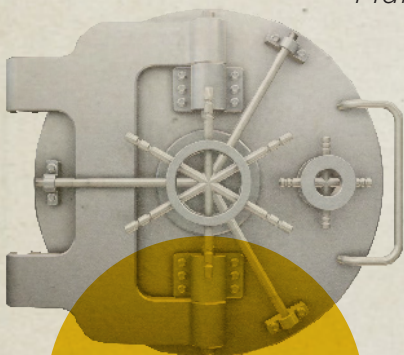


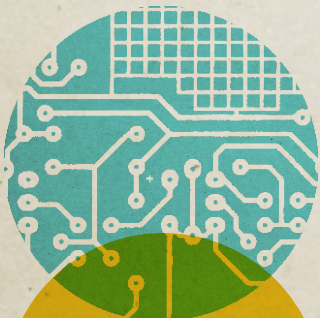


# BITCOIN

*Manual básico (para legisladores  
y diseñadores de políticas)*



POR JERRY BRITO Y ANDREA CASTILLO  
TRADUCIDO POR JUAN LLANOS



Traducción española copyright © 2014 por Juan Llanos

Publicado originalmente con el título “Bitcoin: A Primer for Policymakers”  
Copyright © 2013 por Jerry Brito, Andrea Castillo  
y el Mercatus Center at George Mason University

Mercatus Center at George Mason University  
3434 Washington Boulevard, 4th floor  
Arlington, VA 22201  
703-993-4930  
mercatus.org

**B**ITCOIN ES LA primera moneda digital completamente descentralizada en el mundo. Hace tan solo cuatro años, solo era conocida por un puñado de aficionados en los recónditos foros de Internet. Hoy, la economía de bitcoin es más grande que la de algunas de las naciones más pequeñas del mundo. El valor de un bitcoin (o BTC) ha crecido y fluctuado mucho, desde centavos en sus primeros días hasta más de \$260, el valor máximo que alcanzó en abril de 2013. Se calcula que la capitalización de mercado de la economía de bitcoin supera los mil millones de dólares.<sup>1</sup> Empresas de todo tamaño han mostrado interés en integrar la plataforma de Bitcoin a sus operaciones y ofrecer nuevos servicios dentro de la economía de bitcoin. Los capitalistas de riesgo, además, han comenzado a invertir su dinero en esta creciente industria.<sup>2</sup> El desarrollo de Bitcoin y sus éxitos tempranos son un fascinante testimonio de la inventiva del emprendedor moderno.

Al ser descentralizado, Bitcoin puede usarse de manera pseudónima, lo que ha atraído la atención de los organismos de supervisión de varios países. Las mismas cualidades que hacen a Bitcoin atractivo como sistema de pago también podrían ser explotadas por

---

1. La información financiera suministrada por [bitcoincharts.com](http://bitcoincharts.com) estima que la capitalización de mercado total era \$1,457,815,292 al 29 de mayo de 2013.

2. Sarah E. Needleman y Spencer E. Ante, "Bitcoin Startups Begin to Attract Real Cash," *Wall Street Journal*, 8 de mayo de 2013, <http://online.wsj.com/article/SB10001424127887323687604578469012375269952.html>.

los usuarios para evadir el pago de impuestos, blanquear dinero ilícito o comercializar mercaderías prohibidas. Tanto la Unidad de Inteligencia Financiera, dependiente del Departamento de Tesoro de EE. UU. (en inglés, Financial Crimes Enforcement Network o FinCEN)<sup>3</sup> como el Departamento de Justicia<sup>4</sup> han emitido comunicados públicos sobre la supervisión de las monedas virtuales, incluida bitcoin. Un informe de la Oficina de Responsabilidad Gubernamental (en inglés, Government Accountability Office) sobre las monedas virtuales instó al organismo encargado de la recaudación fiscal de EE. UU. (en inglés, Internal Revenue Service o IRS), por medio de una guía instructiva, a que reduzca los riesgos de violación al código impositivo.<sup>5</sup> El apéndice de dicho informe contiene una carta del Subcomisionado del IRS Steven T. Miller, quien aseguró a dicho organismo que el IRS se encuentra “trabajando para hacer frente a esos riesgos”. Además, un comisionado de la Comisión sobre el Comercio de Futuros sobre Commodities (en inglés, Commodity Futures Trading Commission) expresó recientemente interés en investigar si Bitcoin caía dentro de la jurisdicción de la Comisión.<sup>6</sup> Al considerar cuál es la mejor manera de supervisar esta naciente tecnología, los organismos supervisores del gobierno deben tener cuidado de que la superposición de

---

3. US Department of the Treasury, Financial Crimes and Enforcement Network, “Application of FinCEN’s Regulations to Persons Administering, Exchanging, or Using Virtual Currencies” (Regulatory Guidance, FIN-2013-G001, US Department of the Treasury, Washington, DC, 18 de marzo de 2013), [http://fincen.gov/statutes\\_regs/guidance/html/FIN-2013-G001.html](http://fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html).

4. Jennifer Shasky Calvery, “Combating Transnational Organized Crime: International Money Laundering as a Threat to Our Financial Systems” (Statement for the Record Before the Subcommittee on Crime, Terrorism, and Homeland Security of the House Committee on the Judiciary, 8 de febrero 2012), <http://www.justice.gov/ola/testimony/112-2/02-08-12-crm-shasky-calvery-testimony.pdf>.

5. US Government Accountability Office, “Virtual Economies and Currencies: Additional IRS Guidance Could Reduce Compliance Risks” (report to the Senate Committee on Finance, GAO-13-516, mayo de 2013), <http://www.gao.gov/assets/660/654620.pdf>.

6. Tracy Alloway, Gregory Meyer y Stephen Foley, “US Regulators Eye Bitcoin Supervision,” *Financial Times*, 6 de mayo de 2013, <http://www.ft.com/intl/cms/o/b810157c-b651-11e2-93ba-00144feabdc0.html>.

directrices no obstaculice el prometedor potencial de crecimiento de esta innovadora plataforma financiera.

Este trabajo presenta una breve introducción a la red de Bitcoin, incluidas sus propiedades, operaciones y carácter pseudónimo. Describe los beneficios que permite que la red de Bitcoin se desarrolle y continúe innovando y, al mismo tiempo, resalta los asuntos de interés para consumidores, legisladores y supervisores. Describe también la normativa vigente y analiza otras normas que podrían llegar a ser promulgadas. El trabajo concluye presentando recomendaciones para la formulación de políticas que aliviarán las preocupaciones de mayor interés para los legisladores y al mismo tiempo permitirán la innovación en la red de Bitcoin.

## ¿QUÉ ES BITCOIN?

BITCOIN IS UNA moneda digital de código abierto que permite la transferencia de valor de persona a persona. Entre muchas otras cosas, lo que hace a Bitcoin único es que constituye el primer sistema de pagos digitales completamente descentralizado jamás creado. Esto puede sonar complicado, pero los conceptos subyacentes no son difíciles de comprender.

## Reseña

Antes de que Bitcoin fuera inventado en 2008 por un programador no identificado a quien se conoce como Satoshi Nakamoto, las transacciones realizadas por internet necesitaban siempre de un tercero intermediario de confianza. Por ejemplo, si Alice quisiera enviar \$100 a Bob por internet, tendría que confiar en proveedor de servicio intermediario como lo son Paypal o Mastercard. Este tipo de intermediarios conserva registros de todos los saldos de las cuentas de sus titulares. Cuando Alice le envía \$100 a Bob, PayPal extrae dicho monto de la cuenta de Alice y lo acredita a la cuenta de Bob.

Sin estos intermediarios, existiría el riesgo de que el dinero digital se gaste dos veces. Imagine que no existen intermediarios

que lleven este tipo de contabilidad y que el dinero digital es un simple archivo, como lo son los documentos digitales. Alice podría enviarle \$100 a Bob adjuntando un archivo de dinero a un mensaje. Pero como sucede con el correo electrónico, enviar un documento adjunto no lo elimina de nuestra computadora. Alice conservaría una copia del archivo de dinero después de enviarlo y bien podría enviarlo los mismos \$100 a Carlos. En las Ciencias de la Computación, esto se conoce como el “problema del doble gasto”,<sup>7</sup> hasta la llegada de Bitcoin solo se lo podía resolver empleando un tercero intermediario de confianza que conservara un registro de cada cuenta.

La invención de Bitcoin es revolucionaria porque, por primera vez, el problema del doble gasto puede resolverse sin la necesidad de un tercero. Bitcoin logra esta hazaña mediante la distribución de los registros necesarios entre todos los usuarios del sistema conectados a una red de transmisión de persona a persona. Cada transacción que se produce en la economía de bitcoin queda registrada en un libro digital público, distribuido, que se denomina ‘cadena de bloques’. Cada nueva transacción se verifica contra la cadena de bloques para asegurarse de que los mismos bitcoin no hayan sido gastados previamente, eliminando así el problema del doble gasto. La red global de persona a persona, compuesta por miles de usuarios, toma así el lugar del intermediario, lo que permite a Alice y Bob realizar transacciones sin utilizar Paypal.

Cabe destacar lo antes posible que las transacciones de la red de Bitcoin no están denominadas en dólares o euros o yens, como sí lo están en Paypal, sino que están denominadas en bitcoin. Esto la convierte en una moneda virtual además de una red descentralizada de pagos. El valor de la moneda no está basado en el precio del oro ni determinado por ningún gobierno, sino que es el valor que la gente le asigna. El valor en dólares de un bitcoin lo determina un

---

7. David Chaum, “Achieving Electronic Privacy,” *Scientific American*, agosto de 1992, 96–101.

mercado abierto, de manera similar como se determina la tasa de cambio de dos monedas de curso legal del mundo.<sup>8</sup>

## Operación

Hasta aquí hemos hablado de lo que Bitcoin es: una red descentralizada de pagos de persona a persona y una moneda virtual que, en esencia, funciona como dinero por internet. A continuación, vamos a explicar en mayor detalle cómo es que Bitcoin funciona.

La manera en que se verifican las transacciones y se evita el problema del doble gasto es mediante el ingenioso uso de la criptografía de claves públicas.<sup>9</sup> La criptografía de claves públicas requiere la asignación a cada usuario de dos “claves”: una privada, que debe mantenerse secreta, como una contraseña y una pública que puede compartirse con todo el mundo. Cuando Alice decide transferir bitcoin a Bob, crea un mensaje llamado ‘transacción’ que contiene la clave pública de Bob y lo “firma” con su clave privada. Cualquiera que observe la clave pública de Alice podrá verificar que la transacción fue en verdad firmada con su clave privada, que se trata de un intercambio auténtico y que Bob es el nuevo dueño de los fondos. La transacción—y de esa manera la transferencia de la propiedad de los bitcoin—queda registrada, timbrada con la fecha y la hora y visible en uno de los “bloques” de la cadena de bloques. La criptografía de claves públicas permite que todas las computadoras de la red tengan un registro constantemente actualizado y verificado de todas las transacciones de la red de Bitcoin, lo cual evita el doble gasto y el fraude.

---

8. “Markets,” Bitcoincharts, consultado el 30 de Julio de 2013, <http://bitcoincharts.com/markets/>.

9. Christof Paar, Jan Pelzl y Bart Preneel, “Introduction to Public-Key Cryptography,” capítulo 6 en *Understanding Cryptography: A Textbook for Students and Practitioners*, ed. Christof Paar and Jan Pelzl (New York: Springer, 2010). Se puede consultar una muestra en <http://wiki.cryptorub.de/Buch/download/Understanding-Cryptography-Chapter6.pdf>.

