

DOCTRINA

## Criptomonedas, economía y derecho

*Cryptocurrencies, economic and legal aspects*

Agustín Barroilhet Díez 

*Universidad de Chile*

**RESUMEN** En este artículo sugiero que mientras el derecho tradicional no sea capaz de generar una respuesta coherente y transversal para regular las criptomonedas, y en general, para regular los bienes virtuales, la regulación que busque evitar su mal uso debiera ser la mínima necesaria para cumplir con el objetivo de política estrictamente definido. Todavía no hemos desarrollado las categorías conceptuales adecuadas para regular un fenómeno tan nuevo y, además, desde un punto de vista práctico y financiero, las criptomonedas no han alcanzado importancia suficiente para justificar el esfuerzo regulatorio que las monedas tradicionales demandan. Mi argumento se suma a otras voces que han advertido que las sugerencias por regular las criptomonedas, más que inhibir su desarrollo, corren el riesgo de introducir regulaciones inefectivas y superficiales, que sin embargo pueden dañar a actores particulares, como los nuevos adoptantes y los que quieran experimentar con las tecnologías relacionadas.

**PALABRAS CLAVE** Criptomonedas, Bitcoin, regulación económica, derecho civil.

**ABSTRACT** This article suggests that, while the state of the art in the Civil Law tradition is incapable of producing a coherent and transversal answer to address the regulation of cryptocurrencies, and in general, virtual goods, drafters and lawmakers should aim to produce the rules necessary to achieve narrowly defined and explicit policy goals. In the article I show the shortcomings of using the existing legal concepts to regulate cryptocurrencies, and additionally show that in practice and financially, they have not yet achieved the necessary importance to force traditional concepts used to regulate currency upon them. The argument goes in line with previous literature that claims that current suggestions to regulate cryptocurrencies do not risk inhibiting their development, but risk shallow and ineffective regulation that might damage particular actors like early-adopters or those willing to experiment with newer technologies.

**KEYWORDS** Cryptocurrency, Bitcoin, economic regulation, Civil Law.

## Introducción

En este artículo sugiero que mientras el derecho no sea capaz de generar una respuesta coherente y transversal para regular las criptomonedas y, en general, bienes virtuales, las respuestas regulatorias restrictivas que busquen evitar su mal uso debieran ser puntuales y las mínimas necesarias para cumplir con objetivos de política estrictamente definidos. En este artículo muestro que todavía no hemos desarrollado las categorías conceptuales adecuadas para regular un fenómeno tan nuevo y que, además, desde un punto de vista práctico y financiero, las criptomonedas no han alcanzado importancia suficiente para justificar el esfuerzo regulatorio que las monedas tradicionales demandan. Mi argumento se suma a otras voces que han advertido que las sugerencias por regular las criptomonedas, más que inhibir su desarrollo, corren el riesgo de inducir regulaciones inefectivas y superficiales, que sin embargo pueden dañar a actores particulares, como los nuevos adoptantes y los que quieran experimentar con la tecnología (Kaplanov, 2012). La preocupación que motiva este artículo es que, a propósito de querer, por ejemplo, regular a Bitcoin, la criptomoneda más popular, terminemos regulando torpemente a las primeras bolsas de Bitcoin locales o nuevas aplicaciones de Blockchain, que es la tecnología que posibilita Bitcoin. Aunque en este artículo no me hago cargo del problema de la disrupción y la competencia que ha sido el foco en Chile de la batalla entre intermediadores de criptomonedas y la banca comercial tradicional, quiero ilustrar por qué las criptomonedas son un desafío para el derecho tradicional que va mucho más allá de sus potenciales usos delictivos o las dificultades que presenta para la regulación monetaria.

El desarrollo del argumento es el siguiente. En la primera parte reviso el concepto de monedas virtuales para distinguirlas de otras formas de dinero electrónico. El dinero electrónico no significó una verdadera revolución para el derecho. En contraste, las criptomonedas sí son revolucionarias y por ello es necesario distinguirlas de éste. En la segunda parte desarrollo la historia de las monedas virtuales y de las criptomonedas para explicar el surgimiento de la «riqueza» que los sustenta. Criptomonedas y monedas virtuales no solo comparten la característica de ser digitales. Ambas fueron diseñadas para emular la escasez que existe en el mundo real. Esto es esencial para entender el fenómeno que se quiere regular. En la tercera parte reviso la operatoria de las criptomonedas para ilustrar aspectos en que éstas representan algo totalmente nuevo para lo que muchas de nuestras instituciones legales no están adaptadas. Si el derecho sirve para atribuir responsabilidades o dar certeza a las partes en una transacción, las criptomonedas tienen respuestas programadas y desintermediadas que podrían hacer que muchas de las instituciones legales que buscan cumplimiento o regulan el comportamiento de intermediarios sean inútiles. En la cuarta parte adopto un enfoque funcionalista y me embarco en explorar por qué, desde un punto de vista económico, las criptomonedas son distintas a las monedas tradicionales, y

por qué regularlas pensando en monedas tradicionales, sin distinguir entre ellas, es un error. En la quinta parte, apoyándome en la historia, la operatoria y la economía de las criptomonedas, muestro la ineptitud del sistema legal para enfrentar el fenómeno actualmente, y hago mi defensa de la aproximación cautelosa a su regulación, especialmente si buscan objetivos restrictivos, como proteger a inversionistas y consumidores, o prevenir la comisión de delitos. Concluyo en la sexta parte reiterando mi sugerencia de aproximación regulatoria cautelosa y con respuestas puntuales para remediar problemas inminentes, todo ello mientras no tengamos una idea clara de cómo interactuaremos, humanos deliberantes, con esta nueva forma de generar y transferir riqueza.

### **Criptomonedas y otras formas de dinero digital**

Las criptomonedas son archivos, bits con datos —como los populares PDF o MP3— que buscan cumplir todas las funciones que se le asignan al dinero tradicional, pero usando internet como medio de transmisión. Antes de profundizar en el concepto, su concepción económica y su categorización jurídica, es útil distinguir criptomonedas de otros conceptos similares que invitan a confusión. En el orden tratados, éstos son: i) el dinero digital, ii) el dinero electrónico, iii) las monedas virtuales y, finalmente, iv) las criptomonedas.

El dinero digital o *digital currency* es el nombre genérico que recibe cualquier intangible que se utilice como medio de pago digital. Éste debe entenderse como opuesto a los conceptos de dinero físico, metálico o papel moneda. El dinero digital es el género que incluye todas las otras categorías: el dinero electrónico, las monedas virtuales y las criptomonedas (Arias y Sánchez, 2016: 175-176; Simonetti Rojas, 2017; Tucker, 2009). El concepto, si bien demasiado amplio para categorizarlo jurídicamente, es de interés para economistas porque incluye distintos medios de pago que podrían tener incidencia en el nivel general de precios. Incipientes trabajos en macroeconomía consideran que el dinero digital es una variable que debiera ser considerada en la teoría monetaria, especialmente si llega a funcionar como mecanismo de expansión del crédito bancario (Bjerg y otros, 2017: 20-21; Fung, Molico y Stuber, 2014; Peters, Panayi y Chappelle, 2015).

El dinero electrónico, también denominado *emoney*, es un medio de pago electrónico que eventualmente «obliga en» o da «derecho a» dinero de uso corriente o circulante y que lleva la denominación de éste (Khan, 2008; Rogers, 2005). El Banco Central Europeo lo define como «un depósito electrónico de valor monetario [contenido] en un dispositivo tecnológico [software o hardware] que puede ser usado ampliamente para hacer pagos a entidades distintas que su emisor».<sup>1</sup> Estados Unidos

---

1. Banco Central Europeo, «Electronic money», European Central Bank, disponible en <http://bit.ly/2Yvlwz8>.

cuenta con legislación que regula las transacciones electrónicas y, por tanto, el dinero electrónico desde 1978 (Electronic Fund Transfer Act).

Lo que distingue al dinero electrónico de otras formas de dinero digital es que requiere de una «infraestructura contractual» que asigne responsabilidades entre las partes y contenga mecanismos para convertirlo en dinero corriente, aunque éstos no se utilicen en la práctica (Khan, 2008). Las obligaciones que genera el dinero electrónico son análogas a las que generan las transacciones de documentos representativos de dinero (Khan, 2008; Halaburda y Sarvary, 2016; Rogers, 2005: 1.257-1.262). Con Paypal, por ejemplo, se puede pagar en dólares una compraventa en internet. Pero Paypal se apoya en las tarjetas de crédito y los contratos que las sustentan y que asignan responsabilidades entre las partes. Esta operativa no es radicalmente distinta de como funcionan una nota de crédito o un cheque que se gira contra una cuenta corriente. Como señalan Gans y Halaburda (2015), el dinero electrónico es la «capa digital» del dinero corriente.

Monedas virtuales (*virtual currency*), son monedas digitales no reguladas que sirven como medio de pago en internet (Banco Central Europeo, 2012: 13). Es importante no confundirlas con mecanismos representativos de *commodities*. Estos últimos vendrían a ser la «capa digital» del dinero basado en mercancías (*commodity money*).<sup>2</sup> Las monedas virtuales tienen denominación propia y no tienen correspondencia en el mundo físico. No se transan bajo el supuesto de que sean convertibles en dinero corriente, aun cuando mercados secundarios permitan regularmente dicha conversión (Banco Central Europeo, 2012). Su utilidad como medio de pago —su función principal— está determinada por lo que se pueda comprar directamente con ellas (Gans y Halaburda, 2015). Los programas de fidelización en millas de vuelo son un tipo de moneda virtual de creciente popularidad (Banco Central Europeo, 2012; Castronova, 2014). Millas y monedas virtuales son tan similares cuando se usan como medios de pago que muchas líneas aéreas están explorando transformar sus millas en criptomonedas.<sup>3</sup>

Finalmente, criptomonedas son un tipo de moneda virtual con características particulares que les permiten tener aplicación universal y más extendida. Lo que las hace especiales es que minimizan los potenciales problemas de valor asociados a mundos virtuales en los que no operan las mismas reglas de escasez del mundo real. Son especiales también porque funcionan sin intermediarios que validen las tran-

---

2. Golden Coin, por ejemplo, es una moneda digital respaldada en oro, pero requiere para funcionar que ambas partes entreguen mandato a GCB Suisse AG, que reclama tener el oro de respaldo que las partes transan. Existen muchos tipos de monedas virtuales y para muchos fines distintos. El factor común de estas monedas está en el apelativo de «virtual» como opuesto a «real» o «respaldado».

3. Olga Kharif, «Forget airline miles. Crypto coins are coming to reward programs», *Bloomberg*, 30 de mayo de 2018, disponible en <https://bloom.bg/2YvguD4>.

sacciones y, adicionalmente, porque en las versiones más populares son descentralizadas. Las criptomonedas se emiten y cambian de manos de forma descentralizada utilizando criptografía para mantener fidelidad, además de tecnologías de registro o libros contables que son mantenidos y actualizados por miles de computadores independientemente para verificar que no existan usos duplicados (Brito y Castillo, 2013: 4; Halaburda y Sarvary, 2016: 2-3). Dadas estas especiales características, las criptomonedas aspiran a tener las mismas funciones que el dinero electrónico y, por tanto, el dinero corriente (Halaburda y Sarvary, 2016: 5). Son lo que Makoto anticipó como el «próximo paso lógico pero revolucionario en la historia del dinero».<sup>4</sup>

Antes de definir las criptomonedas técnica, económica y jurídicamente, es útil revisar su historia. Las criptomonedas son el último eslabón en evolución de las monedas virtuales, y conocer esta historia evolutiva permite entender su potencialidad económica y sus limitaciones, además de los desafíos que presentan para la ciencia jurídica.

### **Evolución de las monedas virtuales**

Las criptomonedas —que incorporan por diseño una escasez que no es obvia en el mundo virtual— tienen capacidad de funcionar como medio de pago y reserva de valor sin intermediarios o repositorios centralizados que consoliden, liberen y controlen en general los pagos, lo cual las hace revolucionarias (Doguet, 2012; Jacobs, 2011; Nakamoto, 2009: 2; Peters, Panayi y Chapelle, 2015).<sup>5</sup> Los titulares enfocados en sus usos ilegales, los hackeos masivos a intermediarios y sus espectaculares cambios de valor opacan la dimensión de este salto evolutivo (Kiviat, 2015: 571). Hasta la llegada de las criptomonedas, las monedas virtuales nunca habían sido capaces de transferir valor desligadas de bienes físicos o virtuales, ni habían tenido la virtud de poder ser administradas autónomamente. La trascendencia de este salto es más fácil de entender en una línea evolutiva en la que los juegos de computador proveen el punto de partida más ilustrativo.<sup>6</sup>

---

4. John Michael Makoto Dykes, «Digital cash and the development of the apolitical currency», MIT Computer Science & Artificial Intelligence Lab, 1995, disponible en <http://bit.ly/2Yu7xts>.

5. Denis Rice, «The past and future of Bitcoins in worldwide commerce», *Business Law Today*, 11 de noviembre de 2013, disponible en <http://bit.ly/2XpeKuO>.

6. Elijo la evolución de los juegos en línea en vez de la evolución del dinero electrónico, respecto del cual las criptomonedas también reflejan algunas mejoras porque considero que lo definitorio de una criptomoneda no es el medio en que se transmite o su infraestructura tecnológica, sino el que hayan sido diseñadas con el objetivo expreso de convertirse en verdaderas «monedas» en un sentido económico (*currency*), es decir, en un medio de pago circulante con denominación propia que tiene un valor de intercambio relativo respecto del dinero oficial. Para una historia breve del dinero electrónico en Estados Unidos que parte con el envío de «cables» por el telégrafo, véase Task Force on Stored-Value Cards

## La creación de riqueza digital

Los que vivimos la transición de consolas tipo Atari a los computadores de escritorio conocemos el salto en satisfacción o de utilidad marginal que significó poder grabar en los discos duros localmente los avances en los juegos. El reconocimiento del avance o del «crédito» fue quizás el primer peldaño en la evolución a gran escala que terminó en las criptomonedas. Grabar avances en juegos fue la forma más básica de «acumular» riqueza digital o bienes digitales con potencial de ser objetos de consumo masivo (Bartle, 2004; Lastowka y Hunter, 2004: 24). Esta riqueza digital nació a imagen y semejanza de la riqueza material y siguiendo sus mismas lógicas de escasez, que era lo que los usuarios conocían. En una rápida evolución, jugadores pudieron guardar su riqueza en la forma de inventarios, habilidades para sus personajes, vehículos, desbloqueo etapas, etcétera y, eventualmente, en algún tipo de moneda (Lastowka y Hunter, 2004). Esta primitiva forma de riqueza digital o de creación de bienes digitales —que reflejaba el esfuerzo y tiempo reales de jugadores de computadores—, no obstante, adolecía de un grave defecto para funcionar como reserva de valor: no era escasa. Los archivos locales que guardaban «las riquezas» podían ser copiados a nuevos discos duros de otros usuarios, quienes podían aprovecharse del tiempo y esfuerzo ajenos. Internet inicialmente facilitó esta duplicación. A 56 kbps se podían descargar gratuitamente avances en juegos junto con las instrucciones de cómo instalarlos localmente.<sup>7</sup>

## La creación de monedas virtuales

La llegada de la banda ancha en internet, sin embargo, cambió radicalmente la forma en que los desarrolladores de juegos comenzaron a interactuar con sus usuarios. La banda ancha permitió centralización, la que a su vez le permitió a los desarrolladores aumentar el valor agregado de la experiencia del jugador mediante recompensas programadas —básicamente premios y jerarquías observables por comunidades virtuales— que hoy se consideran esenciales en el diseño de juegos de computador (Wang y Sun, 2011).<sup>8</sup>

---

(1996: 664-668). Para discusiones respecto de Bitcoin como *currency*, véase Blundell-Wignall (2014), Halaburda y Sarvary (2016) y Yermack (2015).

