CRIPTOMONEDAS

Julia Sánchez Roa[1]

RESUMEN

En los últimos años ha proliferado la emisión y el uso de las denominadas monedas virtuales, digitales o criptomonedas. Están presentes en los medios de comunicación. Oímos hablar de criptomillonarios. Conocemos las subidas y bajas de su cotización, intentos de prohibición en algunos países, su emisión por parte de otros, pero ¿qué son realmente? ¿Qué son los token y cómo se diferencian de las criptomonedas? ¿Cuándo surgen y cuál es su utilidad? ¿Es posible su regulación? ¿Tienen realmente futuro? A lo largo de este trabajo se intentará dar respuesta a estos temas que ya han pasado a formar parte de nuestra vida cotidiana.

Palabras claves: Criptomonedas, criptoactivos, monedas virtuales, token, blockchain, Deep web.

ABSTRACT

The issuance and usage of the so called virtual, digital currency or criptocurrency increased over the course of the last few years. They are present in the mass media. We hear about criptomillionaires. We are aware about the share price increases and decreases and also about the attempts of prohibition in some countries, the issuance in other ones, but, what are they actually? What are the tokens and how can we differentiate them from criptocurrencies? Is it possible to regulate them? Is there a real future for them? Across this paper we will try to give an answer to those issues which are now part of our daily life.

Key Words: Criptocurrency, Criptoassets, Virtual Currency, Token, Blockchain, Deep Web.

---

[1] Grado en Derecho por la Universidad Internacional de la Rioja (España), Máster en Ejercicio de la Abogacía por la Universidad Internacional de la Rioja (España). Abogada en ejercicio del Ilustre Colegio de Abogados de Madrid (España). Licenciada en Ciencias Físicas por la Universidad Autónoma de Madrid (España). Presidenta de la Asociación de Profesionales de Sistemas de información del Banco de España (APSIBE). Cuenta con más de treinta años de experiencia en Tecnologías de la Información. Experta en administración electrónica y lucha contra la falsificación de moneda, en la actualidad combina la tecnología y el Derecho, analizando y difundiendo la vertiente técnica y jurídica en ámbitos como las criptomonedas, *Blockchain*, ciberdelincuencia y la Internet profunda.

¿A QUÉ NOS REFERIMOS CUANDO HABLAMOS DE CRIPTOMONEDAS?

Se pueden dar muchas definiciones de criptomoneda. Según el Banco Central Europeo[2] "es la representación digital de valor, no emitida por ninguna autoridad central, institución de crédito o emisor de dinero electrónico reconocido que en ciertas ocasiones, puede ser utilizada como medio de pago alternativo al dinero".

También podríamos definirlas como un sistema de pago a través de Internet, basadas en un sistema peer-to-peer o red entre iguales (P2P), que contienen un elemento de seguridad basado en la criptografía y en donde el valor es transmitido electrónicamente entre las partes, sin unintermediario.

En realidad aunque las llamemos monedas digitales o virtuales, **no son monedas**. Para que fueran consideradas como tales deberían cumplir tres funciones básicas[3]:

1. Ser un medio de pago, para lo cual debería estar aceptadas de forma generalizada en la adquisición de bienes y servicios, con un fraccionamiento suficiente.

2. Unidad de cuenta, porque podemos determinar el valor de cualquier producto en unidades de esta moneda

3. Depósito de valor, manteniendo la capacidad de pago a lo largo del tiempo.

No cuentan con sustento legal en prácticamente ningún país, ni tienen forma física de billetes o monedas, su uso es anónimo, no son respaldadas por autoridades monetarias, la seguridad y la confianza están basadas en protocolos criptográficos, pura matemática en Internet gestionada por la comunidad de usuarios.

El hecho es que por parte de los bancos centrales, hasta el momento únicos emisores legítimos de moneda, no se denominan criptomonedas sino criptoactivos.

---

[2] European Central Bank, "Virtual currency schemes – a further analysis", 2015, 32.