¿Qué queremos decir cuando decimos que es “la red” la que verifica las transacciones y reconcilia el libro? ¿Y cómo es que se crean e introducen nuevos bitcoin a la oferta monetaria? Como ya vimos, dado que Bitcoin es una red de persona a persona, no existe una autoridad central que sea responsable ni de la creación de nuevas unidades monetarias ni de verificar las transacciones. Esta red depende de sus usuarios, quienes brindan su poder computacional para que se puedan registrar y reconciliar las transacciones. Estos usuarios reciben el nombre de “mineros”<sup>10</sup> porque reciben los bitcoin recién generados como recompensa por su trabajo. Los bitcoin se crean o “minan” a medida que miles de computadoras dispersas resuelven complejos problemas matemáticos que verifican las transacciones en la cadena de bloques. Como lo expresó un comentarista,

En realidad, el minado de bitcoin se produce mediante un proceso puramente matemático. Una analogía útil es la de la búsqueda de números primos: solía ser bastante fácil encontrar los números pequeños (en la Gracia Antigua, Eratóstenes produjo el primer algoritmo para encontrarlos). Pero a medida que se los iba encontrando se hacía más difícil encontrar los números más altos. Hoy en día se utilizan computadoras de alta capacidad para hallarlos y quien logra hacerlo es merecedor del respeto de la comunidad matemática (por ejemplo, la Universidad de Tennessee mantiene una lista de los 5,000 más altos).

En el caso de Bitcoin, no se trata de buscar números primos sino una secuencia de datos (conocida

---

10. En general, los mineros tienden a ser entusiastas de la computación comunes, pero a medida que el minado va resultando más difícil y costoso, es probable que esta actividad se profesionalice de alguna manera. Para mayor información, véase Alec Liu, “A Guide to Bitcoin Mining,” *Motherboard*, 22 de marzo de 2013, <http://motherboard.vice.com/blog/a-guide-to-bitcoin-mining-why-someone-bought-a-1500-bitcoin-miner-on-ebay-for-20600>.



como “bloque”) que produzca un patrón particular al aplicársele a los datos el algoritmo hash. Cuando este problema matemático se resuelve, el minero recibe una recompensa en forma de bitcoin (y también un arancel si ese bloque fue utilizado para certificar una transacción). El tamaño de la recompensa se reduce a medida que se van minando nuevas bitcoin en todo el mundo.

La dificultad de esta búsqueda también aumenta de manera que se vuelve computacionalmente cada vez más difícil encontrar una coincidencia. Estos dos efectos se combinan para reducir la tasa de producción de bitcoin a lo largo del tiempo, imitando así la producción de un material como el oro. Llegará un momento en que ya no se podrá producir nuevos bitcoin y el único incentivo que tendrán los mineros serán los aranceles pagados por transacción.<sup>11</sup>

Entonces el protocolo fue diseñado para que cada minero contribuya el poder de procesamiento de su computadora con el fin de mantener la infraestructura necesaria para respaldar y autenticar la red de la moneda. Los mineros reciben unidades de bitcoin recién generadas a cambio de haber contribuido poder de procesamiento para mantener la red y verificar transacciones en la cadena de bloques. Y a medida que se va dedicando más poder de procesamiento al minado, el protocolo irá incrementando la dificultad del problema matemático, de manera de garantizar que el minado de bitcoin se produzca siempre a un ritmo predecible y limitado.

Este proceso de minado de bitcoin no será infinito. Bitcoin fue diseñado para imitar la extracción de oro y otros metales preciosos de la tierra —solo podrá minarse una cantidad conocida y limitada de bitcoin. El número arbitrario elegido para ser el tope

---

11. Ken Tindell, “Geeks Love the Bitcoin Phenomenon Like They Loved the Internet in 1995,” *Business Insider*, 5 de abril de 2013, <http://www.businessinsider.com/how-bitcoins-are-mined-and-used-2013-4>.

es 21 millones de bitcoin. Se proyecta que los mineros extraerán meticulosamente el último “satoshi” o la 0.00000001 parte de un bitcoin en el año 2140. Cuando la capacidad de minado ascienda a determinado nivel alto, la dificultad de minar bitcoin se acrecentará tanto que extraer ese último satoshi va a ser una tarea digital extremadamente difícil. Una vez minado el último satoshi, los mineros que canalicen su procesamiento a la verificación de transacciones serán recompensados con tarifas por transacción en vez de bitcoin. Esto tiene el objeto de asegurarse que los mineros continúen teniendo un incentivo para mantener la red en funcionamiento tras la extracción del último bitcoin.

### Pseudonimidad

Los medios periodísticos han enfocado gran parte de su atención a la supuesta anonimidad que Bitcoin le brinda a sus usuarios. Sin embargo, esta idea surge de una mala comprensión de la verdadera naturaleza de la moneda.

Debido a que las transacciones realizadas por internet hasta hoy siempre han requerido un tercero intermediario, éstas no han sido anónimas. PayPal, por ejemplo, tiene un registro de cada vez que Alice le ha enviado dinero a Bob. Y debido a que las cuentas que Alice y Bob tienen en PayPal están vinculadas a sus respectivas cuentas bancarias, es muy probable que sus identidades sean conocidas. Por el contrario, si Alice le da un billete de \$100 a Bob, no hay intermediarios ni registros de la transacción. Y si Alice y Bob no conocen uno la identidad del otro, podemos decir que la transacción es completamente anónima.

Bitcoin se encuentra en algún lugar entre ambos extremos. Por un lado, los bitcoin son como el efectivo en el sentido que, una vez que Alice le da bitcoin a Bob, éstos dejan de estar en manos de ella y pasan a estar en posesión de él sin que haya participado ningún tercero intermediario que conozca la identidad de ambos. Por otro lado, a diferencia del efectivo, el hecho de que se produjo una transacción entre dos claves públicas, la hora, la

cantidad y otros datos quedan registrados en la cadena de bloque. De hecho, cada transacción que jamás se haya producido en la historia de la economía de bitcoin está a disposición pública en la cadena de bloques.<sup>12</sup>

Si bien las claves públicas de todas las transacciones —también conocidas como “direcciones de Bitcoin”<sup>13</sup>— quedan registradas en la cadena de bloques, esas claves públicas no están vinculadas a ninguna identidad. Si la identidad de una persona fuera vinculada a una clave pública, uno podría revisar las transacciones registradas en la cadena de bloques y ver con facilidad todas las transacciones asociadas con esa clave. Por lo tanto, si bien Bitcoin es muy similar al efectivo en el sentido en que las partes pueden realizar transacciones sin divulgar su identidad el uno al otro, se diferencia del efectivo en que es posible rastrear todas las transacciones enviadas hacia o desde una dirección de Bitcoin en particular. Es por esta razón que Bitcoin no es anónimo sino que es pseudónimo.

Vincular una identidad real a una dirección pseudónima de Bitcoin no es tan difícil como alguien podría imaginarse. Por un lado, la identidad de una persona (o al menos algún dato como puede ser la dirección del protocolo de internet) queda a menudo registrada cuando una persona realiza una transacción por Bitcoin en un sitio web o cuando cambia dólares por bitcoins en una casa de cambio de bitcoin. Para aumentar las probabilidades de permanecer anónimo, uno tendría que usar un software anonimizador como Tor y cuidarse de nunca realizar transacciones con dirección que puedan ser vinculadas a su identidad.

Finalmente, también es posible deducir las identidades simplemente estudiando la cadena de bloques. Un estudio demostró que, mediante técnicas de agrupamiento de la conducta transaccional, se pudo revelar las identidades del 40 por ciento de los usuarios

---

12. Nótese que esto podría ser de gran utilidad para los investigadores económicos.

13. *Bitcoin wiki*, s.v. “Address,” consultado el 30 de julio de 2013, <https://en.bitcoin.it/wiki/Address>.

de Bitcoin en un experimento simulado.<sup>14</sup> Un análisis temprano de las propiedades estadísticas del gráfico de transacciones de Bitcoin reveló cómo mediante un análisis pasivo de la red con las herramientas apropiadas se pudo divulgar la actividad financiera y las identidades de los usuarios de Bitcoin.<sup>15</sup> Un análisis posterior de las propiedades estadísticas del gráfico de transacciones de Bitcoin obtuvo resultados similares con una base de datos más grande.<sup>16</sup> Otro estudio del gráfico de transacciones de Bitcoin reiteró que quien utilice la técnica de “fusión de entidades”<sup>17</sup> podrá observar patrones estructurales en la conducta del usuario y enfatizó que este es “uno de los mayores retos para la anonimidad de Bitcoin”.<sup>18</sup> A pesar de esto, los usuarios de Bitcoin disfrutaban de un nivel de privacidad mucho más elevado que los usuarios de servicios de transferencia digital tradicionales, quienes deben proveer información personal detallada a los terceros intermediarios financieros que faciliten el intercambio.

Si bien con frecuencia se dice que bitcoin es una moneda “anónima”, la realidad es que es muy difícil permanecer anónimo en la red de Bitcoin. Los pseudónimos vinculados a las transacciones registradas en la bitácora pública pueden ser identificados incluso años después de que se haya completado

---

14. Elli Androulaki et al., “Evaluating User Privacy in Bitcoin,” *IACR Cryptology ePrint Archive* 596 (2012), <http://fc13.ifca.ai/proc/1-3.pdf>.

15. Fergal Reid y Martin Harrigan, “An Analysis of Anonymity in the Bitcoin System,” en *Security and Privacy in Social Networks*, ed. Yaniv Altshuler et al. (New York: Springer, 2013), <http://arxiv.org/pdf/1107.4524v2.pdf>.

16. Dorit Ron y Adi Shamir, “Quantitative Analysis of the Full Bitcoin Transaction Graph,” *IACR Cryptology ePrint Archive* 584 (2012), <http://eprint.iacr.org/2012/584.pdf>.

17. La fusión de entidades es el proceso de observar dos o más claves públicas utilizadas al mismo tiempo como input de una sola transacción. De esta forma, aun cuando un usuario tenga varias claves públicas diferentes, un analista puede ir vinculándolas en forma gradual y así eliminar la ostensible anonimidad que el uso de múltiples claves públicas parecería ofrecer.

18. Micha Ober, Stefan Katzenbeisser y Kay Hamacher, “Structure and Anonymity of the Bitcoin Transaction Graph,” *Future Internet* 5, no. 2 (2013), <http://www.mdpi.com/1999-5903/5/2/237>.

un intercambio. Una vez que los intermediarios de Bitcoin cumplan cabalmente con la normativa sobre secreto bancario a la que están sujetos todos los intermediarios financieros, será aún más difícil garantizar la anonimidad, ya que se exigirá a los intermediarios de Bitcoin que recojan información personal de cada uno de sus clientes.

## BENEFICIOS

LA PRIMERA PREGUNTA que mucha gente se hace al empezar a aprender sobre Bitcoin es ¿por qué usar bitcoin cuando puedo usar la moneda de mi país? El bitcoin es hoy una moneda cuyo valor fluctúa considerablemente y que todavía no es muy aceptada en muchos comercios, así que los usos de Bitcoin pueden parecer mayormente experimentales. Para comprender mejor por qué la gente desearía usar bitcoin, es de ayuda pensar en Bitcoin, no necesariamente como reemplazo de las monedas tradicionales, sino como un nuevo sistema de pagos.

### Costos transaccionales más bajos

Al no haber un tercero intermediario, las transacciones realizadas en la red Bitcoin son considerablemente menos costosas y más rápidas que en las redes tradicionales de pagos. Y porque las transacciones son más baratas, Bitcoin hace posible los micropagos y otras innovaciones. Además, Bitcoin ofrece la posibilidad de reducir costos a los pequeños comerciantes y el costo de las remesas transnacionales, aliviar la pobreza mundial al mejorar el acceso al capital, proteger a las personas contra los controles de capital y la censura, garantizar la privacidad financiera de los grupos oprimidos y generar innovación (dentro y por encima del protocolo de Bitcoin). Por otra parte, la naturaleza descentralizada de Bitcoin presenta oportunidades para el delito. El desafío es, entonces, desarrollar procesos que reduzcan las oportunidades criminales y a la vez mantengan los beneficios que Bitcoin ofrece.