7. Incluso en algunas comunidades, como las del juego *Doom*, los usuarios generaban mejoras que ponían, también gratuitamente, a disposición de terceros (De Waal, 1995). Esta posibilidad de duplicación ilimitada era contraria a la escasez, elemento esencial de los medios destinados a transferir valor y potencialmente convertirse en monedas circulantes.

8. La banda ancha transformó al jugador que antes podía ser estrella en su familia o en su barrio poniendo sus iniciales en las listas de ganadores de las consolas o *flippers* —en el estilo de los jugadores en películas de Hollywood como *The last starfighter* o *Cloak & Dagger*— en estrellas reconocidas de comunidades virtuales más amplias y formadas por desconocidos. Para una explicación económica de

Los bienes virtuales de esta primera generación de riqueza digital requerían que se protegiera de remotamente la valiosa identidad digital los jugadores, sus avatares y todo lo que representara esfuerzo o trabajo o avance en el juego. Este almacenamiento remoto o centralización disminuyó la posibilidad de duplicación que sufrió la primera generación de juegos de computador de escritorio.<sup>9</sup>

El paso siguiente en la evolución de las riquezas asociadas a estas plataformas, incluidas sus monedas, fue que los desarrolladores aprovecharon el conocimiento íntimo de los patrones de juegos de sus miles de usuarios para explotar sus disposiciones a pagar en tiempo o dinero por bienes que se ofrecían en sus mundos virtuales. Basándose en este conocimiento, estos desarrolladores generaron estrategias de marketing y segmentación, y comenzaron a vender productos o mejoras que se podían comprar con tarjetas de crédito de forma masiva, e incluso permitieron que estos intercambios se complementaran con bolsas o mecanismos de intercambio entre usuarios en las plataformas (Castronova, 2001; Grinberg, 2012; Halaburda y Sarvary, 2016).<sup>10</sup>

El círculo de producción y comercialización de esta riqueza digital, que corresponde a la riqueza que «respalda» en un sentido económico a las monedas virtuales de las plataformas de juegos, se completó cuando sitios de intercambio como Ebay y la crisis asiática proveyeron el lugar y la mano de obra para que —después de conflictos con desarrolladores de juegos (Castronova, 2006; Shaviro, 2007)<sup>11</sup> e incluso casos judiciales (Bartle, 2004)— se iniciara la venta directa de riquezas digitales en dinero corriente obtenidas por los jugadores-trabajadores de Asia (Shaviro, 2007).<sup>12</sup> Esta actividad de jugar para obtener recompensas escasas en juegos para luego venderlas por dinero corriente, conocida como RMT (*real money trading*) o «cosecha de oro» (*goldfarming*) (Castronova, 2006: 200; Heeks, 2009: 6; Shaviro, 2007: 6), marcó el nacimiento de las monedas de virtuales asociadas a plataformas (Halaburda y Sarvary, 2016).

---

este fenómeno, véase Jeremy Kelly, «Play time: The problem of abundance in MMORPG», Anthemion.org, disponible en <http://bit.ly/2wBeGwe>.

9. Con el poder centralizado de guardar la historia y de proveer los bienes «económicos» virtuales (Shaviro, 2007), los desarrolladores de juegos crearon verdaderos mundos virtuales con leyes físicas propias en que las que se mantuvieron los patrones de escasez, donde los usuarios vivían, competían, se enriquecían, se asociaban, sociabilizaban y perdían para, eventualmente, volver a renacer pobres (Lastowka y Hunter, 2004).

10. De acuerdo con Richard Bartle, padre del primer juego multiusuario derivado de *Dungeons & Dragons*, *MUD1*, en 1979, la primera venta de habilidades de un juego fue en 1987 en el juego *Shades*. La venta no era de objetos, sino de habilidades para obtener la categoría de mago. Véase Dan Hunter, «The early history of real Money trades», *Terra Nova*, 13 de enero de 2006, disponible en <http://bit.ly/2YtnaSz>.

11. Mark Wallace, «The game is virtual. The profit is real», *The New York Times*, 29 de mayo de 2005, disponible en <https://nyti.ms/2YB4OPh>.

12. Mark Wallace, «The game».

A diferencia del dinero electrónico, las monedas virtuales asociadas a plataformas y sus «cosechas de oro» son las reales antecesoras de las criptomonedas (Nazir, Hamilton y Tee, 2017).<sup>13</sup> Lo que las emparenta es una característica económica que adelanto aquí y revisito en el capítulo «Una generalización económica de las criptomonedas»: ninguno de los dos tipos de moneda está asociada a la existencia de otras monedas corrientes o a *commodities* físicos. Son monedas sin respaldo físico y, por tanto, sin ataduras a las leyes de la física y que, sin embargo, cumplen con características económicas esenciales del respaldo físico del dinero corriente: la escasez y rivalidad (LeBlanc, 2016). Las monedas virtuales y criptomonedas son escasas, son bienes rivales que no se pueden poseer al mismo tiempo por dos personas, no tienen respaldo alguno en el mundo físico y derivan su valor de la aceptación por los usuarios (Graf, 2014: 55-58).

A pesar de existir hace más de quince años, las monedas virtuales no han sido una real amenaza para el dinero de uso corriente por su limitada circulación (Banco Central Europeo, 2012). Aunque algunas de ellas han alcanzado niveles de circulación suficientes para servir como medio de cambio de bienes no relacionados con las plataformas que las sostiene —prominentemente drogas y bienes ilegales (Filipkowski, 2008)— nunca han podido desligarse totalmente de ellas, muchas veces por decisión de sus controladores y sus modelos de negocio (Halaburda y Sarvary, 2016). La decisión de los controladores de mantener las monedas virtuales ligadas a las plataformas, junto con su limitada circulación, impiden que se conviertan en medio de cambio, función esencial de la moneda.

### El problema de la tasa de intercambio de las monedas virtuales

El poder adquisitivo de una moneda virtual fuera de la plataforma para la cual fue creada está sujeto principalmente a la relación de precios entre bienes virtuales dentro de la plataforma y los bienes físicos o virtuales fuera de ella. Esta «tasa de intercambio» es, en principio, análoga a la tasa de intercambio entre divisas que existe entre países. Pero en el caso de países, es el mercado el que determina, en la mayoría de los casos, el valor al que se intercambian las respectivas divisas. Este valor responde a una infinidad de variables, como la disciplina fiscal de los países en cuestión, expectativas de su economía y a lo que se pueda comprar hoy o mañana con las respectivas monedas.

El problema con las monedas virtuales es que el soberano de uno de los «países» —el desarrollador de la plataforma— controla absolutamente la provisión de los bienes dentro la plataforma y sus precios: puede fijar precios de los bienes virtuales como oferente, puede cambiar la utilidad marginal que estos proveen, y puede, ade-

---

13. Denis Rice, «The past».



más, producirlos ilimitadamente a muy bajo costo marginal.<sup>14</sup> Ello siempre expone a quienes poseen estos bienes a devaluación relativa que los convierte en «activos riesgosos».<sup>15</sup> No sin fundamento, ya en 2005 *World of Warcraft* era cuestionado por la opacidad en las tasas de intercambio.<sup>16</sup>

En la distópica novela *Ready player one* de Ernest Cline, la moneda del mundo virtual OASIS era tan importante como el dinero en el mundo real. Morir en OASIS y renacer pobre infundía miedo real y llevaba a suicidios y asesinatos en el mundo real. Pero OASIS tenía billones de usuarios y la vida en él era preferible a la vida en el mundo físico decadente que la novela describe (Cline, 2011). Esto está lejos de ser la realidad de las monedas virtuales. El *WoW Gold* se ofrece en internet desde hace más de una década, pero *World of Warcraft*, que es el juego masivo de multijugador con más usuarios el mundo, no pasa de algunos millones de usuarios y el principal uso de las *WoW Gold*, a pesar de las constantes acusaciones de ser un lugar de lavado de dinero, sigue siendo comprar riquezas del juego. Los Linden Dollars del juego *Second life*, que están diseñados para funcionar como moneda virtual fuera de la plataforma donde fueron creados, tampoco han tenido mucho impacto y su circulación activa es limitada (Grinberg, 2012: 171; Halaburda y Sarvary, 2016: 77-78).<sup>17</sup>

---

14. Jeremy Kelly, «Play time».

15. Por ejemplo, si Blizzard Entertainment, dueño de *World of Warcraft*, decidiera duplicar el precio de todo lo que se vende en la plataforma en su propia moneda, el *WoW Gold*, o disminuir a la mitad los bienes disponibles, habrá en la práctica disminuido a la mitad el valor relativo de su moneda.

16. Daniel Terdiman, «Virtual gaming's elusive exchange rates», *CNET*, 5 de agosto de 2005, disponible en <https://cnet.co/2VFwY9Q>. Los desarrolladores de plataforma no usan normalmente el poder monopólico sobre ellas para derrotar la fe en sus propias monedas virtuales. Por el contrario, utilizan este poder para extender el uso de la plataforma fidelizando usuarios y maximizando la rentabilidad de largo plazo (Halaburda y Sarvary, 2016). Para ello, siguen una estrategia de fijar sus precios conforme a la demanda (Gans y Halaburda, 2015). Esto redirige el problema de la tasa de intercambio de las monedas virtuales a los factores que inciden en la demanda directa por los bienes virtuales de las plataformas, y en esa ecuación pesan primordialmente la cantidad de usuarios y el placer que les produzca jugar el juego o participar en la plataforma. Por ello, la tasa de intercambio de una moneda virtual queda determinada por la popularidad de la plataforma a la que está asociada y por la disposición a jugar de sus usuarios más avezados o la disposición a pagar de sus usuarios más adeptos (Shin, 2008). Estos usuarios *cosechan* las recompensas del juego o las compran. Con ello señalizan a través del tiempo dedicado a jugar y a través de sus pagos en dinero corriente el sacrificio de bienes requerido en el mundo real para obtener los escasos bienes virtuales que la plataforma produce y vende (Heeks, 2009; Yamaguchi, 2004).

17. En todo caso, una moneda virtual cuya ventaja es posibilitar la compra de bienes en un juego que cae en desuso es una moneda sin respaldo siquiera virtual y cuyo valor queda en manos del desarrollador sin ninguna de las restricciones descritas. Este problema podría solucionarse, en parte, incrementando la usabilidad de las monedas virtuales en nuevas plataformas. Si un desarrollador o un grupo de ellos permite creíble y consistentemente a los usuarios migrar su riqueza digital de una plataforma a la otra, atenuaría el problema de la tasa de intercambio que aqueja a las monedas virtuales y facilitaría que se usaran como medio de intercambio y reserva de valor. Esto equivaldría a la creación de un dinero privado virtual con un uso potencial preferente: la experiencia superior en juegos y mundos virtuales.

## El problema del control sobre las monedas virtuales

Un segundo problema de las monedas virtuales asociadas a plataforma que limita su circulación es que son centralizadas. Esto deja la riqueza de las partes —o su identidad y propiedad, si se prefiere— a merced de un tercero que media las transacciones entre ambas. La centralización, si además comprende el derecho a emitir moneda, permite que las monedas virtuales sean objeto de un señoreaje abusivo. El primer problema es un problema de todos los medios de pago electrónicos salvo las criptomonedas. El segundo es un problema particular de las monedas privadas no respaldadas, sean éstas de mundos virtuales o de mundos reales. Entender cada uno de estos riesgos de la centralización por separado es útil para entender el salto evolutivo de las criptomonedas y por qué se acercan más que otras monedas virtuales al papel moneda.

La centralización y los costos asociados a la verificación de transacciones, más la pérdida de anonimato formal que ello conlleva, es inevitable en la transmisión de dinero electrónico. En el caso de las monedas virtuales, un tercero —generalmente el dueño de la plataforma en el caso de las monedas virtuales— tiene que registrar las identidades y las transacciones para evitar que las monedas electrónicas o virtuales se gasten dos veces. Esta contabilización o registro no es necesaria en el caso de una transacción que involucra dinero físico, porque ni siquiera un billete falso se puede usar dos veces. Pero, tal como lo muestra la historia temprana de la riqueza digital, esto no es obvio cuando se trata de archivos digitales que son eminentemente copiables (Graf, 2014: 56). Existe además un incentivo psicológico involucrado en mantener esta doble contabilidad en el caso de mundos virtuales (Shaviro, 2007). Para que dos personas acepten que han celebrado realmente una transacción digital y gasten tiempo y trabajo en obtener las riquezas que luego transfieren en el mundo virtual, el saldo que aumenta en la cuenta de una a propósito de una transacción debe disminuir en la cuenta de la otra.<sup>18</sup>

El problema de la centralización había parecido inevitable hasta la aparición de las criptomonedas (Bonneau y otros, 2015; Nakamoto, 2009). Como señala Satoshi Nakamoto en el artículo con las bases conceptuales de Bitcoin, el problema permanente de las transacciones electrónicas es que requieren un validador, pues «el receptor no puede verificar que el emisor no se haya gastado la moneda dos veces». Este

---

18. Inicialmente, antes de la banda ancha, existieron intentos de lidiar con el problema del intermediario vía una encriptación que hiciera ciegas las transacciones para el intermediario en el caso del dinero electrónico. Esta encriptación protegía la identidad de las partes y, por tanto, al menos de manera parcial, el potencial control malintencionado sobre transacciones particulares (Chaum, 1992). Pero la idea, aplicada en experimentos como DigiCash, no funcionaron comercialmente, pues no fueron lo suficientemente atractivas para diferenciarse de las tarjetas de crédito que los consumidores conocían, y que aprovecharon los efectos de red para tomarse rápidamente el *e-commerce* (Grinberg, 2012: 169).

validador —como señaló correctamente Nakamoto— siempre tendrá poder fáctico sobre las partes de una transacción electrónica (Nakamoto, 2009: 2; la traducción de este artículo es nuestra). Por ejemplo, puede denegarse a cursar los pagos, revertirlos, limitarlos a cierto monto, o utilizar el conocimiento de la identidad de las partes para favorecer a una de ellas o favorecerse a sí mismo. Esto es objetivamente un problema para todos aquéllos que quieren transar electrónicamente con la seguridad y el anonimato equivalentes a los que permite una transacción en dinero corriente entre desconocidos.

