierta basada en tecnología de *blockchain* que permite que se construyan aplicaciones inteligentes que atienden distintas necesidades. No obstante, para la creación y funcionamiento de estas aplicaciones, se requieren pagos a través de su propia moneda, *ether*. Recientemente también se anunció la creación de una critpomoneda en Venezuela, que será respaldada por el petróleo y los recursos naturales del país, más esta no será la primera criptomoneda estatal. Para más información véase: *Visual Capitalist*, "The Crypto Universe", septiembre de 2017. Consultado el 31 de enero de 2018 en: https://goo.gl/gWdZx8; Mohit Mamoria, "Everything you've ever wanted to know about Ethereum, patiently explained", *The Next Web*, diciembre de 2017. Consultado el 31 de enero de 2018 en: https://goo.gl/9a9fRZ; y Amelia Heathman, "Move over bitcoin, these countries are creating their own digital currencies", *Veredict*, 27 de septiembre de 2017. Consultado el 31 de enero de 2018 en: https://goo.gl/YxuzQ7

CENTRO DE ESTUDIOS INTERNACIONALES
GILBERTO BOSQUES
ANÁLISIS E INVESTIGACIÓN

Coordinadora General
Adriana González Carrillo

Coordinación y revisión
Arturo Magaña Duplancher
Ana Margarita Martínez

Investigación y elaboración
Inés Carrasco Scherer

Enero de 2018

El **Centro de Estudios Internacionales Gilberto Bosques** del Senado de la República tiene como objeto la realización de estudios y el acopio de información sobre temas de política internacional y política exterior de México; así como el prestar apoyo a las comisiones de relaciones exteriores para el desarrollo de sus actividades y el ejercicio de las facultades exclusivas del Senado en materia de política exterior; además de auxiliar a los órganos directivos, comisiones, grupos parlamentarios y senadores que así lo requieran en cuanto a diplomacia parlamentaria y protocolo en el ámbito internacional.

CGBSenado

http://centrogilbertobosques.senado.gob.mx/