En primer lugar, Bitcoin es atractivo para los pequeños comerciantes conscientes de los costos que siempre están a la búsqueda de maneras de reducir los costos transaccionales de operar un negocio. Las tarjetas de crédito han incrementado la facilidad de procesar pagos pero su uso ha venido acompañado de considerables costos para los comerciantes. Los comercios que desean ofrecer a sus clientes la opción de pagar con tarjetas de crédito deben primero pagar para obtener una cuenta comercial con cada empresa de tarjeta de crédito. Dependiendo de los términos y condiciones contractuales con cada una de ellas, los comerciantes deben pagar una gran variedad de aranceles por autorización, transacción, estados de cuenta, intercambio y servicio al cliente, entre otros. Estos aranceles se acumulan rápidamente y representan un elevado costo de operación. Sin embargo, si un comerciante deja de aceptar el pago en tarjeta para ahorrarse estos aranceles, perderá el volumen de negocio proveniente de clientes que disfrutan pagar con tarjetas.

Al permitir que las transacciones se procesen sin terceros intermediarios, Bitcoin elimina los altos cargos que acompañan la aceptación de tarjetas de crédito. El fondo de inversión Founder's Forum, liderado por Peter Thiel, conocido por sus inversiones en PayPal y Facebook, recientemente invirtió \$3 millones en la empresa procesadora de pagos Bitpay, porque el servicio de esa empresa tiene la capacidad de reducir los costos del comercio internacional por internet.<sup>19</sup> De hecho, muchos pequeños comerciantes ya han comenzado a aceptar bitcoin en un intento por reducir los costos de operar con las empresas de tarjetas de crédito.<sup>20</sup> Otros han adoptado la moneda por su velocidad y

---

19. Tom Simonite, "Bitcoin Hits the Big Time, to the Regret of Some Early Boosters," *MIT Technology Review*, 22 de mayo de 2013, <http://www.technologyreview.com/news/515061/bitcoin-hits-the-big-time-to-the-regret-of-some-early-boosters/>.

20. Gabrielle Karol, "Small Business Owners Say Bitcoins Better Than Credit Cards," *FOX Business, Small Business Center*, 12 de abril de 2013, <http://smallbusiness.foxbusiness.com/entrepreneurs/2013/04/12/small-business-owners-say-bitcoins-better-than-credit-cards/>.

eficiencia en facilitar transacciones.<sup>21</sup> Es probable que Bitcoin continúe reduciendo los costos operativos de los comercios a medida que el público comience a adoptar la moneda.

Aceptar pagos con tarjeta de crédito expone a los comerciantes el riesgo de reversión fraudulenta de transacciones. Los comerciantes han sufrido durante mucho tiempo este tipo de fraude que se produce cuando los clientes falsamente reclaman un reembolso alegando que un producto no ha sido entregado.<sup>22</sup> Esto los expone no solo a perder el pago y el producto mismo, sino a penalidades financieras por la reversión del pago. Al ser un sistema de pagos irreversibles, Bitcoin elimina el “fraude amistoso” causado por el uso indebido de los reembolsos reclamados por el consumidor. Esto es de gran importancia para los comerciantes.

Sin embargo, al consumidor le gusta el sistema de reembolsos porque este lo protege de comerciantes inescrupulosos y de errores operativos. El consumidor puede además disfrutar de otros beneficios financiados con los aranceles cobrados al comerciante. De hecho, es probable que muchos consumidores y comerciantes prefieran el sistema tradicional de tarjetas de crédito aun cuando esté disponible la opción de utilizar Bitcoin. Sin embargo, la existencia de opciones de pago beneficiaría a consumidores de todas las preferencias.

Quienes deseen la protección y los beneficios de utilizar tarjetas de crédito pueden continuar usándolas, aun cuando deban pagar un poco más. Quienes sean más protectores de sus costos y su privacidad, pueden usar Bitcoin. No tener que pagar aranceles

---

21. Bailey Reutzell, “Why Some Merchants Accept Bitcoin Despite the Risks,” *Payments Source*, 21 de mayor de 2013, <http://www.paymentsource.com/news/why-some-merchants-accept-bitcoin-despite-the-risks-3014183-1.html>.

22. Emily Maltby, “Chargebacks Create Business Headaches,” *Wall Street Journal*, 10 de febrero de 2011, <http://online.wsj.com/article/SB10001424052748704698004576104554234202010.html>. Un ejemplo de este tipo de fraudes sería el caso de que Alice le envíe a Bob un pago a través de PayPal por una computadora que Bob listó en Craigslist. Alice viene a la casa de Bob a recogerla, se lleva la computadora y al poco tiempo inicia una solicitud de cancelación (es decir, exige que el pago se revierta). PayPal por lo general exige prueba de envío antes de revertir una transacción y al poder proveerla, Bob es víctima del fraude.

comerciales significa que los comerciantes que acepten Bitcoin tienen la opción de trasladar esos ahorros a los consumidores. Este es el modelo de negocio de Bitcoin Store,<sup>23</sup> que vende miles de productos electrónicos a precios descontados y solo acepta bitcoin. La misma tableta Galaxy Note que se vende en Amazon por \$779 más gastos de envío<sup>24</sup> se vende en Bitcoin Store por solo \$480.<sup>25</sup> De esta manera, Bitcoin ofrece más opciones de bajo costo para quienes busquen gangas y para pequeños comerciantes sin restarle a los servicios de tarjeta de crédito tradicionales que algunos consumidores prefieren.

Como sistema de transmisión de dinero a bajo costo, Bitcoin también promete grandes beneficios. En 2012, los inmigrantes a países desarrollados enviaron al menos \$401,000 millones en remesas familiares a sus parientes residentes en países en vías de desarrollo.<sup>26</sup> Se proyecta que el volumen de remesas ascienda a \$515,000 millones en 2015.<sup>27</sup> La mayoría de estas remesas se envían a desde puntos de venta físicos a través de empresas de envío de dinero tradicionales tales como Western Union o MoneyGram, quienes cobran altos aranceles por el servicio y pueden llegar

---

23. Vitalik Buterin, "Bitcoin Store Opens: All Your Electronics Cheaper with Bitcoins," *Bitcoin Magazine*, 5 de noviembre de 2012, <http://bitcoinmagazine.com/bitcoin-store-opens-all-your-electronics-cheaper-with-bitcoins/>.

24. Oferta de Amazon de una tableta Samsung Galaxy Note, consultada el 29 de mayo de 2013, <http://amzn.com/B00BJXNGIK>.

25. Oferta de Bitcoin Store de una tableta Samsung Galaxy Note, consultada el 29 de mayo de 2013, <https://www.bitcoinstore.com/samsung-galaxy-note-gt-n8013-10-1-32-gb-tablet-wi-fi-1-40-ghz-deep-gray.html>. Los precios de los productos del Bitcoin Store están publicados tanto en bitcoin como en dólares estadounidenses. Al momento de la compra, Bitpay, una empresa de procesamiento de pagos en Bitcoin, determina la tasa de cambio y la reserva durante 15 minutos. Véase las preguntas y respuestas del Bitcoin Store: <https://www.bitcoinstore.com/faq>.

26. World Bank Payment Systems Development Group, *Remittance Prices Worldwide: An Analysis of Trends in the Average Total Cost of Migrant Remittance Services* (Washington, DC: World Bank, 2013), <http://remittanceprices.worldbank.org/-/media/FPDKM/Remittances/Documents/RemittancePriceWorldwide-Analysis-Mar2013.pdf>.

27. Ibid.



a tardar varios días en entregar los fondos en el destino.<sup>28</sup> En el primer trimestre de 2013, el arancel global promedio por enviar remesas ascendía a 9.05 por ciento.<sup>29</sup> Por el contrario, los aranceles en la red de Bitcoin ascienden a menos de 0.0005 BTC,<sup>30</sup> o el 1 por ciento de la transacción.<sup>31</sup> Esta oportunidad de negocio de mejorar el servicio de envío de dinero ha atraído capital de fondos de inversión de gran renombre.<sup>32</sup> Incluso MoneyGram y Western Union están considerando si integrar Bitcoin a sus modelos de negocio.<sup>33</sup> Bitcoin permite realizar remesas de manera instantánea y a bajo costo y la reducción del costo total de las remesas para los consumidores podría ser significativa.

Potencial de combatir la pobreza y la opresión

Bitcoin también tiene el potencial de mejorar la calidad de vida de los más pobres del mundo. Mejorar el acceso básico a servicios financieros es una técnica antipobreza de gran promesa.<sup>34</sup> Según un cálculo, el 64 por ciento de la gente que vive en países en vías de desarrollo no tiene acceso a estos servicios, quizás porque es muy costoso para las instituciones financieras tradicionales ofrecer sus

---

28. Jessica Silver-Greenberg, "New Rules for Money Transfers, but Few Limits," *New York Times*, 1 de junio de 2012, [http://www.nytimes.com/2012/06/02/business/new-rules-for-money-transfers-but-few-limits.html?pagewanted=all&\\_r=0](http://www.nytimes.com/2012/06/02/business/new-rules-for-money-transfers-but-few-limits.html?pagewanted=all&_r=0).

29. World Bank, *Remittance Prices*.

30. *Bitcoin wiki*, s.v. "Transaction fees," consultada el 30 de Julio de 2013, [https://en.bitcoin.it/wiki/Transaction\\_fees](https://en.bitcoin.it/wiki/Transaction_fees).

31. Andrew Paul, "Is Bitcoin the Next Generation of Online Payments?," *Yahoo! Small Business Advisor*, 24 de mayo de 2013, <http://smallbusiness.yahoo.com/advisor/bitcoin-next-generation-online-payments-213922448--finance.html>.

32. Simonite, "Bitcoin Hits the Big Time."

33. Andrew R. Johnson, "Money Transfers in Bitcoins? Western Union, MoneyGram Weigh the Option," *Wall Street Journal*, 18 de abril de 2013, <http://online.wsj.com/article/SB10001424127887324493704578431000719258048.html>.

34. Muhammad Yunus, *Banker to the Poor: Micro-lending and the Battle against World Poverty* (New York: Public Affairs, 2003).

servicios en áreas pobres y rurales.<sup>35</sup> Debido a los impedimentos a desarrollar sucursales bancarias tradicionales en áreas pobres, los habitantes de países en vías de desarrollo han debido recurrir a servicios bancarios móviles para satisfacer sus necesidades financieras. El sistema cerrado móvil de pagos M-Pesa ha tenido particular éxito en países como Kenia, Tanzania y Afganistán.<sup>36</sup> Los emprendedores ya se están enfocando en este modelo; el servicio de billetera de Bitcoin Kipochi desarrolló recientemente un producto que permite a los usuarios de M-Pesa intercambiar bitcoin.<sup>37</sup> Los servicios de banca móvil de los países en vías de desarrollo pueden mejorarse aún más con la adopción de Bitcoin. Como sistema abierto de pagos, Bitcoin puede ofrecer a los habitantes de estos países acceso a servicios financieros de bajo costo a escala global.

Bitcoin también puede proporcionar asistencia a los habitantes de países que estén sujetos a estrictos controles de capital. El total de bitcoin que puede ser minado está limitado y no puede ser manipulado. No existe en Bitcoin una autoridad central que pueda revertir transacciones o impedir el intercambio de bitcoin entre países. Por lo tanto, Bitcoin ofrece una escotilla de escape para quienes deseen una alternativa a la devaluación de la moneda o congelación del mercado de capitales de sus países. Ya hemos visto ejemplos de cómo la gente recurre a Bitcoin para evadir los nocivos efectos del control de capitales y la mala administración de sus bancos centrales. Algunos argentinos, por ejemplo, han adoptado Bitcoin en respuesta a la doble carga que en el país representan una tasa del 25 por

---

35. Oya Pinar Ardic, Maximilien Heimann y Nataliya Mylenko, "Access to Financial Services and the Financial Inclusion Agenda around the World" (Policy Research Working Paper, World Bank Financial and Private Sector Development Consultative Group to Assist the Poor, 2011), <https://openknowledge.worldbank.org/bitstream/handle/10986/3310/WPS5537.pdf>.