El señoreaje sobre las monedas virtuales es potencialmente un problema más difícil de resolver porque el conflicto de interés entre usuarios y el señor o emisor de la moneda virtual es más directo. Los desarrolladores de monedas virtuales no se rigen por instituciones legales que den fe a todos los usuarios de que no cambiarán las reglas o las tasas de intercambio de sus monedas o la cantidad de ellas circulando como lo hacen los bancos centrales. Las monedas virtuales son, por definición, monedas sin respaldo y no reguladas. Por supuesto, emisores podrían amarrarse contractualmente con los usuarios de sus plataformas. Podrían declarar que sus monedas seguirán un patrón estable similar al que tienen las mal denominadas monedas virtuales que reflejan *commodities* o el dinero electrónico. Pero al igual que un dictador que controla la divisa de un país inestable financieramente, el emisor de una moneda virtual siempre puede incrementar su señoreaje, que es el beneficio que tiene ser el controlador de la moneda. Los mecanismos más obvios a su alcance son cambiar el costo en el tiempo de usar la moneda frente a retenerla, o lo que es lo mismo, la tasa de interés de descuento básica de su economía virtual; o aumentar la emisión, lo que da origen a lo que se conoce técnicamente como el impuesto inflacionario. Tanto los desarrolladores de juegos como los patrocinadores de programas de fidelización —como los programas de millas de vuelo— son constantemente acusados de alterar estos factores devaluando sus monedas.<sup>19</sup>

## **La operatoria y ventajas inherentes de las criptomonedas**

La historia y los problemas de las monedas virtuales permiten entender por qué las monedas virtuales han dado tanto que hablar a académicos. Las criptomonedas resuelven en gran parte los problemas de la dependencia de la tasa de intercambio en la demanda por bienes virtuales porque su precio flota libremente conforme a la demanda. Asimismo, las criptomonedas solucionan de manera definitiva el problema de la centralización con la introducción de mecanismos de registro descentralizados que permiten a las partes transar en forma directa sin ninguno de los riesgos aso-

---

19. Kelly Grant, «Saving reward points and miles isn't a sound money strategy», *CNBC*, 3 de agosto de 2016, disponible en <https://cnb.cx/2VCyhGC>; Daniel Terdiman, «Virtual».

ciados a la existencia de intermediarios. Antes de entrar a analizar estas ventajas en profundidad, su potencial impacto económico y los desafíos que imponen al sistema legal, son necesarias algunas nociones de su operatoria. Al igual que la mayoría de los artículos escritos por académicos en el área de las ciencias sociales, esta descripción no pretende ser acuciosa desde un punto de vista computacional.<sup>20</sup>

El *white paper* con las bases conceptuales de Bitcoin, la más popular y extendida de las criptomonedas, sigue siendo un excelente punto de partida para definir todas las criptomonedas en el área de las ciencias sociales y económicas.

Para Satoshi Nakamoto, Bitcoin es:

Un sistema de *efectivo* electrónico [...] basado en prueba criptográfica [...] que permite a las partes transar directamente entre sí sin necesidad de un tercero [que es reemplazado por] una red de par a par (*peer-to-peer*) [descentralizada] que guarda registro cronológico de las transacciones y evita el problema del doble pago (Nakamoto, 2009).

A esta definición algunos autores agregan características como que Bitcoin es un software de código abierto, que permite un cuasianonimato y que tiene costos de transacciones menores a otros sistemas de pago (Brito y Castillo, 2013; Grinberg, 2012).

La operatoria de Bitcoin y todas las criptomonedas que la emulan es tremendamente compleja. Para su estudio es conveniente, siguiendo a Bonneau y sus coautores, dividir el análisis en el de tres componentes del sistema: i) las transacciones encriptadas que mantienen el historial de cada moneda transada e impiden su falsificación; ii) el protocolo que valida y mantiene el registro cronológico de las transacciones y que evita el problema del doble pago o doble uso simultáneo de una misma moneda; y iii) la red de comunicaciones *peer-to-peer* que guarda las copias de las transacciones y el registro anterior de forma descentralizada (Bonneau y otros, 2015; Champagne, 2018: 21). Para efectos de mantener acuciosidad en las referencias, desarrollaré la operatoria de las criptomonedas refiriéndome constantemente a Bitcoin. No obstante, debe entenderse que la descripción en líneas gruesas aplica, salvo que se explicita algo distinto, a la mayoría de las criptomonedas.

---

20. Existe abundante literatura —a la fecha más de 433 artículos indexados en Web of Science— sobre las criptomonedas y sus ventajas y desventajas en diversas áreas del conocimiento. Hace cuatro años solo había 15 artículos indexados en esa base de datos (Spenkelink, 2014). Google Scholar y Scopus sextuplican esta cifra. La revisión exhaustiva de todos los artículos existentes resulta impracticable y, por la especialidad técnica en algunas áreas, inconducente.

## Las transacciones de Bitcoin

En una transacción de Bitcoin, una persona —llamémosla Alice siguiendo la tradición de la literatura de criptografía— envía desde su billetera electrónica un archivo que contiene una llave privada encriptada con datos de una transacción —por ejemplo, cuántos bitcoins o satoshi se envían—<sup>21</sup> a una dirección o llave pública conocida, contenida en la billetera electrónica del computador de Bob, que recibe la transferencia. Esta es la figura básica (Dourado y Brito, 2014; Reid y Harrigan, 2011; Velde y otros, 2013).

La llave privada enviada por Alice a Bob, sin embargo, es una cuerda de 34 caracteres —una serie alfanumérica que técnicamente se denomina *hash*— que se deriva de la dirección pública de Alice, que también es una cuerda de 34 caracteres, y que se recombina matemática y encriptadamente para generar la llave de la transacción. La operación que Alice lleva a cabo para generar la llave que le envía a Bob se denomina técnicamente «firmar» la moneda que se transfiere. Bob sólo puede «ver» en su billetera los bitcoins que Alice le envió porque recibió la llave privada que ella le envió, es decir, los bitcoins con la firma de Alice en su billetera. El total de bitcoins recibidos por Bob conforman una moneda con denominación en bitcoins. Si Bob quiere gastar los bitcoins recibidos de Alice, debe pedirle a su software billetera que genere una nueva llave privada —derivada esta vez de su llave pública en combinación con los datos de una nueva transacción—. Solo con esa llave «firmada» puede volver a enviar los bitcoins. Como cada llave privada que se necesita para transferir se deriva criptográficamente de la llave pública o dirección de quien la transfiere, una operatoria inversa permite descubrir todas las direcciones públicas por las que ha pasado una moneda. Gracias a ello, y en esto radica lo esencial de mecanismo, Bob —y en teoría todos los usuarios de la red Bitcoin— pueden comprobar si Alice era dueña o tenía en su billetera acceso a los bitcoins que le envió a Bob. En esto consiste el sistema de transferencia bajo doble encriptación descrito en casi todos los trabajos sobre monedas virtuales en las áreas de las ciencias sociales (Babaioff y otros, 2012; Böhme y otros, 2015: 215-218; Bonneau y otros, 2015; Brito y Castillo, 2013; Dourado y Brito, 2014; Kroll, Davey y Felten, 2013; Velde y otros, 2013).

Como lo explica de forma muy sencilla Roberts: «Uno puede considerar la llave pública como la ranura de alcancía en la que cualquiera puede depositar [b]itcoins, y la llave privada como la forma secreta de abrir la alcancía que solo conoce el dueño».<sup>22</sup>

---

21. La unidad principal de transacción de la moneda Bitcoin es el bitcoin (1 BTC), la unidad menor es un satoshi (equivalente a 0,00000001 BTC). Usaré en adelante Bitcoin para el sistema de pagos completo y bitcoin para la unidad de cuenta o denominación de pagos hechos con Bitcoin.

22. Jeff John Roberts, «How bitcoin is stolen: 5 commons threats», *Fortune*, 8 de diciembre de 2017, disponible en <http://bit.ly/2M4qZMI>. Una buena representación gráfica animada en inglés de este proceso puede encontrarse en la página «Blockchain demo» del blog de Anders Brownworth, disponible en <https://anders.com/blockchain/>.

La mecánica de la doble encriptación genera una forma de transferir monedas Bitcoin es muy distinta al envío de un archivo. Tampoco se parece a una instrucción para que alguien cargue y debite monedas de una cuenta a otra. Esto último es lo que habitualmente sucede con el dinero electrónico y es la figura que abogados y usuarios acostumbrados a sistemas de pago electrónicos conocen (Khan, 2008; Task Force on Stored-Value Cards, 1996: 660-662).<sup>23</sup>

Las diferencias entre una transferencia de dinero electrónico y de bitcoins son múltiples. De partida, las partes de la transacción no tienen monedas en sus billeteras virtuales, «sino solamente una serie de llaves privadas que les permiten probar que son dueños de las llaves públicas de esas monedas [o direcciones originales antes de la primera transacción] que también se conocen como direcciones Bitcoin».<sup>24</sup>

Un dato curioso de esta operatoria es que cada moneda debe ser transferida en su integridad respecto de cómo se recibió para que su origen pueda ser trazado. Por ello, el emisor debe enviarse el vuelto en bitcoins a sí mismo cada vez que decide usar una moneda que le dio derecho a más bitcoins de los que desea usar en una transacción. El vuelto se convierte en una nueva moneda que puede ser transferida con una nueva llave privada.<sup>25</sup> De manera análoga, monedas recibidas de menor denominación se pueden recombinar para generar una moneda con una denominación en bitcoins más alta.<sup>26</sup> Este diseño tiene varias consecuencias que en teoría importan al derecho y que vale la pena adelantar.

En primer lugar, contrario a lo que sucede con los pagos en el mundo real o los pagos en dinero electrónico, el receptor de una moneda virtual no puede evitar que le «envíen» pagos si la o las direcciones públicas contenidas a su billetera son conocidas. Los pagos hechos en la red Bitcoin son irrechazables o se entienden cursados desde su envío.<sup>27</sup>

En segundo lugar, el envío de bitcoins no es reversible (Bonneau y otros, 2015; Doguet, 2012; Kiviat, 2015; Lemieux, 2016; Nakamoto, 2009; Simonetti Rojas, 2017: 27). El receptor podría hacer la transacción inversa, si el emisor y receptor se cono-

---

23. Rich Apodaca, «Bitcoin: Think of it as electronic cash», *Bitzuma*, 28 de septiembre de 2017, disponible en <http://bit.ly/2Vz8wQA>.

24. George Kimionis, respuesta a consulta «Can a wallet deny payments to it?» en Bitcoin Stack Exchange, 8 de enero de 2015, disponible en <https://bitcoin.stackexchange.com/a/35368>.

25. «Change», Bitcoin Wiki, 25 de julio de 2017, disponible en <https://en.bitcoin.it/wiki/Change>.

26. La analogía entre las criptomonedas y las monedas metálicas es reconocidamente gruesa, pero la operatoria de las transacciones en Bitcoin es como si cada moneda fuera un barra o lingote de oro que se derrite en cada transacción, se vuelve a fundir con un cuño que los dueños se van pasando unos a otros, y que tiene la historia de las direcciones donde se ha usado ese oro desde que se extrajo de la tierra. En esta operatoria el dueño sólo puede reclamar dominio sobre las monedas porque tiene en su poder el cuño que permite trazar el oro de la moneda que fundirá hasta su origen. Rich Apodaca, «Bitcoin».

27. «Change», Bitcoin Wiki.

cen y desean hacerlo. Un juez o árbitro también podría ordenarlo si las partes le han dado poder para hacerlo y han programado su intervención digitalmente dentro de la misma transacción. Pero la operatoria directa entre partes anónimas en Bitcoin es normalmente incondicionada y unidireccional. Por lo tanto, para sujetar las transacciones a condiciones es necesario programar el envío a un fideicomisario (*Bitcoin escrow*) (Brito, Shadab y Castillo, 2015: 206-208). Algunas criptomonedas permiten que las condiciones de pago se programen en la misma transferencia y se verifiquen automáticamente, lo que se denomina un «contrato inteligente» (Bonneau y otros, 2015; McJohn y McJohn, 2016; Szabo, 1997).<sup>28</sup> En la parte denominada «Una generalización legal de las criptomonedas» analizo las implicancias legales de éste u otros problemas que se derivan de la operatoria de criptomonedas.

### El protocolo de Bitcoin (y algunas explicaciones de Blockchain)

Una transacción de [bitcoins] sería insegura si las transacciones fueran simplemente enviadas de usuario a usuario. Ello porque si bien [el sistema criptográfico] puede asegurar que el remitente envió el pago de una transacción que era válida dadas las transacciones anteriores, no hay nada en las transacciones mismas que impida que Alice realice dos transacciones con Bob y Carol simultáneamente en dos transacciones que separadamente parecerían válidas (Bonneau y otros, 2015: 106).

Este es el problema del doble pago al que hace referencia Nakamoto en el *white paper* que dio origen a Bitcoin. El doble pago se produce porque cada moneda en sí misma puede ser trazada a origen por cada usuario individualmente, pero nadie puede estar seguro de que otro usuario no la haya recibido al mismo tiempo (Nakamoto, 2009). Si a esto se le suma la latencia de la red, el resultado puede ser dobles pagos o fraudes masivos (*double-spending problem*).

Para resolver el problema del doble pago, el protocolo Bitcoin tiene una norma sustantiva y una norma procesal. La norma sustantiva señala que sólo el primer uso de una moneda es válido y todos los demás deben ser descartados conforme lo verifique la mayoría de los miembros de la red de usuarios. Esto reenvía el problema a determinar cuál es realmente el primer uso, y aquí es donde entra a jugar la norma procesal. En un escenario en que no existe un validador centralizado y, por tanto, tampoco un reloj único para todas las transacciones (como lo sería el reloj de la oficina de protección de patentes), el tiempo absoluto no sirve como parámetro. Cualquier transacción puede ser antedatada, lo que abre la posibilidad a infinitos

---

28. Vitalik Buterin, «Ethereum white paper: Next generation smart contract and decentralized platform». *Brave New Coin*, 20 de agosto de 2014, disponible en <http://bit.ly/2IiyxFY>; «Not-so-clever contracts», Schumpeter, *The Economist*, 28 de julio de 2016, disponible en <https://econ.st/2VCP2RJ>.

dobles-usos y fraudes. La respuesta a este problema es un registro *ordinal* y encadenado, que nadie puede controlar y que crece por consenso, y que le dice a toda la red cuál ha sido el orden cronológico de las transacciones desde que se iniciaron las transacciones. Este registro, en el caso de Bitcoin, se denomina Blockchain o «cadena de bloques» y su mecánica es esencial para entender por qué Bitcoin puede funcionar sin intermediarios.

