Notas Económicas Regionales

Secretaría Ejecutiva del Consejo Monetario Centroamericano

No. 107, noviembre de 2019

Vulnerabilidades del Bitcoin *

Randall Romero Aguilar†
rromero@secmca.org

Keylin Jiménez Elizondo‡
keylin.jimenez.elizondo@una.cr

A pesar de que en sus inicios en 2008 el Bitcoin era más una curiosidad de interés únicamente para personas muy cercanas a la computación y a las últimas tendencias tecnológicas, a partir de 2017 su explosivo precio despertó el interés del público general y la preocupación de muchas autoridades monetarias. Si bien es cierto su precio se desplomó durante 2018, se ha recuperado considerablemente durante el transcurso de 2019 (ver figura 1).

Según Blundell-Wignall (2014), la crisis financiera de 2008 generó una pérdida de confianza del público en muchos intermediarios financieros y sistemas de pagos. En este contexto, la principal innovación de las criptomonedas (de las cuales Bitcoin fue la primera) fue la de ingeniar un mecanismo para que dos partes pudiesen realizar transacciones sin necesidad de confiar en un intermediario. No obstante, debemos señalar que, aunque en principio sí es posible transar con criptomonedas sin la necesidad de un intermediario, el nivel de conocimiento informático requerido para ello es tan elevado que el público general interesado en utilizar criptomonedas debe hacerlo a través de diversos productos (billeteras, cajeros automáticos) provistos por terceros; es decir, en la práctica lo que terminan haciendo los usuarios de estas criptomonedas es trasladando su confianza de los intermediarios financieros tradicionales (bancos principalmente) a proveedores de servicios que ni siquiera tienen una sede física conocida.

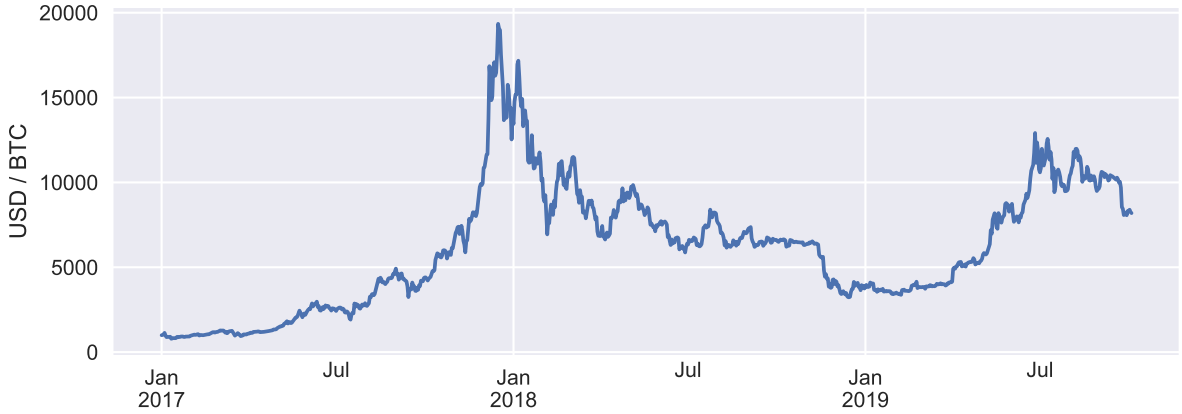
En esta nota revisamos algunas de las principales vulnerabilidades del Bitcoin, muchas de las cuales son extensivas a otras criptomonedas. Estas vulnerabilidades se presentan en cuatro ámbitos: (*1*) volatilidad, (*2*) informático, (*3*) bloqueos y regulaciones, y (*4*) y uso de energía .

*Las opiniones expresadas son las de los autores y no necesariamente representan la posición de la SECMCA, ni de los miembros del CMCA.

†Economista de la Secretaría Ejecutiva del Consejo Monetario Centroamericano (SECMCA). Doctor en Economía por la Ohio State Univesity.

‡Investigadora Junior del CINPE, Universidad Nacional de Costa Rica (UNA).