[3] Las tarjetas de crédito que utilizamos habitualmente son medio de pago que, aunque son aceptadas de forma generalizada, no lo son en todos los lugares. No son unidad de cuenta ni depósito de valor.
El oro es un depósito de valor desde tiempo inmemorial pero ni se utiliza como unidad de cuenta y aunque se podrían comprar productos o saldar cuentas, no serviría en nuestra vida cotidiana para comprar bienes básicos, ni para pagar impuestos

Si hacemos un poco de historia originariamente el dinero era un medio de pago que poseía un valor intrínseco. Cada moneda valía el peso del metal en el que estaba fundida. Más tarde surgen los billetes avalados por el patrón oro. Los emisores de moneda garantizaban a los poseedores de sus billetes y monedas la cantidad de oro de sus correspondientes denominaciones.A partir de 1971 se abandona el patrón oro dando lugar al dinero fiduciario cuyo valor es la confianza que ofrece a sus poseedores la entidad emisora.

ASPECTOS TECNOLÓGICOS

Las criptomonedas se emiten al margen de los gobiernos y bancos centrales y, al menos en teoría, esta función se traslada a todo aquel que quiera participar. Esta generación de moneda se denomina "minado". Estos participantes (mineros) son quienes aportan la seguridad a las transacciones utilizando, en la mayor parte de los casos, la tecnología de blockchain (cadena de bloques).

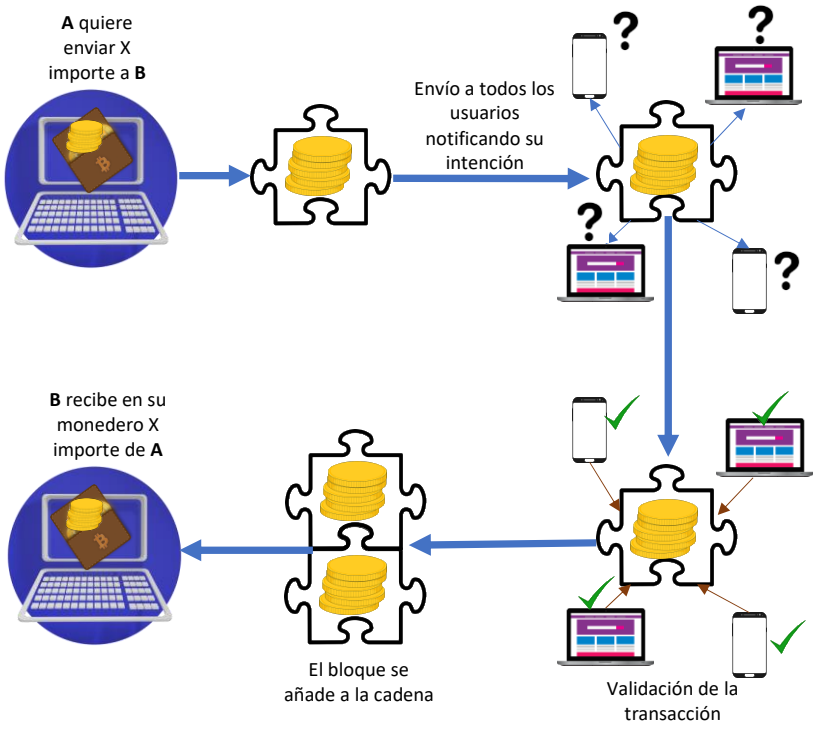
Blockchain es un gigantesco libro de contabilidad distribuido (DLT) [4]en el que los registros (bloques) están enlazados para proteger la seguridad y la privacidad de las transacciones. Se trata de una base de datos distribuida y segura gracias a la utilización de algoritmos criptográficos.

Al realizar una transacción hay varios usuarios (nodos) que se encargan de verificar la transacción y registrarlas en el gigantesco libro de cuentas. Veamos el funcionamiento con un ejemplo. Imaginemos que A quiere enviar a B una determinada cantidad X. Si esta transacción se realizara mediante una transferencia bancaria, A le pediría a su banco que retirara X de su cuenta para enviarla a la cuenta de B. Lo restarían de su saldo, comunicando al otro banco que debe añadir X a la cuenta de B.