La operatoria de Blockchain es el resultado de una serie de reglas que coordina a los computadores o nodos de la red Bitcoin y que busca reemplazar «democráticamente» a una autoridad central que valide las transacciones. ¿Cómo funciona este ingenioso sistema de consenso colectivo «para fijar el tiempo relativo de las transacciones» que ha dado tanto que hablar como el mismo Bitcoin?<sup>29</sup>

El sistema de Blockchain crece por bloques o grupos de transacciones que son fechadas o guardadas ordinalmente en el bloque que las contiene dentro del registro digital. El protocolo sólo permite cerrar un bloque —si prefiere, firmar la hoja de un libro de registro de transacciones para cerrarla— a usuarios especializados de la red que se dedican a resolver problemas matemáticos con un alto grado de aleatoriedad y que requieren mucha capacidad computacional.<sup>30</sup> Estos usuarios se denominan «mineros». Los bloques se cierran cuando un minero que propuso un bloque con transacciones pendientes que sean validables logra resolver el problema matemático requerido que «cristaliza» o «sella» el bloque. El minero que resuelve el bloque o cierra la hoja del libro recibe como pago bitcoins que la red misma genera por este proceso, de ahí el apelativo de «minero». Además, recibe comisiones por las transacciones pendientes validadas. El consenso entre mineros sobre un bloque cerrado se constata cuando los mineros deciden moverse a descifrar un nuevo problema para cerrar el siguiente bloque.<sup>31</sup>

El trabajo de elegir transacciones en apariencia válidas para proponer un bloque y luego competir por resolver un problema matemático para cerrarlo, la denominada «prueba de trabajo» (*proof-of-work*) que ejecutan los mineros, cumple varias funciones en la red Bitcoin y, como mostraré más adelante, respecto de Bitcoin como moneda.

Respecto de la red, la prueba de trabajo y su pago en bitcoins genera incentivos para que los mineros mantengan el registro cronológico de transacciones y asegura

---

29. Tom Espiner, «Is blockchain living up to the hype?», *BBC News*, 23 de octubre de 2018, disponible en <https://bbc.in/2VDIwds>.

30. El balance entre capacidad y suerte para cerrar bloques disminuye, en parte, la posibilidad de que éstas siempre sean cerradas por la misma persona y evitan que el minero con mayor poder de procesamiento computacional se vuelva en los hechos un controlador del registro de transacciones (Bonneau y otros, 2015).

31. Una presentación gráfica animada en inglés de este proceso puede verse en «Blockchain demo» del blog de Anders Brownworth.



que todas las transacciones individuales sean rápidamente validadas apenas son notificadas a la red (Kroll, Davey y Felten, 2013). Esto minimiza el problema del desfase en la validación de transacciones y, por tanto, el problema del doble pago.<sup>32</sup> Hoy, para la mayoría de los usuarios de la red Bitcoin, 50 minutos es suficiente para confirmar con seguridad que la moneda que se recibió no ha sido utilizada dos veces y puede volver a ser utilizada.<sup>33</sup>

Blockchain fue el primer registro contable distribuido o DLT (*distributed, ledger technologies*) o DAO (*decentralized autonomous organization*). Existen cientos de variaciones de DLT o DAO que emulan el funcionamiento de Blockchain para otros usos (Maupin, 2017; Reyes, 2016). A pesar de que han surgido muchas críticas al funcionamiento de Blockchain porque su particular diseño tiene problemas de escalabilidad (Croman y otros, 2016) y porque su sistema de validación de transacciones es costoso en términos de la energía gastada por los computadores para resolver los problemas que permiten cerrar un bloque y no se ajusta a la entidad de las transacciones que procesa, de acuerdo con muchos, Blockchain, el primer DLT, es la principal innovación computacional que trajo Bitcoin al mundo, un invento tan revolucionario como la misma internet (Fenwick, Kaal y Vermeulen, 2017: 363; Kiviat, 2015: 573; Tapscott y Tapscott, 2016).

## La red Bitcoin

Finalmente, el tercer componente, quizás el menos innovador pero estructuralmente esencial, es la red de usuario a usuario (*peer-to-peer*) sobre la que se envían las llaves privadas, se mantienen las llaves públicas, se anuncian las nuevas transacciones y se proponen los nuevos bloques que se agregan a la cadena de Blockchain (Bonneau y otros, 2015: 108).

---

32. Normalmente, dado que las transacciones de bitcoins pueden quedar pendientes por algunos minutos antes de ser incorporadas en un bloque, muchas billeteras electrónicas requieren que una transacción tenga al menos cinco o seis bloques de antigüedad antes de considerarlas completamente validadas (Bonneau y otros, 2015). El sitio <http://data.bitcoinity.org> entrega datos en tiempo real de la demora en que se crean los bloques y la velocidad se ha mantenido estable entre nueve y diez minutos, como fue diseñado. Por ello, para la mayoría de los usuarios, 50 minutos es el tiempo que media entre transacción y transacción con las mismas monedas, sin perjuicio de que todas las ellas son irreversibles entre las partes desde el momento en que se generan.

33. Nótese que cuando no hay consenso entre los mineros, éstos pueden trabajar en cadenas paralelas —con transacciones que divergen— armando lo que denomina una bifurcación en la cadena (*fork*). Pero dado que es difícil que una cadena que contiene transacciones no válidas convenza a más del 50% de la red por mucho tiempo, sobre todo en criptomonedas consolidadas como Bitcoin, y dado que seguir manteniendo una cadena falsa y discrepante resolviendo los problemas matemáticos requeridos para hacerla crecer es, por diseño, antieconómico, las cadenas discrepantes eventualmente mueren y los mineros convergen a la cadena más larga (Doguet, 2012: 1.127; Nakamoto, 2009: 3).

La red de anuncios y su apertura es vital para evitar que mensajes de transferencias sean alterados por un grupo malicioso con exceso de poder computacional. Los nodos en la red de Bitcoin se conectan aleatoriamente al menos con ocho conexiones hacia fuera, y hasta con 125 hacia adentro. Los nodos en conexiones de teléfono no reciben conexiones desde fuera. Para conectar por primera vez las billeteras electrónicas en los computadores de los usuarios se conectan a servidores dedicados o nodos semilla (Bonneau y otros, 2015). Existen programas de billetera que descargan la cadena del Blockchain completa localmente antes de iniciar transacciones y otros programas de billetera que confían en las cadenas que están guardadas en discos de terceros. En cualquier caso, los usuarios pueden establecer en la mayoría de los softwares que solo desean guardar los últimos bloques de la cadena Blockchain localmente. Con esto es suficiente para operar sin necesidad de tener la historia con claves encriptadas de cada moneda transada desde su origen, localmente. Vale la pena reiterar, descargar la cadena con el historial de bloques cerrados y con transacciones validadas es distinto de la actividad de cerrar bloques que ejecutan los mineros.

### **Una generalización económica de las criptomonedas**

Desde el punto de vista económico, la genialidad de las criptomonedas no es el hecho de que puedan transarse sin intermediarios o que no requieran fe (*trustless*) (Bonneau y otros, 2015; Karlstrøm, 2014). Sin duda esto es computacionalmente revolucionario y, como revisaré, un desafío particular para las instituciones legales existentes que regulan las monedas tradicionales principalmente *a través* de quienes las intermedian. Tampoco es el hecho de que sean más portables, divisibles, imperecederas, prácticamente infalsificables, que permitan el anonimato y tengan menores costos de transacción, por mencionar algunas de las atribuciones tradicionales de las monedas en las que las criptomonedas destacan.

Económicamente, la genialidad de las criptomonedas radica en su capacidad de funcionar con una escasez creíble o predecible en un ambiente donde la escasez no es natural. Las criptomonedas tienen la capacidad de generar escasez de la oferta monetaria porque su producción está atada a la «prueba de trabajo» que mantiene la misma red de pagos, y porque esta última está gobernada por desafíos matemáticos adaptativos que requieren de esfuerzo e inversión reales, pero que son comprensibles por todos los usuarios y están abiertos a todos los que quieran resolverlos. Bitcoin, en particular, debe su éxito a esta predictibilidad que fue el incentivo a su adopción temprana. Sólo puedo tratar aquí someramente y a modo de ensayo en qué consiste esta genialidad y cuáles son las limitaciones que se derivan de ella para las criptomonedas como monedas.

## El respaldo de las monedas virtuales

Las monedas derivan su utilidad de lo que se puede comprar con ellas y su poder de compra se basa en la fe que tengan quienes la reciben en pago de poder volver a usarlas. Hace más de un siglo que el oro no se usa como moneda y hace más de 80 años que no se usa como respaldo de moneda. Ni siquiera las mal llamadas monedas virtuales que se respaldan en oro como Goldcoin son realmente monedas. El oro sigue siendo un activo seguro para muchas personas y, por tanto, sirve como instrumento de reserva de valor (Barro y Misra, 2016). Pero dejó de ser unidad de cuenta y medio de cambio, que son las otras funciones clásicas del dinero, porque fue reemplazado por «mejores» monedas. Su historia sirve para ilustrar un popular teorema sobre el origen del valor de cambio del dinero.

Fue Carl Menger, fundador de la escuela austríaca, quien sugirió que la «usabilidad» de una nueva moneda o su liquidez era lo que le permitía imponerse a otras monedas existentes. El triunfo de una moneda, teorizó Menger, se reconoce cuando la nueva moneda comienza a ser el precio de referencia de los otros bienes (Davidson y Block, 2015).

Basado en la idea de Menger, Ludwig von Mises, otro renombrado académico de la escuela austríaca, postuló que toda moneda existente surge de otra moneda, o si se prefiere, hereda su valor de cambio de otra moneda y así sucesivamente hasta que se llega a algún *commodity* usado como moneda por su valor de uso o valor intrínseco (Davidson y Block, 2015: 315-319). Este teorema sobre el respaldo de las monedas se conoce como la «regresión de Von Mises», y como tal enfatiza las expectativas, la subjetividad y el rol de la estructura de precios en la sustitución de una moneda por otra (Rothbard, 1992; Selgin, 1994: 809-810). El oro es un *commodity* de valor intrínseco como joya que pasó a ser moneda, triunfó como tal, luego se convirtió en respaldo de monedas más usables a las que dio credibilidad, las que a su vez dieron origen a muchas de las monedas actualmente en circulación. Los dólares norteamericanos y el peso chileno cumplen cabalmente con la regresión de Von Mises.

Existen acalorados debates respecto de si las criptomonedas como Bitcoin cumplen o no con la regresión de Von Mises, y en el caso de no cumplirlas, cuál sería su respaldo.<sup>34</sup> Si Bitcoin no tiene valor de uso como los *commodities* y no deriva su valor de otra moneda, y sin embargo llega a convertirse en moneda o medio de cambio de alta circulación, derrotarían la hasta ahora incólume regresión de Von Mises (David-

---

34. Patrik Korda, «Bitcoin bubble 2.0», *Patrik Korda's Blog*, 5 de marzo de 2013, disponible en <http://bit.ly/2LZrEym>; Patrick Murphy, «On Bitcoin and Ludwig von Mises' regression theorem», *Free Advice*, 10 de marzo de 2014, disponible en <http://bit.ly/2Mo7eoY>; Michael Suede, «The economics of Bitcoin – Challenging Mises' regression theorem», *Libertarian News*, 7 de julio de 2011, disponible en <http://bit.ly/2M3l88Q>; Peter Šurda, «Re: Bitcoin bubble 2.0 by Patrik Korda», *Economics of Bitcoin*, 6 de marzo de 2013, disponible en <http://bit.ly/2LYZzqP>.

son y Block, 2015). En este debate están quienes sostienen que Bitcoin no desafiaría el teorema, pues si bien no heredaría su valor de cambio de ningún *commodity* o moneda existente, sí habría tenido algún valor de uso anterior a convertirse en medio de cambio (Graf, 2014). Su valor, dicen sus defensores, podría estar justificado como un intento de soportar la causa libertaria.<sup>35</sup> Para los oponentes, en cambio, la pregunta sería impertinente, pues Bitcoin no tendría suficiente circulación para ser considerada moneda, lo que haría el teorema inaplicable (Yermack, 2015). Lo importante del teorema, enfatizan estos últimos autores, es que una moneda debe ser heredera de otra moneda en todo lo que implica la formación de expectativas de ser unidad de cuenta y medio de cambio.

Independientemente de si las criptomonedas cumplen o no con la regresión de Von Mises, ambas partes tienen razón en sus premisas básicas. El valor de cambio de las criptomonedas no se desprende de ningún *commodity* tradicional. Bitcoin, por ejemplo, fue creado como medio de cambio y parece haber sido adoptado *de novo* por su potencial valor como medio de cambio (Graf, 2014). Según Graf, la prueba de trabajo que ejecutan los mineros que mantienen la cadena de Blockchain, y el hardware y la electricidad que usan para minar, no pueden ser considerados respaldo, pues la actividad de minar bitcoins no tiene otro uso fuera de la red Bitcoin.<sup>36</sup>

No obstante la falta de respaldo o bienes físicos —y en esto tienen razón los detractores en el debate—, las criptomonedas no son monedas. Como lo muestran diversos trabajos, Bitcoin y otras criptomonedas no cumplen con la condición de ser un medio de cambio de amplia circulación y sus denominaciones no sirven de precio de referencia de otros bienes debido a su volatilidad (Bedecarratz, 2018: 81; Lo y Wang, 2014; Spenkelnik, 2014).<sup>37</sup> Las criptomonedas no solo son menos líquidas que el oro

---

35. Peter Šurda, «Re: Bitcoin».

36. La prueba de trabajo de los mineros calza mejor con la concepción de Adam Smith de cómo se genera riqueza y con el concepto de escasez, pero en el mundo virtual. Smith señaló que el trabajo «fue el precio primitivo, la moneda original adquirente que se pagó en el mundo por todas las cosas permutables. No con el oro, no con la plata, sino con el trabajo se compró originalmente en el mundo todo género de riqueza (Smith, 1794: 50; véase también Peach, 2009: 393). Las criptomonedas y sus antecesores nacieron con los mundos virtuales y —como si sus diseñadores hubieran querido complacer a Smith— con la escasez programada en ellos. El trabajo requerido para obtener las riquezas (*real money trading*, RMT) —por humanos jugando en el caso de los juegos o el trabajo de computadores resolviendo problemas matemáticos en el caso de las criptomonedas— es el precio primitivo o la moneda original que respalda las criptomonedas (véase la sección «La creación de riqueza digital»).