Figura 1: Precio de un bitcoin, en dólares de Estados Unidos



Fuente: https://www.cryptocompare.com/

1 Volatilidad

La vulnerabilidad más evidente del Bitcoin, tal como lo delatan la figura 1, es la volatilidad de su valor. En 2017 el precio del Bitcoin experimentó una clásica burbuja especulativa, impulsada posiblemente por lo que en inglés se denomina "FOMO" (fear of missing out), lo cual describe una situación en la que inversionistas individuales al observar el creciente valor de un activo, que está haciendo que otros inversionistas tengan grandes ganancias, y por "miedo a quedarse afuera" deciden comprar el activo, con la creencia errónea de que su precio continuará subiendo inexorablemente. Así, habiendo iniciado su precio cerca de USD 1000 en 2017, impulsado por esta manía especulativa el Bitcoin rozó los USD 20 000 el día 16 de diciembre, tan solo para desplomarse posteriormente, cerrando a finlaes de 2017 en USD 13 850 y en 2018 en USD 3747. A pesar de haber ganado terreno en el primer semestre de 2019, en meses más recientes ha tendido a caer por debajo de USD 10 000.

La volatilidad del Bitcoin resulta aún más evidente al analizar los cambios porcentuales semanales en su precio (ver figura 2), en el cual se observa que en períodos tan relativamente cortos como una semana el Bitcoin puede ganar o perder cerca del 30% de su valor de mercado. No es de sorprender, por tanto, que los economistas consideren el Bitcoin como un instrumento de inversión de muy alto riesgo. No obstante, los defensores del Bitcoin consideran que esta volatilidad se debe a su reciente llegada, ya que, si bien se presentó desde 2008, su popularidad se incrementó hasta 2017, razón por la cual aún hay un desconocimiento generalizado del uso y funcionamiento de su tecnología subyacente.

Esta volatilidad del Bitcoin suele explicarse en términos de cuatro factores, a saber (*1*) la especulación, (*2*) la competencia de otras criptomonedas, (*3*) el cierre de casas de cambio,

Figura 2: Cambio porcentual semanal en el precio en dólares de un bitcoin

Fuente: Elaboración propia con datos de https://www.cryptocompare.com/

y (*4*) la concentración de mercado .

Especulación Al ser un mercado relativamente reciente, las suposiciones sobre el futuro de este criptoactivo suelen ser muy cambiantes, en parte en respuesta a la incertidumbre regulatoria (constantes advertencias de países acerca de regulaciones, bloqueos y cierres de casas de cambios). Además, al estar los bitcoins concentrados en pocas manos, las decisiones de un solo usuario pueden generar cambios importantes en su precio.

Inversión en otros criptoactivos La creación de Bitcoin dio paso a una serie de nuevas monedas digitales, entre ellas Ethereum, Ripple, Bitcoin cash, Zcash y Litecoin. Estas nuevas monedas compiten con el Bitcoin, habiendo sido diseñadas para subsanar algunas de las debilidades del Bitcoin. Ahora bien, aunque estas nuevas monedas pueden reducir la demanda por Bitcoin, en la práctiva se ha observado una correlación importante entre los precios de todas ellas.

Cierres de casas de cambio Al igual que con las nuevas criptomonedas, en los últimos años también han proliferado las casas de cambio, generando mayores opciones para poder realizar operaciones con estas monedas. Sin embargo, las regulaciones y los *hackeos*, han provocado el cierre de muchas casas de cambio, a su vez trayendo inestabilidad a las criptomonedas.

Concentración de mercado Roubini (2018) señala que la descentralización de Bitcoin es un mito, por cuanto hay una centralización masiva y concentración de poder oligopólico y carteles entre mineros, casas de cambios y desarrolladores. Así, "los mineros

> están centralizados masivamente, ya que los cuatro principales controlan tres cuartas partes de la minería y se comportan como cualquier oligopolista: suben los costos de transacción para aumentar sus altos márgenes de ganancia" (Roubini 2018, p. 18).

Los factores anteriores ayudan a explicar la volatilidad de corto plazo del Bitcoin. Es importante señalar que en el largo plazo, el Bitcoin tiene una vulnerabilidad aún más notoria: su oferta total fija de 21 millones de bitcoins. Esto lo descalificaría como una moneda viable, porque a menos que el suministro de una moneda siga al PIB nominal potencial, terminaría por degenerar en una economía deflacionaria, en la cual los precios de los bienes *disminuyen* con el tiempo (provocando recesiones por la contracción del gasto de consumo) y las deudas nominales terminen inflándose en términos reales (fenómeno que precipitó la Gran Depresión, según Irvin Fisher) (ibíd.)