36. Jeff Fong, "How Bitcoin Could Help the World's Poorest People," *PolicyMic*, mayo de 2013, <http://www.policymic.com/articles/41561/bitcoin-price-2013-how-bitcoin-could-help-the-world-s-poorest-people>.

37. Emily Spaven, "Kipochi launches M-Pesa Integrated Bitcoin Wallet in Africa," *CoinDesk*, 19 de julio de 2013, <http://www.coindesk.com/kipochi-launches-m-pesa-integrated-bitcoin-wallet-in-africa/>.

ciento de inflación y estrictos controles cambiarios.<sup>38</sup> La demanda de bitcoin es tan fuerte en Argentina que un popular cambiador de moneda virtual está planeando abrir una oficina en Argentina.<sup>39</sup> El uso de Bitcoin en Argentina continúa en crecimiento debido a la mala administración del sistema cambiario local.<sup>40</sup>

Quienes se encuentren en situaciones de opresión o emergencia también podrían beneficiarse de la privacidad financiera que Bitcoin ofrece. Existen muchas razones legítimas por las que uno deseara buscar privacidad en sus transacciones financieras. Un cónyuge envuelto en una situación abusiva puede necesitar gastar dinero discretamente. Una persona que desee acceder a un servicio de salud controvertido podría buscar privacidad financiera con el fin de evitar que sus familiares, empleadores u otros juzguen sus decisiones. Recientes experiencias con gobiernos despóticos sugieren que los ciudadanos oprimidos podrían beneficiarse en gran medida con la posibilidad de realizar transacciones privadas fuera del alcance de las garras de los tiranos. Bitcoin ofrece parte de la privacidad que hemos disfrutado tradicionalmente con el uso del efectivo —además de la conveniente posibilidad de la transferencia digital.

#### Estímulo para la innovación financiera

Una de las más prometedoras posibilidades que Bitcoin ofrece es como plataforma para la innovación financiera. El protocolo de Bitcoin contiene el modelo digital para el desarrollo de una serie de servicios financieros y legales que los programadores pueden desarrollar con facilidad. Debido a que los bitcoin son, en esencia,

---

38. Jon Matonis, “Bitcoin’s Promise in Argentina,” *Forbes*, 27 de abril de 2013, <http://www.forbes.com/sites/jonmatonis/2013/04/27/bitcoins-promise-in-argentina/>.

39. Camila Russo, “Bitcoin Dreams Endure to Savers Crushed by CPI: Argentina Credit,” *Bloomberg*, 6 de abril de 2013, <http://www.bloomberg.com/news/2013-04-16/bitcoin-dreams-endure-to-savers-crushed-by-cpi-argentina-credit.html>.

40. Georgia Wells, “Bitcoin Downloads Surge in Argentina,” *Wall Street Journal Money Beat*, 17 de julio de 2013, <http://blogs.wsj.com/moneybeat/2013/07/17/bitcoin-downloads-surge-in-argentina/>.

simples paquetes de datos, se los puede utilizar para transferir no solo valor monetario sino también acciones, apuestas e información sensible.<sup>41</sup> Algunas de las características funcionales que están incorporadas en el protocolo de Bitcoin incluyen los micro-pagos, la mediación de disputas, los contratos de garantía y las propiedades inteligentes.<sup>42</sup> Estas funciones permitirían el desarrollo simple de servicios de traducción por internet, el procesamiento instantáneo de pequeñas transacciones (como la medición automática del acceso a WiFi) y servicios de acopio público de financiación del tipo de Kickstarter.

Además, los programadores tienen la posibilidad de desarrollar protocolos alternativos por encima del protocolo de Bitcoin de la misma manera que la red y el correo electrónico funcionan encima del protocolo de internet conocido como TCP/IP. Un programador ya ha propuesto una nueva capa de protocolo para ser incorporada por encima del protocolo de Bitcoin que mejora la estabilidad y seguridad de la red.<sup>43</sup> Otro programador creó un servicio digital de escribanía para almacenar de manera anónima y segura una “prueba de existencia” para documentos privados por encima del protocolo de Bitcoin.<sup>44</sup> Otros programadores han

---

41. Jerry Brito, “The Top 3 Things I Learned at the Bitcoin Conference,” *Reason*, 20 de mayo de 2013, <http://reason.com/archives/2013/05/20/the-top-3-things-i-learned-at-the-bitcoin>.

42. Mike Hearn, “Bitcoin 2012 London: Mike Hearn,” YouTube video, 28:19, subido por “QueuePolitely,” 27 de septiembre de 2012, <http://www.youtube.com/watch?v=mD4L7xDNCmA>. La propiedad inteligente es un concepto que permite controlar la propiedad de un objeto a través de contratos realizados en la cadena de bloques de Bitcoin. La propiedad inteligente le permite a la gente intercambiar la propiedad de un bien o servicio una vez que se haya dado una condición utilizando criptografía. Si bien la propiedad inteligente es todavía un concepto teórico, el mecanismo básico se encuentra incorporado en el protocolo de Bitcoin. Véase *Bitcoin wiki*, s.v., “Smart Property,” consultado el 30 de julio de 2013, [https://en.bitcoin.it/wiki/Smart\\_Property](https://en.bitcoin.it/wiki/Smart_Property).

43. J. R. Willett, “The Second Bitcoin Whitepaper” (white paper, 2013), <https://sites.google.com/site/2ndbtcpwaper/2ndBitcoinWhitepaper.pdf>.

44. Jeremy Kirk, “Could the Bitcoin Network Be Used as an Ultrasecure Notary Service?,” *ComputerWorld*, 23 de mayo de 2013, [http://www.computerworld.com/s/article/9239513/Could\\_the\\_Bitcoin\\_network\\_be\\_used\\_as\\_an\\_ultrasecure\\_notary\\_service...](http://www.computerworld.com/s/article/9239513/Could_the_Bitcoin_network_be_used_as_an_ultrasecure_notary_service...)

adoptado el modelo de Bitcoin con el fin de encriptar comunicaciones de correo electrónico.<sup>45</sup> Otro grupo de desarrolladores ha delineado un protocolo adicional que mejorará la privacidad de la red.<sup>46</sup> Bitcoin constituye entonces el cimiento sobre el que se pueden construir estratos adicionales de funcionalidad. La mejor manera de concebir el proyecto Bitcoin es como un proceso de experimentación financiera y de comunicaciones. Los legisladores deben tomar la precaución de que sus directivas no sofoquen las prometedoras innovaciones que se están desarrollando dentro y por encima de este incipiente protocolo.

## DESAFÍOS

A PESAR DE los muchos beneficios que presenta, Bitcoin también tiene aspectos negativos que sus usuarios potenciales deben tomar en consideración. Por ejemplo, el valor de bitcoin ha exhibido una considerable volatilidad a lo largo de su existencia y los nuevos usuarios corren el riesgo de no proteger adecuadamente e incluso perder accidentalmente sus bitcoin si no toman ciertas precauciones. Además, existen preocupaciones acerca de si la piratería informática puede poner en peligro la economía de bitcoin.

### Volatilidad

Bitcoin ha soportado al menos cinco ajustes de precio importantes desde el 2011.<sup>47</sup> Estos ajustes se asemejan a las burbujas especulativas tradicionales: una cobertura mediática excesivamente

---

45. Jonathan Warren, "Bitmessage: A Peer-to-Peer Message Authentication and Delivery System" (white paper, 27 de noviembre de 2012), <https://bitmessage.org/bitmessage.pdf>.

46. Ian Miers et al., "Zerocoin: Anonymous Distributed E-Cash from Bitcoin" (working paper, the Johns Hopkins University Department of Computer Science, Baltimore, MD, 2013), <http://spar.isi.jhu.edu/~mgreen/ZerocoinOakland.pdf>.

47. Timothy B. Lee, "An Illustrated History of Bitcoin Crashes," *Forbes*, 11 de abril de 2013, <http://www.forbes.com/sites/timothylee/2013/04/11/an-illustrated-history-of-bitcoin-crashes/>.

optimista de Bitcoin impulsa a inversionistas novatos a inflar los precios de Bitcoin.<sup>48</sup> La euforia llega a un punto de inflexión y el valor termina por desplomarse en algún momento. Ansiosos por participar, los nuevos inversionistas corren el riesgo de sobrevaluar la moneda y perder su inversión en una crisis económica. El fluctuante valor de Bitcoin ha hecho que muchos observadores se muestren escépticos respecto del futuro de la moneda.

¿Profetiza esta volatilidad el fin de Bitcoin? Algunos comentaristas opinan que sí.<sup>49</sup> Otros sugieren que estas fluctuaciones están probando la resistencia de la moneda y podrían en el futuro reducir su frecuencia a medida que se desarrollen mecanismos para contrarrestar la volatilidad.<sup>50</sup> Si los bitcoin se utilizaran solo como medio para almacenar valor o como unidades contables, la volatilidad de la moneda podría de hecho poner en peligro su futuro. No tiene sentido administrar las finanzas de un negocio o conservar los ahorros en bitcoin si el precio de mercado de la moneda fluctúa de manera volátil e impredecible. Sin embargo, cuando se utiliza a Bitcoin como medio de intercambio, la volatilidad es un problema menor.<sup>51</sup> El comerciante puede tasar el valor al consumidor de sus productos y servicios en moneda tradicional y aceptar como pago el equivalente en bitcoin. Al consumidor que compre bitcoin para realizar una compra por única vez no le importa cuál va a ser la tasa de cambio mañana; solamente le interesa que Bitcoin puede reducir el costo de la transacción hoy. La utilidad de Bitcoin como medio de intercambio podría explicar por qué la

---

48. Felix Salmon, "The Bitcoin Bubble and the Future of Currency," *Medium*, 3 de abril de 2013, <https://medium.com/money-banking/2b5ef79482cb>.

49. Maureen Farrell, "Strategist Predicts End of Bitcoin," *CNNMoney*, 14 de mayo de 2013, <http://money.cnn.com/2013/05/14/investing/bremmer-bitcoin/index.html>.

50. Adam Gurri, "Bitcoins, Free Banking, and the Optional Clause," *Ümlaut*, 6 de mayo de 2013, <http://theumlaut.com/2013/05/06/bitcoins-free-banking-and-the-optional-clause/>.

51. Jerry Brito, "Why Bitcoin's Valuation Really Doesn't Matter," *Technology Liberation Front*, 5 de abril de 2013, <http://techliberation.com/2013/04/05/why-bitcoins-valuation-doesnt-really-matter/>.

moneda ha crecido en popularidad entre los comerciantes a pesar de su volatilidad.<sup>52</sup> También es posible que el valor de los bitcoin se vuelva menos volátil a medida que más gente se familiarice con la tecnología de Bitcoin y desarrolle expectativas realistas acerca de su futuro.