37. La cantidad de criptomonedas circulando, es decir, el total de valor que podría comprar con todas las criptomonedas relevantes en su valor en dólares no supera los 135,1 mil millones de dólares a marzo de 2019, lo que es insignificante si se compara con los 7 billones de dólares en reservas de oro. Toju Ometoruwa, «Understanding cryptocurrency market capitalization», MTC Manager, 9 de marzo de 2019, disponible en <http://bit.ly/2M11nQj>. También el monto es insignificante o con los 5 billones de dólares americanos físicos que circulan en el mundo. Mitchell Hartman, «Here's how much money there is in

y que el dinero: el total de ellas no alcanza a ser el 1,9% del valor del oro mundial, ni cubren el 0,01% del producto mundial al 2018.

Financieramente, las criptomonedas se comportan como un *commodity* artificial con un precio volátil. Selgin (2015), tratando de terciar el debate, denomina a las criptomonedas «monedas derivadas de mercancías sintéticas» (*synthetic commodity money*). Yo sostengo que las criptomonedas responden mucho mejor a una teoría del valor del trabajo requerida para vencer una escasez virtual. Una alternativa para explicar su sustento económico sería denominarlas «monedas virtuales descentralizadas de escasez programada».

Concediendo que los bitcoins no tienen la circulación requerida para desafiar la regresión de Von Mises —aunque ya es un éxito que tengan valor positivo en términos de otra moneda—, la pregunta que sigue es cómo empezó en la práctica a ser Bitcoin intercambiado. ¿Qué fue lo que dio valor cambio? La clave para responder a esta pregunta está en una opción que Satoshi Nakamoto tomó al crear Bitcoin. Esta decisión orienta toda la discusión económica sobre las criptomonedas y la necesidad de regularlas.

### El dilema entre retener el control de la moneda o liberarlo

Todo creador de una moneda virtual o una criptomoneda enfrenta un dilema al momento de crearla: puede retener el control de la oferta monetaria o puede abandonar el control de la misma. Si decide mantener el control habrá creado una nueva forma de dinero privado virtual. En este caso podrá beneficiarse de ser el señor o emisor de la moneda, como se explicó en la sección «El problema del control sobre las monedas virtuales». Si decide, en cambio, desligarse del control, tendrá que obtener su utilidad como usuario de ésta. Las diferencias entre ambas opciones desde un punto de vista económico y legal son radicales.

Mantener el control de una moneda virtual privada implica gatillar todos los problemas asociados a la tasa de intercambio y la centralización revisadas anteriormente. Es difícil que una moneda virtual centralizada genere suficiente consenso en la población para convertirse en un medio de cambio de alta circulación. El problema se agudiza por las posibilidades de que surja competencia. Nadie razonablemente querría correr el riesgo de ser expropiado por un controlador de una moneda, en particular si tiene otras alternativas de monedas más fiables que le permitan reservar dinero e intercambiar los bienes que necesita.<sup>38</sup>

---

the world – and why you’ve never heard the exact number», *Business Insider*, 17 de noviembre de 2017, disponible en <http://bit.ly/2M2nwxO>

38. Los mismos Estados han enfrentado competencia de monedas privadas a lo largo de la historia cuando han enfrentado debilidad financiera o falta de credibilidad. Si en la mayoría de los casos el di-

En cambio, si el creador de una moneda virtual decide entregar el control de la oferta monetaria a un sistema que no dependa de su voluntad, no tendrá el problema de las tasas de intercambio ni podrá aprovecharse del poder de la centralización. Con ello habrá resuelto gran parte de las sospechas permanentes que recaen sobre el dinero privado virtual y no virtual. Pero aun así tendrá que incitar a los usuarios a que adopten su moneda. Para ello deberá ofrecer una criptomoneda que sea tecnológicamente superior y que, por tanto, cumpla las condiciones para superar monedas existentes en alguna o en todas las formas de intercambio donde éstas reinan (Halaburda y Sarvary, 2016: 29-30). Pero, además, deberá poner un incentivo a los primeros adoptantes para que inicien a su costo la circulación y soporten la infraestructura requerida para que la moneda circule antes de percibir los efectos de red y el consecuente aumento de valor de cambio (Halaburda y Sarvary, 2016: 37-41). La genialidad de Bitcoin está precisamente en cómo su creador diseñó este incentivo para la adopción temprana.<sup>39</sup>

Desde el un punto de vista monetario, la actividad de los mineros —la prueba de trabajo— determina de forma *predecible* el crecimiento autónomo de la oferta de bitcoins, y eso facilitó su adopción. No se puede incorporar nuevos bitcoins a la masa existente comprándoselos a alguien. Tampoco hay un banco emisor de bitcoins. No existe otra forma de crear bitcoins que no sea obteniendo premios por cerrar bloques. Cada bitcoin que existe, o fue minado por el mismo Nakamoto y otros usuarios

---

nero estatal ha prevalecido es por coerción monopólica y porque los Estados han hecho esfuerzos por comprometerse legalmente a que su dinero retenga su valor más allá de declarar legalmente su poder liberatorio. Por ejemplo, le han otorgado a *su* dinero la posibilidad de extinguir deudas públicas, que como señala Wray «es lo que se necesita para pagar impuestos» (Barber, 2015). Y han garantizado que compararán y extinguirán su moneda «si su valor real empieza a caer mucho más de 2% al año» (Brad DeLong, «Watching Bitcoin, Dogecoin, etc...», Washington Center for Equitable Growth, 28 de diciembre de 2013, disponible en <http://bit.ly/2LZmGS9>). Quizás gigantes como Amazon o Facebook podrían intentar imponer sus monedas privadas basadas en su prestigio o el tamaño de sus redes y usuarios cautivos sin tener el poder coercitivo del Estado y sin haber asumido compromiso respecto de mantener el valor de sus monedas (Halaburda y Sarvary, 2016). La mayoría de los emisores de criptomonedas privadas que quieran retener el control de éstas tendrán que buscar formas de respaldarlas si quieren que su creación sea aceptada y ceder en parte el control. Tratarán, por ejemplo, de establecer un beneficio al que solo se pueda acceder con su moneda o tratar de atarla a un *commodity*. En este último caso, deberán demostrar que tienen el *commodity* en cantidades suficientes, algo que hasta el momento todos los creadores de monedas virtuales que han seguido esta estrategia han fallado en demostrar (Roubini, 2018).

39. A veces se describe el éxito de Bitcoin como el resultado de aplicar técnicas de «criptoeconomía», que es aplicar conocimientos de criptografía y de economía para diseñar protocolos y aplicaciones robustas que tengan incentivos para los adoptantes humanos que necesitan decidir participar en ellos. En concreto, la criptoeconomía consistiría en el diseño de mecanismos que contengan incentivos para que usuarios participen, y podría ser considerado un subcampo de la microeconomía y la teoría de juegos. Alex Evans, «A crash course in mechanism design for cryptoeconomic applications», *Block Channel*, 16 de octubre de 2017, disponible en <http://bit.ly/2LZBcJI>.

cuando su costo era inexistente o bajísimo —porque los problemas a resolver eran simples y requerían baja capacidad de procesamiento—, o ha sido el resultado de los premios a mineros desde que minar se convirtió en una actividad económica. El pago que hace Bitcoin a los mineros fue la clave que incentivó la adopción que le permitió a Bitcoin romper el estrecho ámbito de circulación de las monedas virtuales existentes.<sup>40</sup>

Tal como señala en retrospectiva Chris Ellis de *Fathercoin*, para que una criptomoneda sea exitosa el único ingrediente verdaderamente esencial es una comunidad dispuesta a aceptarla.<sup>41</sup> Se especula que la persona o grupo de personas que crearon Bitcoin bajo el seudónimo de Satoshi Nakamoto son millonarios por haber acaparado bitcoins anónimamente cuando el costo de hacerlo era ínfimo (Champagne, 2018).

### El dilema entre facilitar la adopción temprana y la estabilidad de precios

Si fuera simplemente por asegurar la adopción temprana y obtener beneficios de diseñar una moneda anónimamente —algo tan obvio que muchos criptoimitadores de Bitcoin han sido acusados de ser esquemas de Ponzi (Roubini, 2018)—, todos los desarrolladores de criptomonedas debieran seguir la misma estrategia de Nakamoto. El problema de esta estrategia es que tiene un costo en el mediano y largo plazo. Como la oferta de moneda debe ser conocida y estable para incentivar la adopción, ésta no puede ajustarse a la demanda, lo que genera volatilidad de precios y frustra la función de ser medio de cambio. Como señala Yermack:

Aunque algunos entusiastas han sugerido una conexión entre la tasa de crecimiento determinado por algoritmos de Bitcoin y la ortodoxia defendida por Milton Friedman [que propuso una función de crecimiento del dinero estable e independiente del Gobierno], el protocolo de Bitcoin parece prestar poca o ninguna atención a la tasa óptima de crecimiento de la masa monetaria (Yermack, 2015: 34).

Cuando la oferta de una moneda no se ajusta a la demanda por la misma, la moneda en cuestión se convierte en deflacionaria. Esto implica que todo lo que se transa

---

40. Sea lo que sea que se diga respecto del idealismo de los primeros adoptantes, el éxito en la adopción de Bitcoin se debe a los incentivos económicos que generaron la comunidad visionaria que le dio sustento. Joshua Davis, «The crypto-currency», *The New Yorker*, 3 de octubre de 2011, disponible en <http://bit.ly/2M4ZXEn>.

41. Michael Grothaus, «How to create your own cryptocurrency», *Fast Company*, 29 de enero de 2014, disponible en <http://bit.ly/2MdoFCq>. Esto es otra característica de la evolución de la moneda que Carl Menger anticipó hace más de un siglo: «Nada ha sido más favorable a la génesis de un nuevo medio de cambio que la aceptación por parte de los sujetos económicos más conscientes y capaces que buscan su propia ganancia y por un buen periodo de tiempo, de un bien eminentemente líquido» (Álvarez y Bignon, 2013: 98; traducción propia).

en bitcoins tendría que bajar su precio en bitcoins constantemente. El costo de obtener la adopción temprana con reglas de crecimiento de la oferta predecibles e inalterables unilateralmente y que sólo se pueden cambiar por consensos que son difíciles de obtener, ha tenido como contrapartida que el precio de las criptomonedas ha sido muy volátil y que, por tanto, las personas no usen bitcoins como medio de cambio ni como unidad de cuenta. Como señala Nouriel Roubini:

La supuesta ventaja de Bitcoin es también su talón de Aquiles, porque incluso si [ya] tuviera una oferta estable de 21 millones [límite de bitcoins que todavía no se ha alcanzado], eso la descalificaría como una moneda viable. A menos que la oferta de una moneda siga el crecimiento del producto, los precios tendrán que sufrir una devaluación (Roubini, 2018).

### El dilema entre la escalabilidad y la seguridad de las criptomonedas

Los problemas descritos por Yermack y por Roubini son conocidos por la comunidad de las criptomonedas desde sus inicios y han sido debatidos. Roubini (2018) bautizó el problema como la «trinidad inconsistente», siguiendo las ideas de uno de los fundadores de una criptomoneda que intentó superar las deficiencias de Bitcoin. Me referiré a esta idea como el «teorema de la imposibilidad de Buterin», respecto de las criptomonedas, en honor a quien lo planteó originalmente.

Vitalik Buterin, en *white paper* que creó Ethereum, una criptomoneda destinada a superar la rigidez de Bitcoin, señaló que las criptomonedas no podían tener al mismo tiempo: i) escalabilidad, es decir, la posibilidad de ajustar la oferta monetaria rápidamente para mantener precios estables y para funcionar como medio de cambio; ii) descentralización, y iii) seguridad. De acuerdo con Buterin, habría que renunciar siempre a una de estas características en el diseño de una criptomoneda para obtener las otras dos.<sup>42</sup> Su teorema es sólido si se contrasta con la evidencia histórica que tenemos de las monedas. Los bancos centrales ofrecen escalabilidad y seguridad, pero son centralizados y controlan la oferta de moneda. Los sistemas descentralizados de las monedas existentes podrían tener más flexibilidad y escalabilidad, pero a costa de la seguridad en la red que debe ir validando las transacciones. Este problema ha sido comprobado con nuevas criptomonedas o *altcoins* que, aunque más escalables en diseño que Bitcoin, son atacadas con éxito por mineros de monedas consolidadas en lo que se denomina un ataque del 51%.<sup>43</sup> Y si se quiere tener un sistema seguro y al mismo tiempo escalable, se debe retener de alguna forma la centralización. Esta

---

42. Vitaly Buterin, «Ethereum».

43. «Bitcoin scams and cryptocurrency hacks list», Bitcoin Exchange Guide, disponible en <http://bit.ly/2M12q2j>.



última fue la apuesta de Ethereum y de otras criptomonedas como Peercoin. Sus protocolos, denominados «prueba de interés» (*proof-of-stake*), le otorgan más peso en el consenso requerido para validar transacciones al usuario que tiene más interés en el destino de la moneda, lo que implica un cierto grado de centralización.

Para concluir respecto de la economía de las criptomonedas, es importante señalar que existen numerosos artículos que proponen mejoras a los protocolos de Bitcoin y de otras criptomonedas populares. Entre las mejoras se busca romper funcionalmente el teorema de la imposibilidad de Buterin haciendo que las criptomonedas descentralizadas y seguras —que son las que demandan mayor capacidad de procesamiento para mantener registros descentralizados inviolables y que actualmente son criticadas por el consumo de energía que requieren—<sup>44</sup> sean asimismo más escalables y, por tanto, permitan que las criptomonedas funcionen como medio de cambio (Ametrano, 2016a, 2016b; Dwyer, 2015; Fung, Molico y Stuber, 2014; Halaburda y Sarvary, 2016; Iwamura y otros, 2014; Selgin, 2015). Estas modificaciones no dejan de tener, en todo caso, riesgo. Dado que deben ser aceptadas por más de la mitad de la red, si la mayoría de los usuarios que se dedican a validar transacciones no logran acordar cambios en los protocolos para implementar mejoras, puede producirse lo que se denomina un *hard fork* o bifurcación dura. En este caso, grupos de nodos de la red quedan funcionando con el protocolo antiguo y otros grupos con el protocolo nuevo, lo que en la práctica da a origen a una nueva criptomoneda.

Con las ideas rudimentarias descritas hasta aquí respecto del origen de las criptomonedas, su funcionamiento técnico y su lógica económica, es posible ahora especular qué tiene que decir el derecho al respecto.

## Una generalización legal de las criptomonedas

El estado del arte del estudio de las criptomonedas en el área del derecho es primario y menor al que se observa en áreas como la ciencia economía.<sup>45</sup> La situación es comprensible. Se trata de una situación enteramente nueva respecto de la cual el de-

---

44. Nathaniel Popper, «El consumo de energía que requiere Bitcoin no es nada trivial», *The New York Times*, 24 de enero de 2018, disponible en <https://nyti.ms/zM2XOch>.