2 Informático

El Bitcoin también presenta vulnerabilidades informáticas considerables, las cuales podrían resumirse en lo que Roubini (ibíd., p.10) denomina la "inconsistente trinidad de Buterin", en alusión a Vitalik Buterin (creador de Ethereum), quien señaló que en *blockchain* no es posible contar simultáneamente con escalabilidad, decentralización, y seguridad. "Bitcoin, por ejemplo, está parcialmente descentralizado, incluso si su minería ahora está masivamente centralizada, pero no es escalable debido a su mecanismo de autenticación de prueba de trabajo (PoW), que permite solo de 5 a 7 transacciones por segundo. Y es seguro, hasta ahora, pero a costa de no tener escalabilidad. Y dado que su minería ahora está masivamente centralizada, como un oligopolio de mineros que controla su minería, su seguridad está en riesgo" (ibíd., p. 10).

Así, en el ámbito de las vulnerabilidades informáticas destacan la lentitud de las transacciones y la posibilidad de robo de las cuentas de Bitcoin.

Lentitud de las transacciones

El intercambio de criptomonedas se realiza mediante plataformas que han sido creadas específicamente para que los usuarios compren y vendan las monedas virtuales: las casas de cambios descentralizadas (DEX). Estas "funcionan sin intermediarios y operan en entornos mantenidos por un software, a través del cual se interactúa con la tecnológica de las distintas blockchains" (González 2018). No obstante,

> La blockchain de Bitcoin contiene ciertas limitaciones en el tamaño de los bloques, impuestas voluntariamente desde sus inicios. Estas limitaciones tienen

> como objetivo favorecer su adopción y mantener la red descentralizada porque es precisamente esa descentralización la que hace que sea resistente a cualquier tipo de censura o de control. Lo que ha ocurrido ahora es que a medida que aumentaba el número de usuarios y por tanto también de transacciones, éstas se hacían más lentas. Si una persona quiere "acelerarlas" y lograr que se confirmen antes tiene que pagar unas comisiones más altas (Preukschat 2017).

Para hacer frente a este problema se ha sugerido actualizar el software de Bitcoin, de manera que se agilicen las transacciones. Sin embargo, la negativa por parte de algunos mineros ha hecho inviable esta propuesta, causando que las plataformas continúen cayendo debido a que no son adecuadas para la cantidad de transacciones que se realizan diariamente.

Robo de criptomonedas mediante hackeos a las DEX

Los distintos hackeos que han sufrido plataformas que intercambian criptomonedas (Bitcoin entre ellas) ponen en duda la seguridad de tales portales. Entre los casos más notorios destacan (ver figura 3) el de Mt. Gox, una empresa con sede en Tokio que en febrero de 2014 perdió bitcoins valorados en ese entonces en cerca de USD450 millones, así como el de Coincheck (otra DEX japonesa), de donde desaparecieron *tokens* de NEM (una criptomoneda) valoradas en USD400 millones en enero de 2018, y más recientemente el caso de la estafa iFan/Pincoin, dos criptomonedas operadas como un esquema de Ponzi, el cual fue puesto en evidencia en abril de 2018, luego de que se había estafado un valor cercano a los USD650 millones de inversionistas en Vietman.

Cabe resaltar que en estos episodios los clientes de las plataformas son los más afectados ya que, al no contar las criptomonedas con regulación ni garantías similares a las de una entidad financiera, los clientes de las plataformas "hackeadas" acaban perdiendo el valor de sus criptomonedas.