### Violaciones a la seguridad

Como moneda digital, Bitcoin presenta ciertos retos específicos relacionados con la seguridad.<sup>53</sup>

Si el usuario no toma precauciones, puede borrar o extraviar sus bitcoin involuntariamente. Una vez perdido el archivo digital, perdido está el dinero, tal como sucede con el efectivo. Si el usuario no protege sus direcciones de Bitcoin privadas, se expone además al riesgo de hurto. Las billeteras de Bitcoin ya ofrecen protección a través de encriptación, pero el usuario debe elegir activar dicha encriptación. Si no lo hace, los bitcoin están sujetos a hurto a través de software malicioso.<sup>54</sup> Los cambiadores de Bitcoin, también han sufrido fallas de seguridad; en 2012, piratas informáticos hurtaron con éxito 24,000 BTC (\$250,000 al precio de agosto de 2013) de una casa de cambio digital llamada Bitfloor<sup>55</sup> y organizó un masivo ataque distribuido de denegación de servicio

---

52. En la actualidad, los proveedores de servicios a comerciantes aceptan el riesgo presentado por la volatilidad y sin embargo mantienen los aranceles en niveles bajos. Queda por verse si este modelo será sostenible en el largo plazo.

53. La mayoría de los desafíos de seguridad se relacionan con las billeteras y as casas de cambio digitales. El protocolo mismo ha demostrado ser considerablemente resistente a la piratería y a los riesgos de seguridad informática. El renombrado especialista en seguridad Dan Kaminsky intentó, en vano, violar el acceso al protocolo de Bitcoin en 2011. Véase Dan Kaminsky, "I Tried Hacking Bitcoin and I Failed," *Business Insider*, 12 de abril de 2013, <http://www.businessinsider.com/dan-kaminsky-highlights-flaws-bitcoin-2013-4>.

54. Stephen Doherty, "All Your Bitcoins Are Ours . . .," *Symantec Blog*, 16 de junio de 2011, <http://www.symantec.com/connect/blogs/all-your-bitcoins-are-ours>.

55. Devin Coldewey, "\$250,000 Worth of Bitcoins Stolen in Net Heist," *NBC News*, 5 de septiembre de 2012, <http://www.nbcnews.com/technology/250-000-worth-bitcoins-stolen-net-heist-980871>.

(en inglés, DDoS) contra la popular casa de cambio Mt. Gox en 2013.<sup>56</sup> (Bitfloor posteriormente regresó los fondos robados a sus clientes y Mt. Gox logró recuperarse de los ataques.) Por supuesto, muchos de los riesgos informáticos que enfrenta Bitcoin son similares a los que enfrentan las monedas tradicionales. Los billetes de dólar pueden ser destruidos o robados, la información financiera personal puede ser hurtada y utilizada por los delincuentes y los bancos pueden ser objeto de robos y ataques de DDoS. Los usuarios de Bitcoin deben preocuparse por aprender acerca de los riesgos y tomar las precauciones necesarias de la misma manera que lo hacen hoy para proteger sus actividades financieras.

### Usos criminales

Existen también razones por las que los legisladores han expresado preocupación por algunos de los usos alternativos que se le puede dar a Bitcoin. Al ser Bitcoin pseudónimo, los legisladores y periodistas han cuestionado si los delincuentes podrían utilizarlo para lavar dinero y aceptar pagos por la compraventa de mercaderías o servicios ilícitos. De hecho, al igual que al efectivo, se lo puede utilizar tanto para el bien como para el mal.

Por ejemplo, podemos explorar el infame mercado negro de la web profunda<sup>57</sup> conocido como “Silk Road” (o ruta de la seda). Silk Road aprovecha la red de anonimización Tor y la naturaleza pseudónima de Bitcoin para proporcionar un vasto mercado donde es posible comprar por correo drogas y otros productos ilícitos. Aunque los administradores de Silk Road no permiten el intercambio de ninguna mercadería que provenga de un fraude o daño, como por ejemplo el uso de tarjetas de crédito robadas o fotografías pedofílicas, permite a los comerciantes vender productos ilícitos

---

56. Meghan Kelly, “Fool Me Once: Bitcoin Exchange Mt.Gox Falls after Third DDoS Attack This Month,” *VentureBeat*, 21 de abril de 2013, <http://venturebeat.com/2013/04/21/mt-gox-ddos/>.

57. *Wikipedia*, s.v. “Deep Web,” consultada el 30 de julio 2013, [http://en.wikipedia.org/wiki/Deep\\_Web](http://en.wikipedia.org/wiki/Deep_Web).



tales como documentos de identidad falsificados y drogas ilegales. La naturaleza pseudónima de Bitcoin les permite a los compradores comprar estos productos por internet de la misma manera que el efectivo tradicionalmente ha permitido comprar productos similares en persona. Un estudio calculó que el volumen total de transacciones de Silk Road asciende a aproximadamente \$1,2 millones,<sup>58</sup> pero el volumen total acumulado en la economía de Bitcoin en junio de 2013 ascendió a \$770 millones. Por lo tanto, las ventas de Silk Road representan una proporción insignificante dentro de la economía total de bitcoin.<sup>59</sup>

La asociación de Bitcoin con Silk Road ha manchado su reputación. Tras la publicación de un artículo sobre Silk Road en 2011,<sup>60</sup> los senadores Charles Schumer y Joe Manchin les enviaron cartas al Procurador General Eric Holder y a Michelle Leonhart, responsable de la Administración Federal del Control de Drogas solicitando la toma de medidas en contra de Silk Road, el software de anonimización Tor y Bitcoin.<sup>61</sup>

Otra de las preocupaciones es que Bitcoin pueda ser utilizado para lavar dinero, financiar el terrorismo y el tráfico de mercancías ilegales. Si bien estas preocupaciones son la actualidad más teóricas que basadas en casos reales, Bitcoin podría ser una opción para quienes deseen mover con discreción dinero obtenido ilegítimamente. Las preocupaciones acerca del potencial de Bitcoin para lavar dinero se vieron avivadas tras el cierre de Liberty Reserve,

---

58. Nicolas Christin, "Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace," *Carnegie Mellon CyLab Technical Reports: CMU-CyLab-12-018*, 30 de Julio de 2012 (actualizado el 28 de noviembre de 2012), [http://www.cylab.cmu.edu/files/pdfs/tech\\_reports/CMUCyLab12018.pdf](http://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab12018.pdf).

59. Jerry Brito, "National Review Gets Bitcoin Very Wrong," *Technology Liberation Front*, 20 de junio de 2013, <http://techliberation.com/2013/06/20/national-review-gets-bitcoin-very-wrong/>.

60. Adrian Chen, "The Underground Website Where You Can Buy Any Drug Imaginable," *Gizmodo*, 1 de junio de 2011, <http://gawker.com/5805928/the-underground-website-where-you-can-buy-any-drug-imaginable>.

61. Brett Wolf, "Senators Seek Crackdown on 'Bitcoin' Currency," *Reuters*, 8 de junio de 2011, <http://www.reuters.com/article/2011/06/08/us-financial-bitcoins-idUSTRE7573T320110608>.

un servicio privado y centralizado de moneda digital con oficinas en Costa Rica, por parte de las autoridades de EE. UU., que iniciaron acciones penales por lavado de dinero.<sup>62</sup>

Si bien Liberty Reserve y Bitcoin parecen similares debido a que ambos ofrecen monedas digitales, existen importantes diferencias entre ambos. Liberty Reserve era un servicio de moneda centralizado cuyo dueño y creador era una empresa privada, presuntamente con el propósito expreso de facilitar el lavado de dinero. Bitcoin no lo es. Las transacciones que se realizaban dentro de la economía de Liberty Reserve no eran transparentes. De hecho, Liberty Reserve les prometía a sus clientes total anonimidad. Bitcoin, por el contrario, es una moneda abierta descentralizada que ofrece un registro público de todas las transacciones. Un lavador de dinero podrá intentar proteger su identidad y sus direcciones de Bitcoin, pero los registros de sus transacciones siempre serán públicos y accesibles en cualquier momento por las autoridades. Por ello, lavar dinero a través de Bitcoin puede considerarse como una tarea mucho más riesgosa que utilizar un sistema centralizado como el de Liberty Reserve. Además, varias casas de cambio digitales han tomado medidas para cumplir con los requisitos legales para la prevención del lavado de dinero, incluido el mantenimiento de registros y la realización de informes.<sup>63</sup> Es probable, entonces, que la combinación de un sistema de registro público y la cooperación de las casas de cambio en recoger información sobre sus clientes hagan de Bitcoin una opción menos atractiva para el lavado de dinero, en comparación con las monedas virtuales privadas y anónimas.

Cabe destacar, además, que muchos de los aspectos negativos potenciales de Bitcoin son los mismos que caracterizan al tradicional efectivo. El efectivo ha sido históricamente el vehículo preferido de los traficantes de drogas y lavadores de dinero, pero los

---

62. "Liberty Reserve Digital Money Service Forced Offline," *BBC News—Technology*, 27 de mayo de 2013, <http://www.bbc.co.uk/news/technology-22680297>.

63. Jeffrey Sparshott, "Bitcoin Exchange Makes Apparent Move to Play by U.S. Money-Laundering Rules," *Wall Street Journal*, 28 de junio de 2013, <http://online.wsj.com/article/SB10001424127887323873904578574000957464468.html>.

legisladores nunca considerarían seriamente prohibir el efectivo. A medida que los supervisores financieros comienzan a contemplar a Bitcoin, deberían actuar con cautela y cuidarse de los riesgos de la sobre-reglamentación. En el peor de los casos, podrían llegar a evitar que negocios legítimos se beneficien de la red de Bitcoin sin que las normativa tenga efecto alguno en prevenir el uso de bitcoin por parte de lavadores y narcotraficantes. Si las casas de cambio digitales se ven tan abrumadas por la carga normativa que tienen que cerrar, por ejemplo, los lavadores de dinero y narcotraficantes podrían seguir inyectando dinero en la red mediante el pago de efectivo a una persona para que les transfiera bitcoin a sus billeteras virtuales. En este escenario, las transacciones beneficiosas se ven impedidas debido al exceso de reglamentación, mientras que las actividades que se perseguía atacar continúan realizándose. El desafío para los legisladores y supervisores es buscar la manera de desarrollar un sistema de supervisión que mitigue el doble riesgo del lavado de dinero y las compras ilegales sin sofocar los beneficios que Bitcoin está preparado para brindar a los usuarios legítimos en sus vidas cotidianas.

## REGLAMENTACIÓN Y SUPERVISIÓN

LAS LEYES Y normas que están hoy en vigor no pudieron haber concebido una tecnología como la de Bitcoin, así que éste existe en una especie de zona gris jurídica. Esto se debe en gran medida a que Bitcoin no encaja exactamente en ninguna de las definiciones jurídicas de moneda u otro institución o instrumento financiero, lo cual dificulta establecer a qué leyes y de qué manera está sujeto.

Esa situación nos recuerda la incertidumbre normativa en la que estuvieron otras nuevas tecnologías tales como la voz sobre protocolo de internet (en inglés, VoIP).<sup>64</sup> Cuando apareció por

---

64. Sam Rozenfeld, "FCC'S VoIP Regulation Dilemma," *Telephony Your Way*, 30 de abril de 2011, <http://www.telephonyyourway.com/2011/04/30/fccs-voip-regulation-dilemma/>.

primera vez la VoIP, la Ley de Comunicaciones y la normativa de la Comisión Federal de Comunicaciones de EE. UU. (en inglés, FCC) solo contemplaban las comunicaciones de voz sobre el sistema público tradicional de redes telefónicas con interruptor. Al igual que Bitcoin, la VoIP competía con una red preexistente altamente reglamentada y era menos costosa y a menudo de persona a persona. Hasta el día de hoy el Congreso y la FCC continúan lidiando con cuestiones de reglamentación, incluidas qué obligaciones de interés público debería requerirse de los operadores de VoIP y si éstos deben o no cumplir con las solicitudes de intervención de comunicaciones formuladas por las autoridades.