45. Desde que Bitcoin naciera en 2009 ha atraído la atención de numerosos académicos en el área del derecho anglosajón, tanto en áreas de doctrina y jurisprudencia, como en áreas periféricas. En la base de datos anglosajona Heinonline Law Journal Library, que contiene 2.600 periódicos y revistas académicas relacionadas con el derecho, ya existen más de 551 que contienen la palabra criptomonedas o derivados. (Datos obtenidos utilizando los resultados de búsqueda de «cryptocurr\*» en HeinOnline Law Journal Library). Bases de datos como Scielo/Scopus (español), Westlaw (México), Westlaw (Chile), ScienceDirect (español) combinadas arrojan una docena de artículos en español. Dialnet y Google Scholar en español tienen centenas de fuentes, pero muchas de ellas correspondientes a artículos no indexados o breves análisis en periódicos legales.

recho positivo tiene pocas respuestas. Con el dinero electrónico fue fácil adaptar las categorías y conceptos existentes, pues las partes y el contenido de las obligaciones, y en general todo lo que interesa al derecho, permanecieron prácticamente inalterados (Khan, 2008; Rogers, 2005). Además, la regulación del dinero electrónico tenía destinatarios obvios que ya estaban sometidos a regulación: los bancos e intermediarios financieros que se llevaron la mayoría de la carga de las innovaciones legales en la materia.

Con las criptomonedas, en cambio, las categorías y conceptos legales existentes, desde los aplicables a la definición de riqueza o de propiedad, a la tradición, a los intermediarios, a la intervención de la fuerza y otros, son difíciles de extender y no funcionan bien en los ambientes virtuales que les sirven de antecedente y sustento (Bartle, 2004; Graf, 2015). Los problemas derivados de la autoejecución de contratos, la irreversibilidad de las transacciones y la existencia de partes anónimas, entre otros, son todos aspectos en que los que el derecho positivo aparece irremediamente sobrepasado.

Para ilustrarlo, usaré como referencia el caso chileno y su tratamiento de Bitcoin. En todo caso, el análisis es aplicable con pequeños ajustes a todas las jurisdicciones de derecho continental.

### ¿Qué tipo de bien son las criptomonedas? El problema de la naturaleza jurídica

De acuerdo con Pérez Abarca y Simonetti Rojas, los bitcoins en Chile serían una cosa no prohibida, por tanto, objeto de comercio humano. Discurriendo sobre qué cosa sería y dado que los bitcoins no están sancionados como dinero por el Estado chileno, Pérez Abarca (2015: 78-80) los declara «divisas», lo que coincide con la jurisprudencia internacional europea. Simonetti Rojas (2017: 38), en cambio, siguiendo la jurisprudencia norteamericana, los denomina «bienes muebles digitales». Esto último equivale a declararlos *commodities* digitales que pueden ser usados como medio de pago. A estas posiciones se puede agregar la de Bedecarratz (2018: 82), que los declara un bien incorporeal *sui generis* que se comporta económicamente de forma similar a un *commodity*. Pérez Abarca y Bedecarratz no justifican su posición en el derecho positivo chileno. Para Simonetti Rojas, dado que la definición del Banco Central chileno, al igual que el de la Corte Suprema norteamericana (Mandjee, 2014), exige que una «divisa» sea dinero legal de otro país y Bitcoin no lo es en ninguno, no podría ser calificado de tal. En todo caso, Pérez Abarca y Simonetti Rojas coinciden en que figura legal aplicable en Chile a una transacción que involucra un pago en bitcoins serían las normas de la permuta y las que regulan la compraventa en subsidio.

De partida, hay que señalar que si alguien quisiera derrotar formalmente cada una de estas definiciones, podría señalar que el Banco Central chileno denomina divisas al dinero emitido por Gobiernos reconocidos y que, por tanto, las criptomo-

nedas no pueden ser divisas, como señala Pérez Abarca. Pero también podría decir que el Código Civil establece que los bienes consisten en cosas corporales e incorporeales (artículo 565), y que los corporales —que tienen un ser real que puede ser percibido— se dividen en muebles o inmuebles, teniendo los primeros las características de que son transportables (artículo 567). De acuerdo con estas definiciones, los bitcoins no podrían ser un *commodity* o un «bien mueble digital» como lo señala Simonetti Rojas. Finalmente, tampoco podrían ser un bien incorporeal, pues éstos son derechos reales que se tienen sobre cosas y que todos los terceros deben respetar, o derechos personales, que se tienen contra terceros determinados (artículo 576). Por tanto, ninguna de las tres definiciones existentes sobreviviría un ataque formalista. El que Bedecarratz denomine a las criptomonedas bienes incorporeales *sui generis* sólo confirma la dificultad de extender las categorías legales existentes en el Código Civil a las criptomonedas.

La determinación de la naturaleza jurídica de las criptomonedas genera innumerables consecuencias en el andamiaje jurídico. Esto abarca desde quién debería regularlas o cómo tributan, hasta cuáles son las obligaciones para las partes que genera una transacción en criptomonedas. Ninguna legislación de naciones avanzadas ha regulado comprensiva y directamente el fenómeno de las criptomonedas. Lo que motivó la jurisprudencia europea respecto de las criptomonedas fue una pregunta anexa sobre si el servicio de intermediación —la comisión del vendedor de criptomonedas en euros— debía pagar el impuesto al valor agregado.<sup>46</sup> Por su parte, lo que ha motivado la jurisprudencia norteamericana es mayoritariamente casos en que se sospecha que las criptomonedas se han usado para lavar dinero. En estos casos se aplican las figuras abiertas diseñadas para capturar este último fenómeno, y se limita a identificar las criptomonedas como un valor apto para lavar dinero. También existen normas dispersas que regulan obligaciones como la que exige a intermediarios financieros guardar datos de sus clientes para mejorar la trazabilidad de las operaciones. Incluso en Asia, donde éstas gozan de más popularidad, la regulación está limitada a aspectos financiero, como exposición al riesgo y obligaciones de información de los intermediarios.<sup>47</sup>

Dejando de lado el formalismo y aceptando que las criptomonedas son un bien innominado que puede ser objeto del comercio humano o un criptoactivo (*crypto-as-*

---

46. Sentencia del caso «Procedimiento prejudicial. Sistema común del impuesto sobre el valor añadido (IVA). Directiva 2006/112/CE. Artículos 2, apartado 1, letra c), y 135, apartado 1, letras d) a f). Servicios a título oneroso. Operaciones de cambio de la divisa virtual «bitcoin» por divisas tradicionales. Exención», Tribunal de Justicia de la Unión Europea, C-264/14, 22 de octubre de 2015, disponible en <http://bit.ly/2I6msFo>.

47. Kevin Helms, «How 5 Asian countries regulate cryptocurrency», News, *Bitcoin.com*, 8 de abril de 2019, disponible en <http://bit.ly/2I6oWQO>.

set), el derecho de las obligaciones también aparece como limitado. Según los autores referidos, la permuta sería la figura legal aplicable. Pero ésta falla cuando se verifica técnicamente en forma descrita en la sección «Las transacciones de criptomonedas».

¿Cómo se transa con criptomonedas? El problema del derecho en los contratos

La permuta es una de las figuras más flexibles del sistema jurídico continental cuando se intercambian cosas que no son dinero. En su base están instituciones legales básicas como la entrega, la posesión y el dominio. Cuando se trata de bitcoins, la entrega material se produciría revelando la secuencia de números que da derecho a los bitcoins y la tradición se produciría —si el término es aplicable— en este mismo instante, pues le daría al nuevo usuario el derecho a usarlos inmediatamente. Como se trata de un bien sujeto a registro, siguiendo los principios generales, el dominio por «confirmación adquisitiva» se adquiriría después de que varios bloques se han agregado a la cadena y la operación queda confirmada la mayoría de los nodos de la red. Con esta adaptación creativa pareciera que las normas existentes de la permuta son suficientes para capturar una transacción en que una de las partes utiliza criptomonedas, aunque no exista precisión sobre cuál es la naturaleza jurídica de las monedas permutadas.

Existen sin embargo varios problemas cuando se analizan potenciales conflictos entre las partes en esta operación tan sencilla. Primero, dado que existe un tiempo entre la transacción y que ésta quede escrita en piedra en bloques de la cadena de registro que impide el doble uso, el pago en criptomonedas, de aceptarse como aparentemente se acepta en Japón, no sería «pago efectivo». Dicho de otra forma, las criptomonedas permitirían una doble posesión «física» que no es simplemente un registro duplicado. La complicación adicional aquí es que no existe contrato con ningún emisor, ni si quiera con la fundación Bitcoin encargada de promover la tecnología, para descartar una operación o preferir la otra ni para corregir el registro. Un usuario podría revelar las claves privadas sin intención de transferir el dominio y transferirlo, como sucedió en el caso de un usuario que exhibió sus llaves privadas en un programa de televisión para ilustrar la tecnología y que le fueron robadas en el acto.<sup>48</sup> Cabe recordar que de acuerdo con la norma sustantiva del protocolo Bitcoin, la primera transacción debe ser validada, independientemente de las condiciones en que se haya producido. Técnicamente es imposible pedir a cada nodo de la red que verifique si los antecedentes de cada transacción son legítimos. Esto es contrario a lo que comanda el derecho tradicional. Blockchain, si es que es prueba de algo, lo es de posesión, independiente de si es legítima o ilegítima (Graf, 2015). En la red Bitcoin no existen los bitcoins robados, porque en su diseño no puede haber terceros con la

---

48. John Jeff Roberts, «How bitcoin».

posibilidad de controlar transacciones o revertirlas. El modo de transarlos hace que la figura del robo, y en general la causa y el objeto en términos del Código Civil, sean irrelevantes.

Los problemas de la simple permuta no terminan con el problema de la entrega, la posesión o la causa. Si se pudiera conocer al ladrón de bitcoins o a quién los ha recibido no debiendo recibirlos, un juez no tendría cómo forzar a su poseedor a devolverlos. El acceso a la secuencia alfanumérica para transferir una moneda no es derecho personal o un crédito, porque no hay contra quién ejercerlo (Graf, 2014: 59). Por tanto, no hay cómo embargar bitcoins.<sup>49</sup> Salvo que la autoridad consiga acceso al computador o las llaves privadas que dan derecho a ellos o torture al poseedor para que revele las secuencias, no podrá embargar. Los bitcoins podrían existir como secuencias sólo en la mente del ladrón y ahí serían intocables. La alternativa sería forzarlo al cumplimiento alternativo. La inconsistencia en esta opción es que el juez estaría forzando a devolver un bien que el ladrón todavía posee simplemente porque no tiene cómo forzarlo a devolverlo. Ya se han producido casos de divorcio en Inglaterra en que una de las partes protegió su patrimonio en bitcoins.<sup>50</sup>

Las instituciones tradicionales, el derecho real de propiedad —que contiene la definición de cosa— y las instituciones derivadas como la posesión y la tradición, o la ejecución forzada, no parecen fácilmente aplicables a las criptomonedas. Como señala Graf,

el clasificacionismo burocrático que insiste en que todas las actividades pueden caer dentro de un set limitado de categorías expandibles definidas por el legislador ha sido poderoso en la historia [...] En el caso de Bitcoin toma la forma de intentos de llamar a Bitcoin ilegal porque no calza en ninguna de las categoría o constructos existentes (Graf, 2015).

Hasta ahora, los trabajos legales existentes tienden a evitar la tediosa tarea de definir la naturaleza jurídica de las criptomonedas. Es más fácil recurrir a la definición legal de dinero para descartar que las criptomonedas lo sean, o tratar de ver qué hacen las personas que los tienen, si los usan como medio de pago o inversión, para ver si deben ser regulados por los bancos centrales, las agencias que protegen las inversiones privadas, las que controlan el intercambio de divisas internacionales, el derecho de los contratos, o para escapar de la regulación de todos ellos, entre otras posibilidades (Grinberg, 2012: 194; Haesly, 2016; Kaplanov, 2012: 150; Litwack, 2015: 310; Walch, 2016). Como el simple ejemplo de la permuta lo demuestra, todas estas

---

49. Sergio Carrasco, «¿Pueden embargarse bitcoins u otras monedas virtuales?», *Derecho en Red*, 4 de septiembre de 2013, disponible en <http://bit.ly/2M3bTqo>.

50. Kevin Peachy, «Divorcing couples may clash over Bitcoin», *BBC News*, 15 de febrero de 2018, disponible en <https://bbc.in/2M5fzYH>.

aproximaciones serán insatisfactorias en la medida en que no nos hagamos las preguntas legales en el orden correcto poniendo a la persona en el centro del análisis, como sugiere Graf (2015).

### Una aproximación regulatoria a las criptomonedas

El derecho positivo tiene pocas respuestas actuales para enfrentar el fenómeno de las criptomonedas y es riesgoso tratar de insertar nuevas regulaciones en sistemas jurídicos locales sin tener claridad respecto de su naturaleza jurídica y sin que el lenguaje haya decantado lo suficiente como para regular con precisión el fenómeno (Walch, 2016). Existe además el riesgo adicional de que intentos prematuros de regulación imprecisos inhiban desarrollos tecnológicos paralelos que se relacionen con la tecnología; por ejemplo, los desarrollos de Blockchain (Kiviat, 2015).

No obstante estas objeciones, el funcionamiento propio las mismas y la economía que las sustenta dan pistas de cómo se podría comenzar a tender a un «cerco regulatorio» alrededor de estas tecnologías que permita resolver los problemas inminentes y regularlas comprensivamente cuando ello se justifique y pueda hacerse de forma efectiva.

Lo primero es destacar es que la amenaza de regulación local tiene impacto en la adopción, a pesar de que las herramientas regulatorias tradicionales aparezcan como técnicamente ineptas. El precio en dinero corriente de las criptomonedas reacciona positiva o negativamente a noticias en las que se anuncia que éstas podrían ser prohibidas o aceptadas en algunas economías relevantes (Auer y Claessens, 2018). Algunas razones que podrían explicarlo es que las noticias afectan las expectativas. Por ejemplo, las noticias de aumento de interoperabilidad con bancos e instituciones financieras tiene impactos positivos en el precio corriente de las criptomonedas (Auer y Claessens, 2018). Por el contrario, las prohibiciones, aunque no sean efectivas, limitan la capacidad de circulación de las criptomonedas especialmente entre usuarios menos avanzados o adversos al riesgo.

En general, existen tres grandes áreas que se usan para justificar una regulación *restrictiva* de las criptomonedas: evitar ilícitos, proteger a consumidores e inversionistas, y proteger la estabilidad financiera y el sistema de pagos (Auer y Claessens, 2018; Puvogel Rojas, 2018). Como señalé en las secciones «El dilema entre facilitar la adopción temprana y la estabilidad de precios» y «El dilema entre la escalabilidad y la seguridad de las criptomonedas», dada su limitada circulación y las barreras tecnológicas para superar los problemas de escalabilidad y seguridad, no existen amenazas para la estabilidad financiera y el sistema de pagos. Así lo han hecho ver diversos informes del Banco de Pagos Internacional (BPI, 2018). Me enfocaré, por tanto, en los dos primeros objetivos.