[4] Las aplicaciones de la tecnología Blockchain son muy diversas:

- Registro de documentos: blockchain es un gran registro al que muchas partes pueden acceder desde cualquier lugar del mundo. Ya está siendo utilizada para registrar y verificar la autenticidad de toda clase de documentos, desde títulos universitarios y actas matrimoniales hasta historiales médicos.
- Contratos inteligentes y aplicaciones descentralizadas (Dapps): blockchain también es capaz de crear la infraestructura adecuada para crear contratos inteligentes, es decir, acuerdos digitales automatizados en los que nuevamente se elimina la necesidad de confiar en terceras partes para su cumplimiento. Los términos quedan establecidos en principio a conveniencia de las partes, y más tarde son cumplidos gracias al código, como una tarea programada.
- Transacciones y sistemas de pago: por la propia naturaleza del blockchain, la velocidad, la seguridad y la privacidad que permite a los usuarios a la hora de realizar transacciones. La mayor parte de los bancos y grandes empresas están trabajando en el desarrollo de sus propias plataformas.

Pues bien, esta misma transacción realizada con criptomonedas, tal y como se representa en el en el siguiente gráfico elaborado específicamente para este trabajo, funcionaría de esta forma. La primera diferencia sustancial es que nadie sabrá quién es A ni B, únicamente que desde un monedero digital (equivalente a la cuenta bancaria) se quiere transferir una cantidad a otro monedero. A envía un mensaje a los usuarios notificando su intención. Estos comprueban que tiene saldo suficiente. Si es así, anotan esta transacción de forma provisional. Conforme pasa el tiempo y se van completando más transacciones se va conformando un bloque. Al llegar a la capacidad de la cadena de bloques se procede a validarlo.



Mediante complicados algoritmos matemáticos que requieren elevada potencia de computación, y por lo tanto alto consumo energético, los bloques quedan registrados de forma permanente en la cadena. Uno solo de estos bloques no podría ser modificado sin alterar todos los que están enlazados con él, algo que sería realmente improbable pues el resto de los nodos lo deberían validar. Este mecanismo asegura la integridad de la operación.

En el proceso de minado, los mineros reciben avisos de nuevas transacciones agrupadas

en bloques. Unos compiten con otros y el primero que consigue crear un bloque válido recibe una recompensa por el servicio, en la criptomoneda que esté operando.

La cadena de bloques está sincronizada entre los nodos de forma irreversible. Nadie podrá modificar el libro de registro sin que el resto se entere.

Esta tecnología permite asimismo asegurar la trazabilidad de las transacciones. Aunque no sean conocidas las identidades de A y B, es público el camino que ha seguido el envío.La transferencia de A a B se realiza de forma rápida y sin comisiones.

PRINCIPALES CRIPTOMONEDAS

Cronológicamente los primeros medios de pago virtuales fueron GoldAge[5] y LibertyDollars(2006)[6]. Eran centralizadas, es decir, operadas y supervisadas desde un solo punto.

Actualmente se cifran en más de 1.500, no dependen de ninguna entidad ni autoridad central, son por lo tanto descentralizadas.

Bitcóin[7]es sin duda la criptomoneda más popular y extendida en el mundo.En 2008SatoshiNakamoto[8] publicó en 2008 un artículo[9] en el que anunciaba que había desarrollado un nuevo sistema de pago electrónico, estando, basado en el trabajo que, sobre la base de la criptografía de clave pública que daba una solución al problema de los pagos electrónicos había publicado WeiDai describiendo lo que denominó el b-Money.En 2009 se publicó en el portal P2P, nuevamente bajo el nombre de SatoshiNakamoto, un mensaje del mismo en el que presentaba el portal oficial de bitcoin, las características fundamentales de esta nueva moneda digital describió el protocolo bitcóin, pero no fue hasta 2009 cuando la divisa entró en funcionamiento.

Bitcoin tiene un suministro finito de 21 millones que se espera alcanzar para el año 2140, un número finito con el fin de que fuera un medio de pago deflaccionario.

---

[5]Clausurado por las autoridades americanas por violación de la normativa bancaria *knowyourcustomer* (KYC).