Sin embargo, afortunadamente, el Congreso y la FCC han trazado un camino para al VoIP que ha aclarado gran parte de la ambigüedad normativa sin sobrecargar a la nueva tecnología con la pesada normativa preexistente que estado dirigida a los monopolios telefónicos. Como consecuencia, la VoIP ha prosperado como tecnología, ha facilitado el ingreso de competidores a un mercado que antes estaba estancado y ha reducido los costos y mejorado el acceso para el consumidor. Sería deseable que los legisladores buscaran lograr el mismo resultado con Bitcoin.

Bitcoin tiene las propiedades de un sistema electrónico de pagos, de una moneda, de un bien, entre otras cosas. Por ello, es probable que reciba el escrutinio de distintas agencias de supervisión. Abajo resumimos algunas de las cuestiones que deberán resolver estas agencias a medida que vayan preparándose para reglamentar a Bitcoin.

¿Son legales las monedas privadas?

Una de las primeras preguntas iniciales sobre Bitcoin ha sido si la moneda digital es legal, dado el monopolio que el gobierno federal tiene sobre la emisión de moneda de curso legal. Parece que la respuesta es afirmativa. La Constitución de EE. UU. sólo prohíbe

a los estados acuñar moneda.<sup>65</sup> Las monedas emitidas en forma privada no están prohibidas y de hecho hay hoy una gran cantidad de monedas locales en circulación.<sup>66</sup> Con el fin de promover las economías locales, tanto empresarios como legisladores han desarrollado varias monedas alternativas en los últimos años, como la Cascadia Hour Exchange en Portland y los Life Dollars en Bellingham, Washington.<sup>67</sup>

Lo que los privados no pueden hacer es emitir moneda que se parezca a la de los EE. UU.<sup>68</sup> Un tristemente célebre caso es el de Bernard von NotHaus, quien fue condenado en 2011 por imprimir y distribuir una moneda respaldada por el oro denominada “Liberty Dollar”. El delito que cometió no fue emitir una moneda alternativa, sino crear una moneda que se parecía mucho al dólar estadounidense e intentar ponerlo en circulación como si fueran dólares, alentando a otros a hacer lo mismo.<sup>69</sup> A diferencia del Liberty Dollar, Bitcoin no corre el peligro de ser confundido con el dólar estadounidense.

Leyes sobre transmisión de dinero

En EE. UU., una empresa que transmite fondos de una persona a otra es un transmisor de dinero y debe obtener una licencia en 48 estados y en el Distrito de Columbia para poder operar como tal.<sup>70</sup> Los transmisores de dinero están sujetos a la Ley de Secreto

---

65. U.S. Const. art I § 10.

66. U.S. Const. art I § 10.

67. Blake Ellis, “Local Currencies: ‘In the U.S. We Don’t Trust,’” *CNN Money*, 27 de enero de 2012, [http://money.cnn.com/2012/01/17/pf/local\\_currency/index.htm](http://money.cnn.com/2012/01/17/pf/local_currency/index.htm).

68. 18 U.S.C. §§ 485 and 486.

69. Grinberg, “Bitcoin,” 193n158.

70. *Hearing on the Regulation of Non-bank Money Transmitter—Money Services Businesses*, 112th Congress (2012) (declaración de Ezra C. Levine), testimonio ante el Subcommittee on Financial Institutions and Consumer Credit of the House Committee on Financial Services, [http://financialservices.house.gov/uploaded\\_files/hhrg-112-ba15-wstate-elevine-20120621.pdf](http://financialservices.house.gov/uploaded_files/hhrg-112-ba15-wstate-elevine-20120621.pdf).

Bancario (en inglés, BSA) conforme a su reglamentación por parte de FinCEN. Además, la Ley USA PATRIOT Act convirtió en delito penal operar un negocio de transmisión de dinero sin licencia.<sup>71</sup>

El propósito del licenciamiento de los transmisores de dinero por parte de los Estados ha sido históricamente la protección al consumidor.<sup>72</sup> Debido a que los transmisores de dinero (o los emisores de giros postales) no suelen ser bancos asegurados por la Corporación para el Aseguramiento de los Depósitos (en inglés, FDIC), el consumidor puede quedar desamparado si un transmisor de dinero no cumple con la obligación de entregar los fondos al beneficiario por él designado. El licenciamiento intenta minimizar este riesgo. El licenciamiento de transmisores de dinero por los Estados se generalizó tras una serie de fallas en empresas de giros postales que recibió amplia cobertura periodística en los años 80.<sup>73</sup>

La BSA, por otra parte, busca evitar o detectar el lavado de dinero y la financiación del terrorismo.<sup>74</sup> Exige a los transmisores de dinero y a otras instituciones financieras que se registren en FinCEN, instrumenten programas de prevención del lavado de dinero, conserven archivos sobre sus clientes y envíen al gobierno informes sobre transacciones sospechosas y otros datos.

Debido a que no es una empresa ni una persona jurídica, sino que es una red de persona a persona, Bitcoin mismo no puede ser considerado un transmisor de dinero. La pregunta es, entonces, ¿se ajustan algunos de los actores del ecosistema de Bitcoin a las definiciones legales de “transmisor de dinero” que los convertirían en sujetos obligados a cumplir con la normativa estadual y federal?

En marzo de 2013, FinCEN publicó una guía sobre la aplicación de la BSA a las monedas virtuales, incluida Bitcoin. La guía define

---

71. 18 U.S.C. § 1960.

72. Aaron Greenspan, *Held Hostage: How the Banking Sector Has Distorted Financial Regulation and Destroyed Technological Progress* (Palo Alto, CA: Think Computer Corporation, 2011), <http://www.thinkcomputer.com/corporate/whitepapers/heldhostage.pdf>.

73. *Ibid.*, 3.

74. 31 U.S.C. § 5311.

tres categorías de personas potencialmente sujetas a la normativa como transmisores de dinero:

*Usuario* es la persona que obtiene moneda virtual con el fin de comprar productos y servicios. *Cambiador* es quien se dedica al negocio de intercambiar moneda virtual por moneda real, fondos u otra moneda virtual. *Administrador* es quien se dedica al negocio de emitir (poner en circulación) una moneda virtual y quien tiene la potestad de redimir (o quitar de circulación) dicha moneda virtual.<sup>75</sup>

Podemos aplicar cada una de estas definiciones a los participantes del ecosistema de Bitcoin. La definición más clara es la de *cambiador*. Si uno se dedica al negocio de cambiar dólares por bitcoin y viceversa, podemos concluir que, según la guía, es transmisor de dinero y por lo tanto tiene que registrarse en FinCEN y cumplir con las normas relevantes que obligan a mantener registros y enviar reportes. Además, dado que los estados se basan en las determinaciones de FinCEN sobre qué entidades son o no transmisores de dinero, es probable que un cambiador deba también obtener licencias de transmisor de dinero en los estados.

Menos claras son las obligaciones de quienes se ajustan a la definición de “usuarios” de Bitcoin. La guía establece que si uno obtiene bitcoin “con el fin de comprar y vender productos y servicios”, uno no es transmisor de dinero y no está sujeto a la normativa de FinCEN. Sin embargo, no explica cómo aplica la ley si uno obtiene bitcoin *no* para comprar productos y servicios. Algunas de las razones por las que uno podría adquirir bitcoin incluyen (1) especular que el precio de bitcoin va a subir, (2) simplemente porque uno confía más en la estabilidad de una moneda virtual que en la de una “moneda real” (pensemos en Argentina o Zimbabwe)

---

75. FinCEN, *Application of FinCEN's Regulations*.

o (3) porque uno desea hacer un envío de moneda a un familiar que se encuentra en el extranjero. En ninguno de estos casos estaría claro si los usuarios de Bitcoin están exentos de las obligaciones de registro, mantenimiento y reportes impuestos por FinCEN. Esto crea un ambiente de incertidumbre reglamentaria que podría afectar negativamente la adopción de Bitcoin.

Donde existe mayor confusión es en la manera en que la guía se aplica a los mineros de Bitcoin, quienes crean nuevos bitcoin al poner su poder de computación al servicio de la red de Bitcoin. La tercera clase de personas que la guía define son los “administradores”, pero la definición solo se aplica a las monedas virtuales centralizadas en las que existe una autoridad central que pone en circulación la moneda. Por ejemplo, es claro que Amazon.com es administrador de su nueva moneda virtual llamada “moneda de Amazon”.<sup>76</sup> Por lo tanto, la guía tiene una sección en la que se refiere a monedas virtuales descentralizadas como Bitcoin. Según esa sección, un minero que mina bitcoin y luego los usa para “comprar productos o servicios reales o virtuales” es considerado un usuario y por lo tanto no está sujeto a la normativa.<sup>77</sup> Pero si el minero vende los bitcoin minados por él “a otra persona a cambio de moneda real o su equivalente”, entonces el minero cumple con los requisitos para ser considerado transmisor de dinero y por lo tanto queda sujeto a la normativa.<sup>78</sup>

No es claro cómo esta reglamentación de los mineros devenidos transmisores de dinero promovería los intereses de protección al consumidor o prevención del lavado de dinero. Los mineros no estarían transmitiendo bitcoin de una parte a otra porque esos bitcoin están siendo creados de la nada. Si los mineros venden esos bitcoin que minan, solo hay dos partes en la transacción.

---

76. Ingrid Lunden, “Amazon Now Offers Amazon Coins Virtual Currency on Kindle Fire, Gives \$5 in Free Coins to All Users,” *TechCrunch*, 13 de mayo de 2013, <http://techcrunch.com/2013/05/13/amazon-launches-amazon-coins-virtual-currency-on-kindle-fire-gives-5-in-free-coins-to-all-users/>.

77. *Ibid.*

78. *Ibid.*



Como consecuencia, no existe un consumidor para proteger ni un potencial delincuente buscando convertir “dinero sucio” en dinero limpio.

Finalmente, la guía señala que la normativa de FinCEN define a la moneda como la moneda de un estado, por lo que la guía también se refiere a esta definición como “moneda real”.<sup>79</sup> Luego introduce un nuevo concepto que llama “moneda virtual” sobre el cual se fundamenta toda la guía.<sup>80</sup> La guía define a una moneda virtual como “un medio de intercambio que opera como una moneda en algunos ambientes, pero que no tiene los atributos de una moneda real”.<sup>81</sup> Luego introduce un nuevo concepto al explicar que existen diferentes tipos de “moneda virtual” y que la guía en cuestión es aplicable solo a la “moneda virtual convertible”, a la que define como “la que tiene un valor equivalente en moneda real o actúa como sustituto de una moneda real”.<sup>82</sup> Mientras la definición de moneda (también conocida como “moneda real”) fue adoptada a través del proceso oficial de creación de normas, los otros nuevos y sustantivos conceptos, “moneda virtual” y “moneda virtual convertible”, existen solo en esta guía. Como consecuencia, se puede argumentar que la guía incluye nueva legislación en vez de interpretar leyes y normas preexistentes, lo cual necesitaría de un proceso oficial de creación de normas conforme a lo dispuesto en la Ley de Procedimiento Administrativo.

Reglamentación de la Comisión sobre el Comercio de Futuros sobre Commodities (en inglés, Commodity Futures Trading Commission o CFTC)

Por su naturaleza, se puede concebir a los bitcoin como una commodity o como una moneda. De hecho, el economista George

---

79. FinCEN, *Application of FinCEN's Regulations*.

80. Ibid.

81. Ibid.

82. Ibid.

Selgin se ha referido a Bitcoin como “dinero de commodity sintético”.<sup>83</sup> Esto ha atraído la atención de la CFTC, que tiene la potestad de reglamentar los futuros sobre commodities y los mercados en los que estos se comercializan, así como algunos instrumentos de divisas.<sup>84</sup>

Bart Chilton, uno de los comisionados de la CFTC, declaró recientemente en el *Financial Times* que Bitcoin “es con seguridad algo que necesitamos explorar”.<sup>85</sup> Otras fuentes confirmaron que la CFTC está investigando “seriamente” las monedas virtuales.<sup>86</sup> Si la CFTC elige reglamentar las transacciones de bitcoin, una de las preguntas obvias es si lo hará bajo su potestad para supervisar futuros sobre commodities o bajo su autoridad para reglamentar divisas.