La primera aproximación al fenómeno debiera ser distinguir qué tipo de mone-

da se está tratando de regular. Como se señaló en el capítulo «Una generalización económica de las criptomonedas», las criptomonedas tienen formas muy distintas de enfrentar el problema del respaldo y de la adopción temprana, lo que da origen a criptomonedas de distinta naturaleza. Siguiendo las distinciones hechas en esa sección, la regulación debiera ser muy distinta en el caso de criptomonedas centralizadas o respaldadas que en el caso de monedas descentralizadas de escasez programada —o sin respaldo— como Bitcoin. En el caso de las primeras, la regulación debiera ser menos intensa o intrusiva porque la mecánica misma con la que operan permite que el derecho tradicional sea más efectivo. Como regla general, mientras más confianza requiera alguno de los componentes del sistema de la criptomoneda en cuestión (*trust*), menos necesaria será la regulación por razones restrictivas, pues la confianza se construye, por definición, utilizando herramientas existentes, como el derecho de los contratos.<sup>51</sup>

El caso más complejo es el de criptomonedas descentralizadas y no respaldadas que se mantienen con tecnologías sin confianza (*trustless*) como Blockchain y en las que existe cuasianonimato, especialmente cuando se las regula por razones restrictivas, como la protección del consumidor, la protección de inversionistas o para evitar ilícitos.

El principal problema de la regulación en este caso es que los fines son claros pero las herramientas existentes débiles, lo que permite que destinatarios puedan decidir caer fuera o dentro de la misma. Por ejemplo, si el temor es que Bitcoin se esté usando para financiar o pagar lo que Foley, Karlsen y Putniņš (2018) denominan el *black e-commerce*, que acaparaba al 2018 el 25% de las transacciones en criptomonedas, el riesgo de la prohibición es inhibir el 75% de las actividades legales.<sup>52</sup> Por eso las «listas negras» de direcciones de bitcoins involucradas en transacciones ilegales como medio de prevenir delitos, como se ha propuesto (Bedecarratz, 2018), pueden resultar inefectivas para el objetivo.

---

51. Por ejemplo, si una criptomoneda se respalda en algún *commodity*, los contratos de suscripción que se vuelven al portador debieran ser suficientes para reclamar que éstas sean convertibles al *commodity* de respaldo. En estos casos quizá convendría solo monitorear el encaje o las reservas del *commodity* ofrecido para preservar la estabilidad de los medios. Un razonamiento similar puede aplicarse a casos en que existe renuncia al anonimato, o en que funcionan nodos o personas autorizadas, y casos en que la moneda tiene un controlador. La centralización es una ventaja para regular porque le pone cara y domicilio al controlador, al que pueden imponérsele normas similares a las aplicables al dinero privado.

52. El caso típico sería prohibir el uso de una tarjeta de crédito convencional para comprar bitcoins en una bolsa local, prohibiéndole a los bancos cursar dichas transacciones o a la bolsa local funcionar. Técnicamente es fácil para quien quiere delinquir esconder sus actividades en internet, comprar en bolsas extranjeras simulando comprar otro tipo de bienes o migrar a criptomonedas más opacas. Este comportamiento es precisamente lo que Auer y Claessens (2018) encontraron en su estudio. Los niveles de transacciones ilegales en Bitcoin fueron disminuyendo en la medida en que este sistema acaparó más atención pública y los delincuentes migraron a criptomonedas más opacas.

Por todo lo anterior, una aproximación al fenómeno de las criptomonedas, especialmente las descentralizadas y sin respaldo, debiera ser uno que obedezca a razones *expansivas*, que invite a generar puntos de contacto con el sistema legal existente y que normalice su uso. La idea es lograr que más usuarios adopten monedas y les den trazabilidad y más atención pública. Esto no evitará el delito. Quien quiera delinquir o estafar a consumidores o inversionistas podrá hacerlo desde monedas más opacas. Este comportamiento es precisamente lo que unos autores encontraron (Auer y Claessens, 2018). Los niveles de transacciones ilegales en Bitcoin fueron disminuyendo en la medida en que este sistema acaparó más atención pública.

Las acciones posibles para implementar esta estrategia son variadas. Por ejemplo, permitir que se puedan comprar con tarjetas de crédito, que estén reconocidas como instrumento de inversión, que se invite a los emisores a registrarse y transparentar cifras de uso y sus fórmulas de oferta monetaria, que se permita tributar las ganancias y pérdidas, y descontar costos —algo que ya se implementa en Chile según el Oficio 963-2018 del Servicio de Impuestos Internos—, que las bolsas o intermediarios sean autorizados y guarden registros de sus clientes —enfoque conocido como *know your client*—, entre otros (Gamble, 2017: 352; Mandjee, 2014: 34-38; Maupin, 2017: 5-6; Ven, 2018: 20).

Estas medidas, que no regulan comprensivamente el fenómeno, no son incompatibles con la discusión en tribunales de problemas que se produzcan en transacciones con criptomonedas y con la persecución *ex post* activa de los fraudes a inversionistas y consumidores, y de todos los delitos por los medios que la ley permita en tribunales. Los tribunales tienen un rol muy importante en levantar las preguntas que el sistema jurídico deberá responder cuando estemos en condiciones de tener una regulación comprensiva y permanente de esta nueva tecnología. No se trata de construir una regulación sobre la base de fallos judiciales nacionales y extranjeros, los que pueden ser doctrinariamente muy deficientes, sino de levantar las preguntas que el sistema legal deberá responder. La preocupación de intentar una regulación comprensiva y por motivos restrictivos, reitero, es que por tratar de incidir en fenómenos que se pueden controlar siquiera medianamente, como el uso de criptoactivos en lavado de dinero, inhibamos la innovación tecnológica y el desarrollo normal de las criptomonedas y perjudiquemos a los nuevos adoptantes.

## Conclusión

Frente a vacíos tan importantes en el derecho positivo, es inevitable sugerir lo obvio. Se necesitan un nuevo enfoque, nuevas normas e instituciones para poder capturar correctamente lo que hacen los usuarios con las criptomonedas. Hasta el momento, sin embargo, no es necesario hacerlo a cabalidad. El riesgo de regular inhibiendo la innovación disruptiva es alto, y las ganancias de hacerlo, pocas. Parece mejor estra-



tegia limitarse a tratar de evitar usos ilegales y perseguir los abusos inminentes como lo hacen otras jurisdicciones, e intentar normalizar el uso de las criptomonedas facilitando su interacción con el sistema legal, especialmente en casos de criptomonedas consolidadas. Tal como no se puede cobrar impuestos personales en economías con alto grado de informalidad, ningún objetivo regulatorio respecto de las criptomonedas va a poder alcanzarse si éstas se mantienen artificialmente opacas y al margen del sistema legal.

La mejor aproximación por el momento es, por tanto, esperar. Ver cómo van evolucionando los conflictos entre partes que transen en criptomonedas en tribunales. Los tribunales, que funcionan de manera descentralizada y extendiendo normas existentes a hechos sobrevinientes, tienen la aptitud de levantar información transversal sobre potenciales conflictos como los que describí en la sección anterior a propósito de la permuta y la ejecución forzada, o de determinar la operatoria criminal en las criptomonedas que estén envueltas. Con algunos años de conflictos y las preguntas que acarrearán, podremos estar en condiciones de entender qué problemas les producen las transacciones en criptomonedas a personas reales en transacciones reales, y diseñar regulación que las ponga a ellas en el centro. Después de todo, las criptomonedas podrán ser un bien programado, pero la justicia es una institución humana que requiere observar cómo se comportan las personas frente a un nuevo bien inexistente hasta hoy en la historia humana.

## Referencias

- ÁLVAREZ, Andrés y Vincent Bignon (2013). «L. Walras and C. Menger: Two ways on the path of modern monetary theory». *European Journal of the History of Economic Thought*, 20 (1): 89-124. DOI: [10.1080/09672567.2011.596939](https://doi.org/10.1080/09672567.2011.596939).
- AMETRANO, Ferdinando M. (2016a). «Bitcoin, Blockchain, and distributed ledgers: Between hype and reality». *SSRN Electronic Journal*. DOI: [10.2139/ssrn.2832249](https://doi.org/10.2139/ssrn.2832249).
- . (2016b). «Hayek money: The cryptocurrency price stability solution». *SSRN Electronic Journal*. DOI [10.2139/ssrn.2425270](https://doi.org/10.2139/ssrn.2425270).
- ARIAS, Gonzalo y Andrés Sánchez (2016). «The digital currency challenge for the regulatory regime». *Revista Chilena de Derecho y Tecnología*, 5 (2): 173-209. DOI: [10.5354/0719-2584.2016.43541](https://doi.org/10.5354/0719-2584.2016.43541).
- AUER, Raphael y Stijn Claessens (2018). «Regulación de las criptomonedas: Evaluación de reacciones del mercado». Informe Trimestral del BPI. Disponible en <https://bit.ly/2TZktpy>.
- BABAIOFF, Moshe, Shahar Dobzinski, Sigal Oren y Aviv Zohar (2012). «On Bitcoin and red balloons». Proceedings of the 13th ACM Conference on Electronic Commerce: 56-73. DOI: [10.1145/2229012.2229022](https://doi.org/10.1145/2229012.2229022).

- BANCO CENTRAL EUROPEO (2012). *Virtual currency schemes*. Frankfurt am Main: European Central Bank.
- BARBER, Andrew (2015). «Bitcoin and the philosophy of money: Evaluating the commodity status of digital currencies». *Spectra*, 4 (2). DOI: [10.21061/spectra.v4i2.241](https://doi.org/10.21061/spectra.v4i2.241).
- BARRO, Robert J. y Sanjay Misra (2016). «Gold returns». *The Economic Journal*, 126 (594): 1.293-1.317. DOI: [10.1111/ecoj.12274](https://doi.org/10.1111/ecoj.12274).
- BARTLE, Richard A. (2004). «Pitfalls of Virtual Property». Disponible en <http://bit.ly/2IoSHoY>.
- BEDECARRATZ, Francisco Javier (2018). «Riesgos delictivos de las monedas virtuales». *Revista Chilena de Derecho y Tecnología*, 7 (1): 79-105. DOI: [10.5354/0719-2584.2018.48515](https://doi.org/10.5354/0719-2584.2018.48515).
- BJERG, Ole, Duncan McCann, Laurie Macfarlane, Rasmus Hougaard Nielsen y Josh Ryan-Collins (2017). *Seigniorage in the 21st Century: A study of the profits from money creation in the United Kingdom and Denmark*. Frederiksberg: Copenhagen Business School.
- BLUNDELL-WIGNALL, Adrian (2014). «The Bitcoin question: Currency versus trustless transfer technology». *OECD Working Papers on Finance, Insurance and Private Pensions*. DOI: [10.1787/20797117](https://doi.org/10.1787/20797117).
- BÖHME, Rainer, Nicolas Christin, Benjamin Edelman y Tyler Moore (2015). «Bitcoin: Economics, technology, and governance». *The Journal of Economic Perspectives*, 29 (2): 213-238. DOI: [10.1257/jep.29.2.213](https://doi.org/10.1257/jep.29.2.213).
- BONNEAU, Joseph, Andrew Miller, Jeremy Clark, Arvind Narayanan, Joshua A. Kroll y Edward W. Felten (2015). «SoK: Research perspectives and challenges for Bitcoin and cryptocurrencies». 2015 IEEE Symposium on Security and Privacy: 104-121. DOI: [10.1109/SP.2015.14](https://doi.org/10.1109/SP.2015.14).
- BPI, Bank for International Settlements (2018). «Criptomonedas: Más allá del fenómeno de moda». Informe Económico Anual 2018 del BPI. Disponible en <http://bit.ly/2Ilkqjj>.
- BRITO, Jerry y Andrea Castillo (2013). *Bitcoin: A primer for policymakers*. Arlington: Mercatus Center at George Mason University.
- BRITO, Jerry, Houman B. Shadab y Andrea Castillo (2015). «Bitcoin financial regulation: Securities, derivatives, prediction markets, and gambling». *Columbia Science and Technology Law Review*. DOI: [10.2139/ssrn.2423461](https://doi.org/10.2139/ssrn.2423461).
- CASTRONOVA, Edward (2001). «Virtual worlds: A first-hand account of market and society on the cyberian frontier». *CESifo Working Paper Series*, 618. Disponible en <http://bit.ly/2IkoIo2>.
- . (2006). «A cost-benefit analysis of real-money trade in the products of synthetic economies». *Info*, 8 (6): 51-68. DOI: [10.1108/14636690610707482](https://doi.org/10.1108/14636690610707482).
- . (2014). *Wildcat currency*. New Haven: Yale University Press.
- CHAMPAGNE, Phil (2018). *El Libro de Satoshi*. Madrid: Blockchain España.

- CHAUM, David (1992). «Achieving electronic privacy». *Scientific American*, 267 (2): 96-101. DOI: [10.1038/scientificamericano892-96](https://doi.org/10.1038/scientificamericano892-96).
- CLINE, Ernest (2011). *Ready player one*. Portland: Broadway Books.
- CROMAN, Kyle, Christian Decker, Ittay Eyal, Adem Efe Gencer, Ari Juels, Ahmed Kosba, Andrew Miller, Prateek Saxena, Elaine Shi, Emin Gün Sirer, Dawn Song, Roger Wattenhofer (2016). «On scaling decentralized blockchains». En Jeremy Clark, Sarah Meiklejohn, Peter Y.A. Ryan, Dan Wallach, Michael Brenner y Kurt Rohloff (editores), *Financial cryptography and data security: FC 2016. Lecture notes in computer science* (pp. 106-125). Berlín: Springer. DOI: [10.1007/978-3-662-53357-4\\_8](https://doi.org/10.1007/978-3-662-53357-4_8).
- DAVIDSON, Laura y Walter E Block (2015). «Bitcoin, the Regression Theorem, and the emergence of a new medium of exchange». *The Quarterly Journal of Austrian Economics*, 18 (3): 311-338. Disponible en <http://bit.ly/2HZ9uJf>.
- DOGUET, Joshua J. (2012). «The nature of the form: Legal and regulatory issues surrounding the Bitcoin digital currency system». *Louisiana Law Review*, 73 (4): 1.118-1.153. Disponible en <http://bit.ly/2HYyIHF>.
- DOURADO, Eli y Jerry Brito (2014). «Cryptocurrency». En *The New Palgrave Dictionary of Economics* (pp. 1-9). Londres: Palgrave Macmillan.
- DWYER, Gerald P. (2015). «The economics of Bitcoin and similar private digital currencies». *Journal of Financial Stability*, 17: 81-91. DOI: [10.1016/j.jfs.2014.11.006](https://doi.org/10.1016/j.jfs.2014.11.006).
- FENWICK, Mark, Wulf A. Kaal y Erik P. M. Vermeulen (2017). «Legal education in the Blockchain revolution». *Vanderbilt Journal of Entertainment & Technology Law*, 20 (2): 351-383. Disponible en <http://bit.ly/2HXHc1A>.
- FILIPKOWSKI, Wojciech (2008). «Cyber laundering: An analysis of typology and techniques». *International Journal of Criminal Justice Sciences*, 3 (1): 15-27. DOI: [10.2139/ssrn.2939127](https://doi.org/10.2139/ssrn.2939127).
- FOLEY, Sean, Jonathan R. Karlsen y Tālis J. Putniņš (2018). «Sex, drugs, and Bitcoin: How much illegal activity is financed through cryptocurrencies?» *The Review of Financial Studies*, 32 (5): 1.798-1.853. DOI: [10.1093/rfs/hhz015](https://doi.org/10.1093/rfs/hhz015).
- FUNG, Ben, Miguel Molico y Gerald Stuber (2014). «Electronic money and payments: Recent developments and issues». Bank of Canada. Disponible en <http://bit.ly/2HX9dqC>.
- GAMBLE, Connor (2017). «The legality and regulatory challenges of decentralised crypto-currency: A Western perspective». *International Trade and Business Review*, 20.
- GANS, Joshua S. y Hanna Halaburda (2015). «Some economics of private digital currency». En Avi Goldfarb, Shane M. Greenstein y Catherine E. Tucker (editores), *Economic analysis of the digital economy* (pp. 257-276). Oxford: Oxford University Press. DOI: [10.7208/chicago/9780226206981.003.0009](https://doi.org/10.7208/chicago/9780226206981.003.0009).
- GRAF KONRAD S. (2014). «COMMODITY, scarcity, and monetary value theory in light of bitcoin». *Prices & Markets*: 1-24. Disponible en <http://bit.ly/2HY84hZ>.