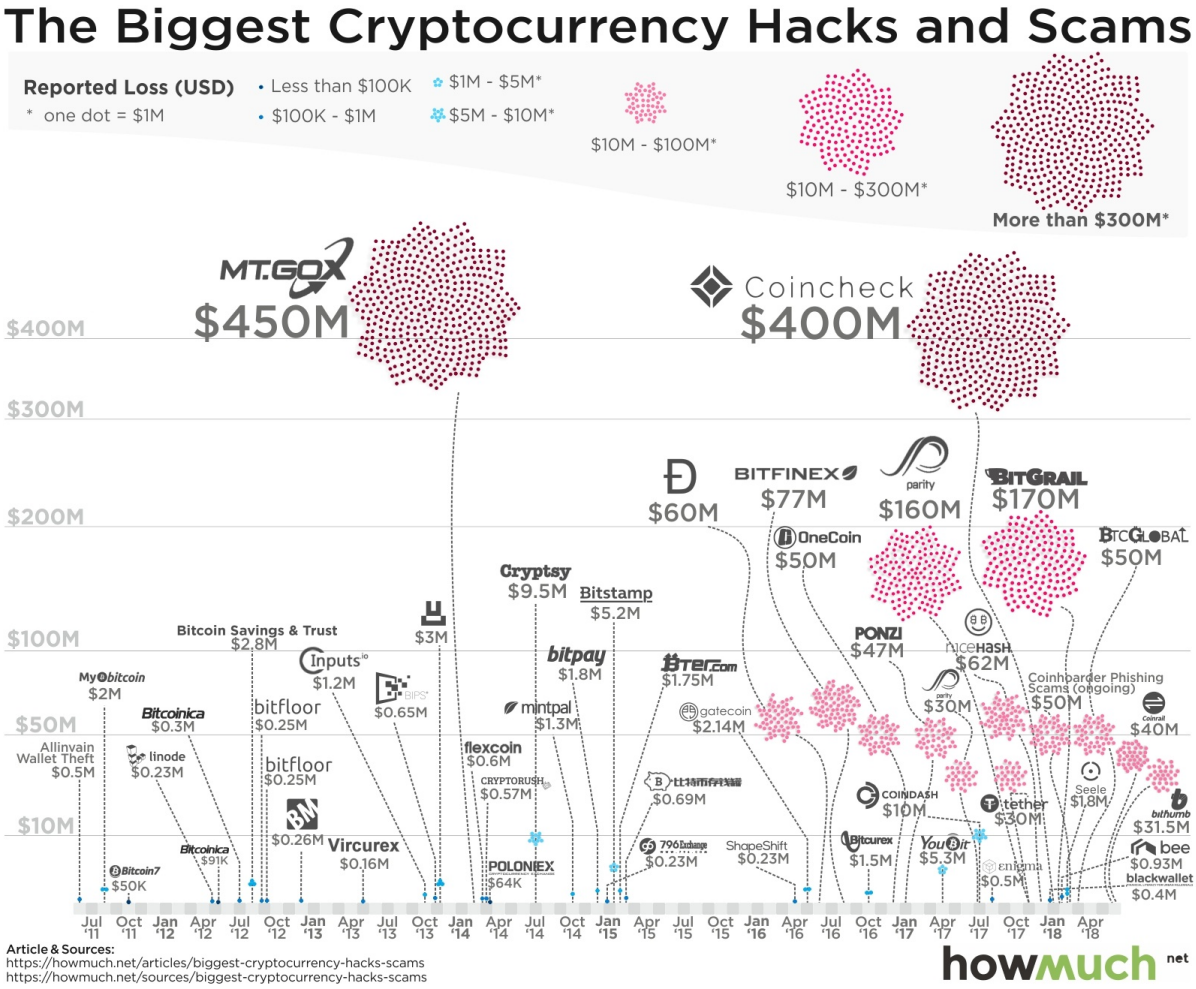
3 Bloqueos y Regulaciones

Otro de los desafíos a los que se enfrentan Bitcoin y demás criptomonedas es el de los bloqueos por parte de instituciones financieras y de empresas publicitarias, así como regulaciones oficiales.

Bloqueos y cierres por parte de instituciones financieras

Una manera de pagar con bitcoins es "pre-cargarlos" en una tarjeta de crédito o débito, para lo cual se adquieren bitcoins a cambio de fondos de cuentas expresadas en monedas

Figura 3: Los robos y estafas más grandes de criptomonedas



Fuente: https://howmuch.net/articles/biggest-crypto-hacks-scams/

de curso legal. No obstante, diversas entidades financieras han bloqueado las tarjetas de crédito que utilizan bitcoin. Por ejemplo, Visa, uno de los principales proveedores de tarjetas de crédito, anunció a inicios de 2018 que el servicio quedaba suspendido de manera indefinida. (El Español 2018). Ahora bien, aunque los proveedores devuelvan las criptomonedas de manera tal que sus clientes no pierdan sus recursos, este tipo de bloqueos le resta liquidez a Bitcoin, al no poder ser utilizado fácilmente como medio de pago.