Si bien la Ley de Intercambio de Commodities define a los “contratos de divisas a plazo” y a las “permutas de divisa”, no define a las “divisas” ni a la “moneda extranjera”, probablemente porque el Congreso consideró que estos términos eran obvios. Por lo tanto, si la CFTC decide aplicar su reglamentación sobre divisas a las transacciones de Bitcoin, tendrá que tomar la determinación de que los bitcoin son considerados “moneda extranjera”. Si bien concebible, dicha determinación estaría en desacuerdo con la interpretación más común de moneda extranjera es aquella emitida por gobiernos extranjeros.

A modo ilustrativo, podemos echar un vistazo a la Ley Dodd-Frank de Reforma de Wall Street y Protección al Consumidor de 2009, que expande la autoridad de la CFTC para reglamentar las divisas. El Título 10 de la ley también establece la Oficina de Protección al Consumidor de Servicios Financieros (en inglés, CFPB) y para los fines de ese título define a la “moneda

---

83. George Selgin, “Synthetic Commodity Money” (working paper, Department of Economics, University of Georgia, Athens, 2013), [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2000118](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2000118).

84. 7 U.S.C. §§ 2(C) and 2(E).

85. Alloway, Meyer y Foley, “US Regulators Eye Bitcoin.”

86. Ibid.

extranjera” como “el intercambio, a cambio de una compensación, de la moneda de Estados Unidos o de un gobierno extranjero por la moneda de otro gobierno”.<sup>87</sup> Esta definición nos da una pista de cómo el Congreso concibe a la “moneda extranjera” y es claro que el intercambio de bitcoin quedaría fuera de esta definición porque los bitcoin no son la moneda de ningún gobierno.

La conexión entre moneda extranjera y emisión por parte de un gobierno es común. Por ejemplo, la definición de moneda del Ministerio de Economía (adoptada a través del proceso de creación de normas, como indicamos antes) es

la moneda de metal o papel de los Estados Unido o de cualquier otro país que esté designada como de curso legal y que circule y se acostumbre utilizar y sea aceptada como medio de intercambio en el país de emisión. Moneda incluye certificados de plata de EE. UU., billetes en circulación de EE. UU. y billetes en circulación de la Reserva Federal. Moneda incluye también billetes extranjeros oficiales que se acostumbre utilizar y sean aceptados como medio de intercambio en un país extranjero.<sup>88</sup>

Esto coincide con la definición de “dinero” del Código Comercial Uniforme, como “medio de intercambio autorizado o adoptado por un gobierno interno o extranjero [incluida] una unidad monetaria contable establecida por una organización intergubernamental o mediante acuerdo entre una o más naciones”.<sup>89</sup>

Por el contrario, la CFTC bien podría tratar a los bitcoin como commodities. La Ley de Intercambio de Commodities define a las commodities como toda “mercadería o artículo . . . y todo servicio,

---

87. Dodd-Frank Wall Street Reform and Consumer Protection Act § 1002 (16); 12 U.S.C. § 5481 (16) (2012).

88. 31 C.F.R. § 1010.100(m).

89. Unif. Commercial Code §§ 1–201.

derecho e interés . . . en los que se trafiquen en el presente o en el futuro contratos para su entrega futura”, con excepción de las cebollas y los recibos de la entrada del cine.<sup>90</sup> Por lo tanto, los bitcoin podrían llegar a cumplir con la definición de commodities porque son artículos que pueden ser comercializados y sometidos a contratos de futuros. Sin embargo, cabe señalar que los bitcoin son un tipo de commodity muy diferente de las tradicionales, como lo son el oro, el maíz o el petróleo, los que son tangibles y tiene usos intrínsecamente valiosos. No olvidemos que la CFTC tiene potestad, no sobre los commodities mismos, sino sobre los contratos de futuros sobre los commodities. Sin embargo, un intercambio de bitcoin por dólares u otra moneda nacional por lo general ocurre simultáneamente y no es parte de un contrato de futuros. Por lo tanto, la reglamentación que la CFTC pueda encarar sobre los bitcoin *como commodities* puede llegar a ser limitada. Sin embargo, en la medida en que se vayan desarrollando mercados de futuros de bitcoin es probable que estén sujetos a la supervisión de la CFTC.<sup>91</sup>

Reglamentación de las transferencias electrónicas de fondos  
El ultimo posible vector de reglamentación de Bitcoin bajo la ley vigente en la actualidad que vamos a considerar es la normativa emanada de la Ley de Transferencia Electrónica de Fondos (en inglés, EFTA)<sup>92</sup> y su aplicación a través de la Reglamentación E de la Reserva Federal.<sup>93</sup> El propósito de la EFTA es establecer los respectivos derechos y obligaciones de los consumidores y las instituciones financieras en la transferencia electrónica de

---

90. 7 U.S.C. § 1a (9).

91. Sin embargo, están surgiendo mercados de futuros de Bitcoin. Véase Cyrus Farivar, “Taming the Bubble: Investors Bet on Bitcoin via Derivatives Markets,” *Ars Technica*, 11 de abril de 2013, <http://arstechnica.com/business/2013/04/taming-the-bubble-investors-bet-on-bitcoin-via-derivatives-markets/>.

92. 15 U.S.C. §§ 1601–1692 (2013).

93. 12 C.F.R. §§ 205.1–205.20.

fondos.<sup>94</sup> Tal como sucede con otras leyes y normas que hemos comentado, la EFTA no parece contemplar una moneda virtual descentralizada como Bitcoin.

La ley define a las transferencias electrónicas de fondos como “toda transferencia de fondos, que no sea una transacción originada por cheque, giro o instrumento de papel similar, que sea iniciada a través de una terminal electrónica, un instrumento telefónico, una computadora o una cinta magnética con el fin de solicitar, instruir o autorizar a una institución financiera a debitar o acreditar una cuenta”.<sup>95</sup> Además define a una “institución financiera” como un “banco Nacional o Estadual, una asociación de ahorro y préstamos Federal o Estadual, un banco de ahorros mutuos, una cooperativa Federal o Estadual o cualquier otra persona que, directa o indirectamente, mantenga una cuenta a nombre de un consumidor”.<sup>96</sup> Estas definiciones y las reglamentaciones que ellas fundamentan asumen que las transferencias electrónicas de fondos inevitablemente van a involucrar a “instituciones financieras” y “cuentas”. Sin embargo, Bitcoin va en contra de esta noción.

El sistema mismo de Bitcoin no se ajusta a la definición de “institución financiera” porque, como lo indicamos antes, no se trata de una empresa o persona jurídica sino de una red global de persona a persona. En consecuencia, una dirección de Bitcoin con la que se asocien los bitcoin en la red no puede considerarse como una cuenta residente en una institución financiera. Además, como lo indicamos en la explicación técnica sobre cómo se transfieren los bitcoin de una dirección a otra, en el sistema de Bitcoin no existe una “institución financiera” u otro tercero de ningún tipo que “debite o acredite una cuenta”. Las transferencias electrónicas de fondos entre direcciones son llevadas a cabo por los usuarios solos, quienes firman una transacción con la clave privada asociada con una dirección de Bitcoin que ellos

---

94. 15 U.S.C. § 1693(b).

95. 15 U.S.C. § 1693a (7).

96. 15 U.S.C. § 1693a (9).

controlan. La red de Bitcoin se limita a confirmar que la transacción sea legítima.

Si bien muchos usuarios almacenan “archivos de billeteras”<sup>97</sup> con sus claves privadas en sus propias computadoras u otros aparatos,<sup>98</sup> otros delegan la protección de sus claves a servicios de billeteras en línea.<sup>99</sup> Estos servicios de billetera ofrecidos por terceros también brindan una mayor facilidad de uso que el software de Bitcoin instalado en la computadora. Por lo general, los usuarios crean una “cuenta” en este tipo de servicios de billetera y vinculan sus direcciones de Bitcoin con esas cuentas. Es concebible que este tipo de servicios en línea pueda llegar a ajustarse a la definición de “institución financiera” bajo la EFTA y por lo tanto estén sujetos a su reglamentación. Sin embargo, podría argumentarse que estos servicios no se dedican a la transferencia electrónica de datos porque no inician las transferencias.<sup>100</sup> Las transferencias son realizadas por los usuarios directamente y verificadas por la red de Bitcoin; los servicios de billetera en línea solo proporcionan el software y el almacenamiento que les permite a los usuarios interactuar con la red de Bitcoin.

Finalmente, existen nuevas normas del CFPB que enmiendan la Reglamentación E y están especialmente dirigidas a los proveedores de servicios de transferencia de dinero. Estas normas exigen a los proveedores divulgar las tasas de cambio y los aranceles asociados con las transferencias internacionales e investigar y remediar

---

97. *Bitcoin wiki*, s.v. “Wallet,” consultada el 30 de julio de 2013, <https://en.bitcoin.it/wiki/Wallet>.

98. Matthew Sparks, “Winklevoss Twins Back Bitcoin as Bubble Bursts,” *Telegraph*, 12 de abril de 2013, <http://www.telegraph.co.uk/technology/news/9989610/Winklevoss-twins-back-bitcoin-as-bubble-bursts.html>.

99. *Bitcoin wiki*, “EWallet,” consultada el 30 de Julio de 2013, <https://en.bitcoin.it/wiki/EWallet>.

100. Nikolei M. Kaplanov, “Nerdy Money: Bitcoin, the Private Digital Currency, and the Case against Its Regulation,” *Loyola Consumer Law Review* 25, no. 1 (2012).

errores de procesamiento.<sup>101</sup> También obligan a los operadores a proveer un período de 30 minutos o más en el cual el consumidor pueda cancelar una transacción.<sup>102</sup> Este requisito puede considerarse incompatible con el protocolo de Bitcoin, porque todas las transacciones de bitcoin son irreversibles. Una manera de cumplir con esta norma podría ser retrasar la ejecución de las transacciones. Sin embargo, el verdadero problema es que este requisito se opone fundamentalmente al propósito de la tecnología.

## RECOMENDACIONES

COMO HEMOS VISTO, Bitcoin no encaja perfectamente en ninguno de los compartimentos normativos. Ese suele ser el sello distintivo de una tecnología disruptiva. Es claro que Bitcoin constituye un logro tecnológico revolucionario que presagia sorprendentes beneficios potenciales para la humanidad. Sin embargo, como sucede con cualquier tecnología que puede usarse para el bien, también puede usarse para el mal. El desafío para los legisladores será promover los usos beneficiosos de Bitcoin y a la vez minimizar sus consecuencias negativas. Concluimos con algunas recomendaciones para ayudar a los legisladores a cumplir con este doble objetivo.

### No restringir a Bitcoin

Debido a que Bitcoin es en esencia dinero por internet, algunos de los que trafican drogas y otras mercancías ilícitas en línea lo han encontrado ideal como medio de intercambio.<sup>103</sup> Enfrentados con

---

101. Consumer Financial Protection Bureau, “Summary of the Final Remittance Transfer Rule (Amendment to Regulation E)” (Washington, DC: Consumer Financial Protection Bureau, 2013), [http://files.consumerfinance.gov/f/201305\\_cfpb\\_remittance-transfer-rule\\_summary.pdf](http://files.consumerfinance.gov/f/201305_cfpb_remittance-transfer-rule_summary.pdf).

102. Ibid.

103. Andy Greenberg, “Founder of Drug Site Silk Road Says Bitcoin Booms and Busts Won’t Kill His Black Market,” *Forbes*, 16 de abril de 2013, <http://www.forbes.com/sites/andygreenberg/2013/04/16/founder-of-drug-site-silk-road-says-bitcoin-booms-and-busts-wont-kill-his-black-market/>.

este hecho, el impulso inicial de algunos legisladores será exigir la imposición de restricciones a la tecnología.<sup>104</sup> Sin embargo, existen muchas buenas razones para resistir este impulso.