- . (2015). *Are Bitcoins ownable?: Property rights, IP wrongs, and legal-theory implications*.
- GRINBERG, Reuben (2012). «Bitcoin: An innovative alternative digital currency». *Hastings Science & Technology Law Journal*, 4 (1): 159-208. Disponible en <http://bit.ly/2HVwfgR>.
- HAESLY, Kenneth B. II (2016). «How to solve a problem like Venezuela: An argument for virtual currency». *Law and Business Review of the Americas*, 22 (3): 261-270. Disponible en <http://bit.ly/2HXl1bJ>.
- HALABURDA, Hanna y Miklos Sarvary (2016). *Beyond bitcoin: The economics of digital currencies*. Basinstoke: Palgrave Macmillan.
- HEEKS, Richard (2009). «Understanding «gold farming» and real-money trading as the intersection of real and virtual economies». *Journal for Virtual Worlds Research*, 2 (4): 4-27. DOI: [10.4101/jvwr.v2i4.868](https://doi.org/10.4101/jvwr.v2i4.868).
- IWAMURA, Mitsuru, Yukinobu Kitamura, Tsutomu Matsumoto y Kenji Saito (2014). «Can we stabilize the price of a cryptocurrency?: Understanding the design of Bitcoin and its potential to compete with Central Bank money». *SSRN Electronic Journal*: 1-39. DOI: [10.2139/ssrn.2519367](https://doi.org/10.2139/ssrn.2519367).
- JACOBS, Edwin (2011). «Bitcoin: A bit too far?». *Journal of Internet Banking and Commerce*, 16 (2). Disponible en <http://bit.ly/2wDBHij>.
- KAPLANOV, Nikolei (2012). «Nerdy money: Bitcoin, the private digital currency, and the case against its regulation». *Loyola Consumer Law Review*, 25 (1): 111-174. Disponible en <http://bit.ly/2wFmr4u>.
- KARLSTRØM, Henrik (2014). «Do libertarians dream of electric coins? The material embeddedness of Bitcoin». *Distinktion: Journal of Social Theory*, 15 (1): 23-36. DOI: [10.1080/1600910X.2013.870083](https://doi.org/10.1080/1600910X.2013.870083).
- KHAN, Ali (2008). «A theoretical analysis of payment systems». *South Carolina Law Review*, 60 (2): 1-66. Disponible en <http://bit.ly/2wDCCzh>.
- KIVIAT, Trevor I. (2015). «Beyond Bitcoin: Issues in regulating Blockchain transactions». *Duke Law Journal*, 65: 569-608. Disponible en <http://bit.ly/2wFUKbv>.
- KROLL, Joshua, Ian Davey y Edward Felten (2013). «The economics of Bitcoin mining or, Bitcoin in the presence of adversaries». *The Twelfth Workshop on the Economics of Information Security* (pp. 11-32). Washington DC, 11 y 12 de junio de 2013.
- LASTOWKA, Gregory y Dan Hunter (2004). «The laws of the virtual worlds». *California Law Review*, 92 (1): 1-74. DOI: [10.15779/Z386H7P](https://doi.org/10.15779/Z386H7P).
- LEBLANC, Gannon (2016). «The effects of cryptocurrencies on the banking industry and monetary policy». Tesis Open Access Senior Honors, Eastern Michigan University. Disponible en <http://bit.ly/2MtROJX>.
- LEMIEUX, Victoria Louise (2016). «Trusting records: Is Blockchain technology the answer?». *Records Management Journal*, 26 (2): 110-139. DOI: [10.1108/RMJ-12-2015-0042](https://doi.org/10.1108/RMJ-12-2015-0042).

- LITWACK, Seth (2015). «Bitcoin: Currency or fool's gold: A comparative analysis of the legal classification of Bitcoin notes & comments». *Temple International & Comparative Law Journal*, 29 (2). Disponible en <http://bit.ly/2Iop67P>.
- LO, Stephanie y Christina Wang (2014). «Bitcoin as money?». *Current Policy Perspectives*, 14 (4). Disponible en <http://bit.ly/2wEyqiE>.
- MANDJEE, Tara (2014). «Bitcoin, its legal classification and its regulatory framework», *Journal of Business and Securities Law*, 15 (2): 157-218. Disponible en <http://bit.ly/2wEyWNC>.
- MAUPIN, Julie (2017). «Mapping the global legal landscape of Blockchain and other executive summary: Distributed ledger technologies». CIGI Academic Paper Series. Disponible en <http://bit.ly/2wBhCsK>.
- MCJOHN, Stephen M. e Ian McJohn (2016). «The Commercial Law of Bitcoin and Blockchain transactions». *Uniform Commercial Code Law Journal*. Disponible en <http://bit.ly/2wEIRCG>.
- NAKAMOTO, Satoshi (2009). «Bitcoin: A peer-to-peer electronic cash system Bitcoin: A Peer-to-Peer Electronic Cash System». Bitcoin.org. Disponible en <https://bitcoin.org/en/bitcoin-paper>.
- NAZIR, Mohamed, John R Hamilton y SingWhat Tee (2017). «Real money trading in virtual worlds». Proceedings of the 17th International Conference on Electronic Business. Dubai. Disponible en <http://bit.ly/2KtsSzD>.
- PEACH, Terry (2009). «Adam Smith and the labor theory of (real) value: A reconsideration». *History of Political Economy*, 41 (2): 383-406. DOI: 10.1215/00182702-2009-007.
- PÉREZ ABARCA, Rubén Ignacio (2015). «El régimen jurídico del contrato de permutación en la jurisprudencia». Memoria para optar al grado de licenciado en Ciencias Jurídicas y Sociales, Universidad de Chile. Disponible en <http://bit.ly/2WOMWTy>.
- PETERS, Gareth W. Efstathios Panayi y Ariane Chapelle (2015). «Trends in cryptocurrencies and blockchain technologies: A monetary theory and regulation perspective». *Journal of Financial Perspectives*, 3 (3): 92-113. Disponible en <http://bit.ly/2wFi614>.
- PUVOGEL ROJAS, Max (2018). «Blockchain y monedas virtuales: Una aproximación jurídica». Memoria para optar al grado de licenciado en Ciencias Jurídicas y Sociales, Universidad de Chile. Disponible en <http://bit.ly/2wEBsDy>.
- REID, Fergal y Martin Harrigan (2011). «An analysis of anonymity in the Bitcoin system». 2011 IEEE Third International Conference on Privacy, Security, Risk and Trust and 2011 IEEE Third International Conference on Social Computing. (pp. 1.318-1.326). Disponible en <http://bit.ly/2wzZgbJ>.
- REYES, Carla (2016). «Moving beyond Bitcoin to an endogenous theory of decentralized ledger technology regulation: An initial proposal». *Villanova Law Review*, 61 (1): 191-234. Disponible en <http://bit.ly/2Xt8H8H>.

- ROGERS, James Steven (2005). «The new old law of electronic money». *Southern Methodist University Law Review*, 58 (4): 1.253-1.312. Disponible en <http://bit.ly/2XzrdfK>.
- ROTHBARD, Murray (1992). *The gold standard: Perspectives in the Austrian school*. Auburn: Ludwig von Mises Institute.
- ROUBINI, Nouriel (2018). «Crypto is the mother of all scams and (now busted) bubbles while Blockchain is the most over-hyped technology ever, no better than a spreadsheet/database». Testimonio para la audiencia del Senado de Estados Unidos sobre Banking, Housing y Community Affairs. Washington, DC.
- SELGIN, George (1994). «On ensuring the acceptability of a new fiat money». *Journal of Money, Credit and Banking*, 26 (4): 808-826. DOI: [10.2307/2077948](https://doi.org/10.2307/2077948).
- . (2015). «Synthetic commodity money». *Journal of Financial Stability*, 17: 92-99. DOI: [10.1016/j.jfs.2014.07.002](https://doi.org/10.1016/j.jfs.2014.07.002).
- SHAVIRO, Steven (2007). «Money for Nothing: Virtual Worlds and Virtual Economies». Disponible en <http://bit.ly/2EUz2VQ>.
- SHIN, Dong Hee (2008). «Understanding purchasing behaviors in a virtual economy: Consumer behavior involving virtual currency in Web 2.0 communities». *Interacting with Computers*, 20 (4-5): 433-446. DOI: [10.1016/S0953-5438\(08\)00025-8](https://doi.org/10.1016/S0953-5438(08)00025-8).
- SIMONETTI ROJAS, Joaquín Ignacio (2017). «Concepto y naturaleza jurídica de las criptomonedas». Memoria para optar al grado de Licenciado en Ciencias Jurídicas, Facultad de Derecho, Pontificia Universidad Católica de Valparaíso.
- SMITH, Adam (1794). *Investigación de la naturaleza y causas de la riqueza de las naciones*. Valladolid.
- SPENKELINK, Hardwin (2014). «The adoption process of cryptocurrencies: Identifying factors that influence the adoption of cryptocurrencies from a multiple stakeholder perspective». Tesis de grado para optar al master en Industrial Engineering and Management, Universidad de Twente. Disponible en <http://bit.ly/2XCk8uw>.
- SZABO, Nick (1997). «Formalizing and securing relationships on public networks». *First Monday*, 2 (9). Disponible en <http://bit.ly/2XwocK2>.
- TAPSCOTT, Don y Alex Tapscott (2016). *Blockchain revolution: How the technology behind Bitcoin is changing money, business, and the world*. Nueva York: Penguin.
- TASK FORCE ON STORED-VALUE CARDS (1996). «A commercial lawyer's take on the electronic purse: An analysis of Commercial Law issues associated with stored-value cards and electronic money report». *The Business Lawyer*, 52 (2): 653-727. Disponible en <http://bit.ly/2Ikh53P>.
- TUCKER, Peter (2009). «The digital currency doppelganger: Regulatory challenge or harbinger of the new economy note». *Cardozo Journal of International and Comparative Law*, 17 (2): 589-626. Disponible en <http://bit.ly/2ZsovpP>.
- VELDE, François y otros (2013). «Bitcoin: A primer». *Chicago Fed Letter*, 317. Disponible en <http://bit.ly/2Xuc1QS>.

- VEN, Nathan van de (2018). «Explaining the early responses to blockchain technology». Tesis para optar al grado de master, Universidad de Leiden. Disponible en <http://bit.ly/2XzuCew>.
- DE WAAL, Brent (1995). «Motivations for video game play: A study of social, cultural and physiological factors». Tesis para optar al grado de Master of Arts (Communication), Universidad Simon Fraser. Disponible en <http://bit.ly/31bMHkX>.
- WALCH, Angela (2016). «The path of the Blockchain lexicon (and the law) The Law of FinTech Symposium». *Boston University Review of Banking and Financial Law*, 36: 1-13. Disponible en <http://bit.ly/2QMX9KQ>.
- WANG, Hao y Chuen-Tsai Sun (2011). «Game reward systems: Gaming experiences and social meanings». *Think Design Play*, 6: 15. Disponible en <http://bit.ly/2XuE7LF>.
- YAMAGUCHI, Hiroshi (2004). «An analysis of virtual currencies in online games». *SSRN Electronic Journal*. DOI: [10.2139/ssrn.544422](https://doi.org/10.2139/ssrn.544422).
- YERMACK, David (2015). «Is Bitcoin a real currency? An economic appraisal». *NBER Working Series*: 31-43. DOI: [10.3386/w19747](https://doi.org/10.3386/w19747).

### Sobre el autor

Agustín Barroilhet Diez es abogado. Profesor asociado de Derecho Económico de la Facultad de Derecho de la Universidad de Chile. Licenciado en Ciencias Jurídicas y Sociales y master en Derecho Tributario, ambos por la Universidad de Chile. LL.M. Stanford Law School y doctor en Derecho por Georgetown University, Estados Unidos. Su correo electrónico es [abarroilhet@derecho.uchile.cl](mailto:abarroilhet@derecho.uchile.cl).  <http://orcid.org/0000-0002-2646-9750>.

La *Revista de Chilena de Derecho y Tecnología* es una publicación académica semestral del Centro de Estudios en Derecho Informático de la Facultad de Derecho de la Universidad de Chile, que tiene por objeto difundir en la comunidad jurídica los elementos necesarios para analizar y comprender los alcances y efectos que el desarrollo tecnológico y cultural han producido en la sociedad, especialmente su impacto en la ciencia jurídica.

### EDITOR GENERAL

Daniel Álvarez Valenzuela  
([dalvarez@derecho.uchile.cl](mailto:dalvarez@derecho.uchile.cl))

### SITIO WEB

[rchdt.uchile.cl](http://rchdt.uchile.cl)

### CORREO ELECTRÓNICO

[rchdt@derecho.uchile.cl](mailto:rchdt@derecho.uchile.cl)

### LICENCIA DE ESTE ARTÍCULO

Creative Commons Atribución Compartir Igual 4.0 Internacional



La edición de textos, el diseño editorial  
y la conversión a formatos electrónicos de este artículo  
estuvieron a cargo de Tipografía  
([www.tipografica.cl](http://www.tipografica.cl)).