[6] Estuvo presente en los medios de comunicación al ser detenido su fundador en mayo de 2013 como consecuencia de haber facilitado el blanqueo de 6.000 millones de dólares, procedentes de delitos tales como fraudes con tarjetas de crédito, robos de identidad, fraude de inversiones, piratería informática, pornografía infantil y tráfico de drogas, entre otros.
Grupo de Acción Financiera Internacional, "Monedas Virtuales. Definiciones, claves y riesgos potenciales", 2014,10.

[7] Más información en https://bitcoin.org/es/Bitcoin en Paraguay http://www.bitcoin-py.com/

[8]SatoshiNakamoto es seudónimo de la persona o grupo de personas que crearon el protocolo bitcoin y su software de referencia, Bitcoin Core. Hoy en día sigue sin conocerse su identidad.

[9]SatoshiNakamoto, "Bitcoin: un sistema de dinero en efectivo electrónico", (2008), https://bitcoin.org/files/bitcoin-paper/bitcoin_es.pdf

Su valor oscila continuamente y ha aumentado de forma considerable desde su nacimiento. Y es que, mientras que en sus inicios no alcanzaba el dólar, el valor hace apenas unos meses era de 19.000 dólares, para pasar a valer en agosto de 2018 apenas 6.000 dólares.

El segundo lugar en capitalización lo ocupa Ethereum[10]. En realidad, la moneda se llama mether y Ethereum hace referencia a un sistema que permite a los usuarios crear aplicaciones basadas en monedas virtuales que pueden ir más allá de su simple uso financiero al sistema que la controla. Lo más destacado de esta criptomoneda es su elevada velocidad de transacción y también que ha introducido en el mundo virtual el concepto de contratos inteligentes. Este método permite a usuarios o empresas firmar contratos sin comisiones ni control por parte de ningún país.

Litecoin[11] es una criptomoneda que permite realizar pagos instantáneos y de costo casi cero a cualquier parte del mundo. La ventaja de Litecoin es que provee tiempos de confirmación de transacción más rápidos que cualquier otra. Es una red súper simple para aquellos que necesitan mover pequeñas cantidades de dinero rápidamente.

Ripple[12] se creó para el sistema bancario ya que permite pagos globales más rápidos y a menor coste. En el sistema habitual, las transacciones trasfronterizas requieren un intermediario (y a veces varios) entre los bancos, lo que retrasa su finalización. Ripple funciona como si fuese una entidad de crédito que presta servicio a otros nodos o usuarios que realizan transacciones de crédito (intercambio de fondos o préstamos) dentro de un círculo con el que se mantiene una relación de confianza (sabemos que podemos "comerciar" con ellos). Al existir esta relación de confianza entre los participantes en la red, la suma de todas estas conexiones genera una red de usuarios y "entidades" entre las cuales fluye el crédito y, por tanto, entre las que se pueden realizar transacciones económicas. Esto permite simplificar enormemente las transacciones regulares para los consumidores de todo el mundo**.**

[10]Más información en https://www.ethereum.org
[11]Más información enhttps://litecoin.org/es/
[12]Más información enhttps://ripple.com

Dash se puede utilizar para pago entre consumidores pero nació con la idea de permitir pagos instantáneos en Internet y en tiendas físicas. Muchos establecimientos aceptan Dash igual que si utilizaran la moneda en curso legal del país, pero la transacción es más rápida.

Monero[13] es la criptomoneda de los más preocupados por la privacidad. Desarollada sobre el protocolo CryptoNote, un sistema de cifrado que hace que las transacciones no estén firmadas por una sola persona, sino por varias a la vez. Lo que hace es mezclar todos los moneros de todas aquellas personas que hagan transacciones de tal manera que sea imposible saber el origen de los fondos y cuál es el destino.

Por último mencionar IOTA, una criptomoneda no basada en la cadena de bloques que, aunque no tiene límites para su uso, está especialmente pensada para micropagos en el entorno del Internet de las Cosas[14]. Aumentó su valor casi un 500% los primeros días de diciembre de 2017.

La relevancia de bitcoin en el mundo de las criptomonedas es innegable, hasta el punto de que existe una denominación concreta para referirse a las criptomonedas diferentes al bitcoin o que se han creado como una alternativa al protocolo original. Son las *Altcoins*. Se pueden diferenciar dos grupos. El primero incluye las criptomonedas que provienen de una bifurcación (*fork*) de bitcoin, como son Litecon, Dogecoin, entre otras; y un segundo grupo que han construido su propio blockchain, utilizando hasta algoritmos de minería diferentes al de bitcoin. En este grupo encontramos a Ethereum, Nxt.