En primer lugar, como tecnología, Bitcoin no es ni bueno ni malo, sino que es neutral. Los billetes de papel, como los bitcoin, pueden usarse para transacciones ilícitas sin que por ello se nos ocurra proscribirlos. Solo prohibimos su *uso ilícito*. Además, solo hay pruebas anecdóticas del punto hasta el cual los bitcoin se utilizan para transacciones delictivas. Sería sabio poner el uso delictivo de la tecnología en perspectiva junto a los usos legítimos. A medida que la economía de bitcoin crezca, es probable que los usos legítimos de bitcoin superen ampliamente las transacciones criminales,<sup>105</sup> tal como sucede con los billetes de papel.

En segundo lugar, cualquier intento de restringir la tecnología de Bitcoin solo perjudicaría a los usos legítimos casi sin afectar los usos ilegítimos. Debido a la naturaleza global y descentralizada de la red, es virtualmente imposible apagar a Bitcoin. Bitcoin no es una empresa ni una entidad que pueda ser blanco de una acción. En lugar de ello, Bitcoin y su registro de transacciones existen solo en una red distribuida de persona a persona creada por sus usuarios. Tal como sucedió con el servicio de transferencia de archivos de persona a persona BitTorrent, restringir cualquiera de los computadores individuales que conforman el sistema de persona a persona tendría un efecto mínimo en el resto de la red. Por lo tanto, proscribir el uso de Bitcoin no debilitaría la red; solo serviría para garantizar que se le niegue el acceso a la tecnología a los usuarios respetuosos de la ley. Como consecuencia de esto, se privaría a la sociedad de disfrutar los

---

104. Charles Schumer y Joe Manchin, Letter to Attorney General Eric Holder and Drug Enforcement Administration Administrator Michele Leonhart, 6 de junio de 2011. Available at <http://www.manchin.senate.gov/public/index.cfm/press-releases?ID=284ae54a-acfl-4258-be1c-7acee1f7e8b3>.

105. Jan Jahosky, "BitPay Eclipses Silk Road in Bitcoin Sales with Explosive \$5.2M March," *BitPay Blog*, 2 de abril de 2013, <http://blog.bitpay.com/2013/04/bitpay-eclipses-silk-road-in-bitcoin.html>.



potenciales beneficios de Bitcoin sin ver descenso alguno en su uso criminal.

En tercer lugar, si Bitcoin fuera proscrito, el gobierno se privaría de la oportunidad de supervisar a los intermediarios participantes de la economía de bitcoin, como lo son los cambiadores y los transmisores de dinero. El interés del gobierno en detectar y evitar el lavado de dinero y la financiación del terrorismo se vería promovido mucho mejor, no con la prohibición de la tecnología, sino con la exigencia a los intermediarios de que conserven registros y reporten actividades sospechosas, como lo hacen las instituciones financieras tradicionales. Una vez más, restringir el uso de Bitcoin tendrá el efecto indeseado de que solo los delincuentes utilicen la tecnología. Cualquier intermediario ilícito que surgiera, tales como cambiadores o procesadores de pagos, quedarían exentos de regulación.

Finalmente, aun cuando Estados Unidos proscriba el uso de Bitcoin, es probable que muchos otros países no lo hagan, por reconocer la gran cantidad de beneficios potenciales que ofrece la tecnología. Por ejemplo, el banco central finlandés, ha declarado que la moneda digital no es ilegal,<sup>106</sup> lo cual ha hecho que muchos negocios finlandeses comiencen a aceptar bitcoin.<sup>107</sup> Al prohibir el uso de Bitcoin, los Estados Unidos se podrían a sí mismos en una posición de desventaja competitiva internacional en el desarrollo y uso de lo que puede llegar a ser la próxima generación en sistemas de pagos.

Homogeneizar la reglamentación y promover el desarrollo

En vez de reaccionar exageradamente ante los usos ilícitos de Bitcoin, los legisladores deberían tener la sensatez de abordar los

---

106. Matt Clinch, "Bitcoin Utopia? Interest Is Sky High in This Euro Nation," *CNBC*, 4 de abril de 2013, <http://www.cnbc.com/id/100618694>.

107. Jan Jahosky, "BitPay Exceeds 1,000 Merchants Accepting Bitcoin," *BitPay Blog*, 11 de septiembre de 2012, <http://blog.bitpay.com/2012/09/bitpay-exceeds-1000-merchants-accepting.html>.

desafíos impuestos por la nueva tecnología con calma y cautela. Hacerlo le permitiría al ministerio público perseguir los objetivos de detectar y prevenir el lavado de dinero y la financiación del terrorismo y al mismo tiempo asegurarse de que la sociedad no se priva de los múltiples beneficios de Bitcoin. Afortunadamente, hasta el día de hoy, las agencias de supervisión han actuado con cautela y han empezado a integrar a Bitcoin lentamente en el marco normativo vigente. Los legisladores pueden tomar algunas medidas básicas para mantener el equilibrio correcto.

En el corto plazo, FinCEN debería esclarecer las dudas que surgieron de su reciente guía, en especial en lo que respecta a los mineros y los usuarios que no obtienen bitcoin para comprar productos o servicios, sino para otros fines legítimos y legales. Debería hacer esto invitando a la comunidad de Bitcoin, compuesta por desarrolladores, mineros, empresas y usuarios, a participar de un procedimiento público de notificación y comentario. Mientras la misión de FinCEN es salvaguardar el sistema financiero de todo abuso criminal, también tiene la obligación de no impedir indebidamente el desarrollo tecnológico. Trabajando con los usuarios legítimos de Bitcoin, no hay dudas de que FinCEN lograría sus metas y a la vez reduciría la incertidumbre reglamentaria.

En el largo plazo, los legisladores deberían definir con mayor precisión el estatus normativo general de Bitcoin. Como hemos visto, la moneda digital no se ajusta a ninguna de las categorías o definiciones legales existentes. No es una divisa, no es una commodity tradicional, ni siquiera es una simple red de pagos. En consecuencia, aplicar la normativa vigente hoy a Bitcoin podría obstruir su desarrollo sin que se produzcan beneficios palpables para la ley o el bienestar de los consumidores. Por ello, los legisladores deberían considerar la creación de una nueva categoría que tome en cuenta la naturaleza singular de la tecnología. También deberían considerar detenidamente qué reglamentación, si es que corresponde, sería aplicable a los cambiadores de bitcoin, los procesadores de pago y los usuarios.

Finalmente, los legisladores no solo deberían permitir el continuo desarrollo de Bitcoin, sino que deberían además fomentar su crecimiento mediante la revisión de las barreras normativas actuales. Uno de los mayores obstáculos para la adopción de Bitcoin es la exigencia de que las empresas que se dediquen a la transmisión de dinero deban adquirir una licencia en cada estado. Este proceso duplicativo, laborioso y costoso representa una barrera para el comercio inter-estadual sin ofrecer demasiados beneficios al consumidor. Los legisladores y supervisores federales deberían considerar los méritos de aplicar el principio de prioridad federal.

## CONCLUSIÓN

BITCOIN ES UNA fascinante innovación que tiene el potencial de mejorar enormemente el bienestar de la humanidad e impulsar desarrollos potencialmente revolucionarios en el ámbito de los pagos, las comunicaciones y las empresas. La inteligente manera en que Bitcoin utiliza la encriptación de claves públicas y la red de persona a persona resuelve el problema del doble gasto que hasta hoy había impedido el desarrollo de las monedas digitales descentralizadas. Estas propiedades se combinan para crear un sistema de pagos que podría reducir los costos transaccionales en los comercios y las remesas de dinero, aliviar la pobreza, proporcionar un medio de evadir los controles de capital y las malas administraciones monetarias, permitir la privacidad financiera legítima en internet y estimular nuevas innovaciones financieras. Por otra parte, como “efectivo digital”, Bitcoin puede ser utilizado para el lavado de dinero y el comercio ilícito. La proscripción de Bitcoin no es la solución contra estos flagelos, como tampoco lo es proscribir el efectivo.

A final de cuentas, Bitcoin puede llegar a fallar como moneda digital y sistema de pagos experimental. Podría surgir un problema totalmente imprevisible que destruyera la economía de bitcoin. Bitcoin podría ser reemplazado por otra cripto-moneda superior. También podría desaparecer por ser una moda pasajera. Las

razones por las que puede fallar son infinitas, pero una de ellas no debería ser que los legisladores no comprendieron su funcionamiento y su potencial. En última instancia, no estamos abogando por Bitcoin, sino por la innovación. Es importante que los legisladores permitan que este experimento continúe. Ellos deben trabajar para esclarecer de qué manera Bitcoin debe ser reglamentado y homogeneizar la normativa para que todos tengamos la oportunidad de aprender cuán innovador Bitcoin puede llegar a ser.

## LECTURAS MÁS EXTENSAS

Satoshi Nakamoto. “Bitcoin: A Peer-to-Peer Electronic Cash System.” White Paper, 2008. <http://bitcoin.org/bitcoin.pdf>.

Reuben Grinberg. “Bitcoin: An Innovative Alternative Digital Currency.” *Hastings Science & Technology Law Journal* 4 (2011): 160–208. [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1817857](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1817857).

William J. Luther. “Cryptocurrencies, Network Effects, and Switching Costs.” Mercatus Working Paper, Mercatus Center at George Mason University, Arlington, VA, forthcoming. [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2295134](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2295134).

George Selgin. “Synthetic Commodity Money.” Working paper, University of Georgia Department of Economics, Athens, GA, April 10, 2013. [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2000118](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2000118).

Nikolei M. Kaplanov. “Nerdy Money: Bitcoin, the Private Digital Currency, and the Case against Its Regulation.” *Loyola Consumer Law Review* 25 (2012): 111–174. [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2115203](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2115203).

European Central Bank. “Virtual Currency Schemes.” October 2012. [http://www.ecb.europa.eu/pub/pdf/other/virtual\\_currencyschemes201210en.pdf](http://www.ecb.europa.eu/pub/pdf/other/virtual_currencyschemes201210en.pdf).



## SOBRE LOS AUTORES

JERRY BRITO es investigador sénior y director del programa de la política de tecnología del Mercatus Center at George Mason University. También es profesor adjunto de derecho en George Mason University. Su investigación se concentra en la política de tecnología y de internet, los derechos de autor y el proceso regulatorio. Sus artículos de fondo han aparecido en *Wall Street Journal*, *New York Times* y otros medios. Con Susan Dudley, Brito es coautor de *Regulation: A Primer*. Además es editor de *Copyright Unbalanced: From Incentive to Excess*. Sirve como presentador de *Surprisingly Free*, un podcast semanal que presente entrevistas con una mezcla ecléctica de autores, académicos y empresarios a la intersección de tecnología, política y economía. Brito también contribuye artículos a *Technology Liberation Front*, un blog que trata de la política de tecnología. Ha creado varios sitios web con la meta de promover transparencia y responsabilidad en el gobierno, por ejemplo [OpenRegs.com](http://OpenRegs.com) y [WCITLeaks.org](http://WCITLeaks.org). Brito recibió su JD de la facultad de derecho de George Mason University y la licenciatura en ciencias políticas de Florida International University.

ANDREA CASTILLO es asistente de investigación en el Mercatus Center at George Mason University. Es coautora de *Liberalism and Cronyism: Two Rival Political and Economic Systems* con Randall G. Holcombe. También contribuye al blog *Neighborhood Effects* y sirve como columnista para *The Ümlaut*. Recibió la licenciatura en economía y ciencias políticas de Florida State University.