Además, bancos comerciales alrededor del mundo (por ejemplo en Colombia y Australia) han bloqueado cuentas de plataformas que operan con Bitcoin. Por su parte, muchos bancos centrales advierten sobre el peligro de utilizar Bitcoin y otros criptoactivos, por no contar los mismos con ningún respaldo institucional.

Regulaciones de gobiernos

Otro obstáculo que enfrenta Bitcoin son los esfuerzos de distintos gobiernos por regularlo. Parte del interés de los gobiernos por regular a las criptomonedas surge del anonimato asociado con las transacciones, el cual facilita la evasión fiscal, el blanqueo de capitales y la financiación de grupos terroristas.

Así, los gobiernos de países alrededor del mundo han recurrido a distintos grados de regulación, y así Bitcoin es legal en algunas jurisdicciones (Estados Unidos, países europeos, Australia, Nueva Zelanda, por ejemplo) o completamente ilegal en otras (Argelia, Bolivia, Ecuador, Egipto, Marruecos, Nepal, Pakistán, entre otros). Una posición intermedia muy común es la de considerar al Bitcoin como legal, pero prohibirle al sistema bancario la tenencia o movimiento de bitcoins (Arabia Saudita, Canadá, China, Colombia, India, Jordania, Tailandia y Taiwan, por citar algunos).

Por otro lado, la Comisión de Bolsa y Valores (SEC, por sus siglas en inglés) de Estados Unidos, ha anunciado que todas aquellas plataformas que ofrezcan la opción de intercambios de las monedas digitales, deben estar registradas en la SEC. Esta decisión se tomó debido a que consideran que "muchas plataformas se refieren a sí mismas como de intercambio lo que puede dar la impresión errónea a los inversores de que están regulados o cumplen con los estándares regulatorios de una bolsa de valores nacional" (Aguilar 2018). En principio, el registro de estas plataformas permitirá a la SEC proteger a los diferentes clientes de posibles fraudes.

Algunos gobiernos ya han ido más allá de establecer regulaciones, y han recurrido a allanamientos de importantes casas de cambio de criptomonedas, ante sospechas de lavado de dinero o de evasión de impuestos. Por ejemplo, en España "desarticularon dos redes de lavado de activos que realizaban operaciones de compraventa a través de criptomonedas" (El Espectador 2018).

Publicidad en redes sociales

No solo son los gobiernos y las instituciones financieras quienes bloquean y regulan a Bitcoin. En respuesta a los robos y estafas mencionados en la sección anterior, a inicios de 2018 Facebook y Google decidieron prohibir la publicidad de criptomonedas en sus redes, lo cual representó un golpe al valor del Bitcoin, puesto que estas dos empresas concentran dos tercios del negocio de la publicidad en Internet (Solís 2018). Esta decisión se tomó para evitar que los usuarios sean estafados, puesto que en muchos casos las ofertas

de bitcoin anunciadas en la publicidad proviene de empresas que "no operan de buena fe".

No obstante, meses después Facebook cambió su posición, permitiendo la publicidad sobre criptomonedas, pero asegurando que:

> Trabajarán para garantizar que estas sean seguras, pero continuarán "prohibiendo los anuncios que promocionen opciones binarias y ofertas iniciales de monedas (ICO por sus siglas en inglés)". La firma resaltó que "no todos los que quieran anunciarse podrán hacerlo", existen requisitos. Entre estos: los anunciantes deben enviar una solicitud para evaluar su elegibilidad, mostrar licencias y antecedentes públicos de sus negocios (El Universal 2018).

Por su parte, Google ha levantado parcialmente la prohibición de publicidad, aunque a igual que Facebook prohíbe las ICO.

4 Uso de energía

De todas las deficiencias de Bitcoin quizás la más notoria sea el elevado uso de energía que utiliza este sistema de transacciones (ver datos en Cuadro 1). Por ejemplo, se estima que en 2018 Bitcoin requirió cerca de 73.1 terawatt-horas para funcionar, un consumo eléctrico similar al de Austria, o bien cercano al consumo de electricidad de 6,8 millones de hogares en Estados Unidos

Este gasto de electricidad es también notorio en términos de consumo por transacción: para procesar una sola transacción se requirió en promedio de 778 kilowatt-horas, energía suficiente para abastecer de energía por casi un mes completo a un hogar típico de Estados Unidos. En contraste, esa misma cantidad de energía es suficiente para procesar cerca de 460 mil transacciones por Visa.