En este entorno es frecuente confundir el concepto de criptomonedas con el de token, ya que ambas describen unidades de valor de una cadena de bloques. Los token son comúnmente emitidos por emprendimientos fintech. Se asemeja a las criptomonedas en que su valor es aceptado por una comunidad y utilizan blockchain, sin embargo su objetivo no es sólo ser un medio de pago pues puede representar cualquier activo

[13] https://getmonero.org
[14] Internet de las cosas (IoT por sus siglas en inglés), un concepto que nació en el Instituto de Tecnología de Massachusetts (MIT). Se trata una revolución en las relaciones entre los objetos y las personas con Internet.

fungible y negociable. La mayor parte de tokens se distribuyen a través de una Oferta Inicial de Moneda (ICO).

1	Bitcoin	$141.191.662.624	$8.375,86
2	Ethereum	$81.512.010.593	$835,71
3	Ripple	$39.294.373.206	$1,01
4	Bitcoin Cash	$20.832.751.755	$1.228,31
5	Cardano	$10.192.009.210	$0,393103
6	Litecoin	$8.334.167.960	$151,09
7	Stellar	$7.224.120.863	$0,391929
8	NEO	$6.900.660.000	$106,16
9	EOS	$5.812.391.598	$8,80
10	NEM	$5.066.828.999	$0,562981
11	IOTA	$5.014.328.221	$1,80
12	Dash	$4.800.078.316	$609,41
13	Monero	$3.880.037.710	$247,03

Capitalización criptomonedas 10 de febrero 2018
Fuente: www.coimarketcap.com

CÓMO SE CONSIGUEN

Las formas más habituales de conseguir criptomonedas son las siguientes:

1. Aceptándolas como medio de pago. Esta es la manera más sencilla. Aunque no son muy números, si existen comercios, hoteles, etc. en las que son aceptadas.
2. Minando. Se trata de una analogía digital, al igual que ocurre con la minería de recursos naturales como el carbón o el oro. Como se ha comentado anteriormente, los mineros ponen poder de computación al servicio del sistema y cambio son recompensados con criptomonedas.

   Una de las alternativas que desde hace poco tiempo se están barajando consiste en la minería en la nube o *cloudmining*. Es un proceso de minado de Bitcoins que se hace de manera remota, en un centro de datos que cuenta con capacidad de procesamiento compartida. De modo, que el usuario pueda gestionar su

propia mina, sin tener que gestionar prácticamente nada. Empresas privadas ofrecen este servicio alrededor del mundo, permitiendo la minería de bitcoins con un bajo coste de mantenimiento lo que se traduce en una mayor rentabilidad y ganancia. Sin embargo es necesario tener cuidado pues más del 90% de las páginas de minería en la nube que se han desarrollado en 2017 han resultado ser una estafa piramidal[15], ya que duraban escasamente cuatro meses de operación quedándose estancada la inversión.

3. Visitando páginas de internet. Existen una amplia gama de páginas de internet que funcionan como plataformas en las que por ver la publicidad ofrecen a cambio una pequeña cantidad.

4. Realizando apuestas. El anonimato hace de las monedas digitales un medio muy atractivo para apostar. En algunos países la legislación obliga a apostar en casas de apuestas dadas de alta en el país. Al ser desconocida la identidad no puede ser identificada la nacionalidad del apostante. Desde el punto de vista fiscal también presenta ventajas pues las transacciones son prácticamente irrastreables y por lo tanto opacas.

5. Invirtiendo. En los últimos meses han experimentado fuertes revalorizaciones que reflejan patrones propios de burbujas especulativas[16]. Autoridades monetarias están advirtiendo de que al carecer de valor intrínseco, se convierten en inversiones altamente especulativas que podrían acarrear la pérdida total de las cantidades invertidas.