Parte del enorme consumo de electricidad de Bitcoin está asociado con la forma en que se "emiten" o "minan" nuevos bitcoins. El sistema está diseñado para que la emisión de un nuevo bitcoin requiera una prueba de trabajo, que básicamente consiste en resolver un problema criptográfico cuya solución es muy sencilla de verificar pero encontrar tal solución requiere de mucho trabajo de computador (de ahí su nombre). Al ser este un sistema competitivo (en el sentido de que el primer minero que resuelva el problema obtiene el bitcoin), se desperdicia una cantidad importante de energía (todos aquellos mineros que no lograron resolver el problema a tiempo, e incluso la del que sí lo resuelve, porque ha resuelto un problema intrascendente *per se*). Lo ineficiente de minar bitcoins de esta manera es más que evidente cuando se piensa en términos del "señoreaje": los datos del Cuadro 1 muestran que 77% del valor de los bitcoins minados solo "sirven" para cubrir la factura

Cuadro 1: Estadísticas sobre el bitcoin 2018

Descripción	Valor
Ingresos globales de la minería (anualizado)	$4,745 millones
Costos globales de la minería (anualizado)	$3,656 millones
Costo actual de la minería, como porcentaje del ingreso	77.04%
Consumo eléctrico actual estimado de Bitcoin	73.12 TWh
País más cercano en términos de consumo de electricidad	Austria
Hogares de EE.UU. que podrían abastecerse con la energía utilizada por Bitcoin	6,8 millones
Electricidad consumida por transacción	778 KWh
Días que un hogar de EE.UU. podría abastecerse con la energía utilizada por una transacción	26.3
Consumo de electricidad de Bitcoin (% consumo mundial)	0.33%
Huella de carbono anual	35,830 kt de CO_2
Huella de carbono por transacción	381.35 kg de CO_2

Fuente: Digiconomist 2018

eléctrica necesaria para minarlos.

Todo este desperdicio de energía tiene un efecto nefasto para el medio ambiente: Se estima que la huella de carbono del sistema Bitcoin es comparable con la de todo Dinamarca, y que la huella de carbono de una sola transacción en Bitcoin es similar a la producida por 700 mil transacciones de Visa o bien la de cerca de 50 mil horas de ver videos en Youtube.

A manera de conclusión

En esta nota hemos llamado la atención acerca de las vulnerabilidades del Bitcoin. Aunque nuestra discusión se centra en esa criptomoneda en particular, muchas de las vulnerabilidades aquí señaladas aplican en mayor o menor medida a otras criptomonedas.

No es en vano que todos los bancos centrales miembros del Consejo Monetario Centroamericano se han pronunciado sobre este tema (ver Cuadro 2), enfatizando los riesgos que el público enfrenta al utilizar criptomonedas, recordando que ninguna de ellas tiene curso legal en la Región, y que cada persona que "invierte" en este tipo de activos lo hace bajo su propio riesgo.

Cuadro 2: Posiciones de los Bancos Centrales del CMCA respecto de las criptomonedas

Costa Rica

- El Banco Central de Costa Rica (BCCR) advierte sobre los riesgos asociados de utilizar criptomonedas.
- Señala que el único ente con autorización de emitir dinero es el BCCR, por ende, las criptomonedas no pueden considerarse como moneda de curso legal.
- Si bien no prohíbe su uso, no cuenta con respaldo alguno del BCCR.

El Salvador

- El Banco Central de Reserva (BCR) indica que las criptomonedas no tienen curso legal en ninguna jurisdicción.
- Cualquier transacción será bajo responsabilidad y riesgo de quien la realice.
- Se aclara que, por el momento, no existe un marco legal ni regulatorio que se aplique a estas monedas virtuales.
- Representantes del banco, advierten que las estafas se han vuelto una consecuencia del uso de las criptomonedas.

Guatemala

- Al igual que en los casos anteriores el Banco de Guatemala manifiesta que las criptomonedas no son de curso legal en el país.
- Los particulares pueden intercambiar criptomonedas, pero no pueden utilizarlas con poden liberatorio ilimitado.
- Representantes del Banco resaltan el riesgo del uso de criptomonedas y que este debe asumirlo cada usuario. Aunado a ello, recalcan que entre los principales problemas que presentan las monedas virtuales se encuentran la volatilidad y el tema de impuestos.

Honduras

- El Banco Central de Honduras (BCH) no regula ni garantiza el uso de las criptomonedas, por ello, no existe un respaldo ante la utilización o aceptación de estas monedas.
- De igual forma, advierte que la responsabilidad y riesgo de su uso recae sobre quien lo utilice.
- Representantes del banco, indican que cuando el auge de estas monedas sea mayor, se requerirá de especialistas para un mayor entendimiento del tema.

Nicaragua

- No existe un pronunciamiento oficial por parte del Banco Central de Nicaragua, sin embargo, ya se han realizado distintas transacciones en el territorio nicaragüense, lo cual indica que no presentan algún tipo de prohibición efectiva.
- Representantes del Banco indican que no hay un acuerdo sobre la importancia de las criptomonedas entre altos cargos y que es un tema aún impreciso.

República Dominicana

- El Banco Central de la República Dominicana advirtió a aquellos organismos que se encuentran regulados por el sistema financiero que vinculaciones a negocios relacionados con criptomonedas hará que asuman sanciones.
- Respecto a las operaciones de particulares señala que el banco no regula, ni supervisa, ni garantiza este tipo de transacciones.
- Representantes del Banco indican que las monedas virtuales no cumplen con las características de monedas de curso legal, debido a que no se aceptan en cualquier lugar, son muy volátiles y no se cambian rápidamente.

Fuente: Sitios de Internet de los Bancos Centrales del CMCA.

Referencias

Aguilar, Jorge (8 de mar. de 2018). *EE.UU. pone cerco al bitcoin*. URL: https://www.abc.es/economia/abci-eeuu-pone-cerco-bitcoin-201803080238_noticia.html.

Associated Press (11 de dic. de 2017). *El precio del primer bitcoin sube en su debut en la bolsa*. URL: https://www.elnuevodia.com/negocios/economia/nota/elpreciodelprimerbitcoinfu 2381313/.

Blundell-Wignall, Adrian (2014). *The Bitcoin Question. Currency versus Trust-less Transfer Technology*. Inf. téc. 37. OECD.

Digiconomist (6 de nov. de 2018). *Bitcoin Energy Consumption Index*. URL: https://digiconomist.net/bitcoin-energy-consumption.

El Español (5 de ene. de 2018). *Visa bloquea las tarjetas de crédito que usan bitcoins*. URL: https://www.elespanol.com/economia/empresas/20180105/visa-bloquea-tarjetas-credito-usan-bitcoins/274973147_0.html.

El Espectador (11 de nov. de 2018). *Criptomonedas, la nueva modalidad para lavar dinero*. URL: https://www.elespectador.com/noticias/judicial/criptomonedas-la-nueva-modalidad-para-lavar-dinero-articulo-799491.

El Universal (28 de jun. de 2018). *Facebook vuelva a aceptar publicidad de criptomonedas*. URL: http://www.eluniversal.com.mx/techbit/facebook-vuelve-aceptar-publicidad-de-criptomonedas.

González, Glenda (8 de jul. de 2018). *Conoce estas 5 plataformas descentralizadas para el intercambio de criptomonedas*. URL: https://www.criptonoticias.com/colecciones/conoce-5-plataformas-descentralizadas-intercambio-criptomonedas/.

Preukschat, Alex (13 de nov. de 2017). *SegWit2x, el nuevo bitcoin de la industria corporativa de Bitcoin*. URL: https://www.eleconomista.es/firmas/noticias/8739786/11/17/SegWit2x-el-nuevo-bitcoin-de-la-industria-corporativa-de-Bitcoin.html.

Roubini, Nouriel (1 de oct. de 2018). *Exploring the Cryptocurrency and Blockchain Ecosystem*. URL: https://www.banking.senate.gov/imo/media/doc/Roubini%20Testimony%2010-11-18.pdf.

Solís, Alessandro (16 de mar. de 2018). *Google y Facebook eliminan la publicidad de bitcoin*. URL: https://www.economiadigital.es/tecnologia-y-tendencias/bitcoin-publicidad-google-facebook-twitter_543545_102.html.