USO DE LAS CRIPTOMONEDAS

Inicialmente nacieron como una forma de pago anónima y segura. Bitcoin es aceptada

[15] La empresa MinerWorld, que tiene sede en Brasil, aseguraba que sus operaciones en Paraguay se encontraban respaldadas por la Comisión de Valores de este país. El 3 de octubre de 2017 la Comisión de Valores de Paraguay emitió la circular no. 015/2017, en la cual desmintió estas aseveraciones y enfatizó que las operaciones de esta empresa son completamente ilegítimas, encubriendo un esquema piramidal o ponzi para estafar a los usuarios, por lo que pueden emprender medidas legales al respecto.

[16] Banco de España, "Comunicado conjunto de la CNMV y del Banco de España sobre "criptomonedas" y "ofertas iniciales de criptomonedas" (ICOs)", (8 de febrero de 2018), https://www.bde.es/f/webbde/GAP/Secciones/SalaPrensa/NotasInformativas/18/presbe2018_07.pdf

por más de 100.000 comerciantes[17] en más de 92 países, de los cuales 6.000 tienen presencia física y hay más de 13 millones de billeteras virtuales creadas.Aunque el volumen de transacciones con bitcoin se incrementa más del 50% anual, su número está muy lejano de las transferencias y pagos del sistema financiero.

Pero en realidad las criptomonedas se emplean en la actualidad más como un activo una reserva de valor que como un medio de pago, de ahí que en muchas ocasiones de las denomine criptovalores o criptoactivos. Son objeto de especulación constante. Su gran volatilidad hace que en unos días se revaloricen un 50% o pierdan su valor en mayores porcentajes.

La primera transacción completada con bitcoin se produjo en mayo de 2010. Un programador compró dos pizzas y pagó por ellas 10.000 bitcoins, equivalentes entonces a 40 dólares norteamericanos. Hoy equivaldrían a unos 90 millones de dólares.

Pero el uso de las criptomonedas también cruza al otro lado de la ley. El anonimato que proporcionan las convierte en el medio de pago perfecto para el pago de ilícitos.

En la internet profunda (Deep web) los productos que se adquieren en los mercados clandestinos (armas, drogas, pornografía de menores, etc.) se pagan con bitcoin, si bien los delincuentes se están moviendo hacia Monero ya que el rastreo por parte de las fuerzas policiales en la práctica es imposible[18].

Lamentablemente otro uso que aparece con frecuencia en los medios de comunicación[19] es el pago de rescates tras el ataque de un ramsonware[20]. En los ataques se incorpora un código malicioso en los ordenadores que hace que estos no se puedan utilizar a no ser que se pague una determinada cantidad en bitoins u otra criptomoneda.

---

[17] Banco de la República de Colombia, "Criptomonedas", *Documentos técnicos o de trabajo* (octubre 2017), 7, http://www.banrep.gov.co/docum/Lectura_finanzas/pdf/documento-tecnico-criptomonedas.pdf

[18] Europol, "Internet Organised Crime Threat Assessment (IOCTA)",(2017, 61

[19] Uno de los más conocidos fue Wannacry. El ataque empezó el viernes 12 de mayo de 2017, y ha sido descrito como sin precedentes en tamaño, infectando más de 230.000 ordenadores en más de 150 países Los países más afectados que han sido reportados fueron Rusia, India, Taiwán, el servicio nacional de salud de Gran Bretaña, Telefónica de España, FedEx, aerolíneas LATAM, bancos a nivel mundial, etc.

[20] El ransomware (también conocido como rogueware o scareware) restringe el acceso al sistema y exige el pago de un rescate para eliminar la restricción.

Una modalidad de actividad ilícita no muy conocida es el *criptojacking*o minería ilegal. Los ciberdelincuentes toman el control de ordenadores ajenos para utilizarlos para la explotación de criptomonedas como bitcoin. Para caer presa de esta amenaza, es suficiente con visitar una de las más de 50.000 páginas web que contienen el código malicioso. En ellas, se incluye una programación que obliga a los ordenadores a minar criptomonedas a nombre de los hackers. La CPU del equipo afectado se secuestra de tal manera que es de poco uso para cualquier otra actividad.

Y una vez que los delincuentes tienen las criptomonedas en sus monederos ¿qué hacen con ellas? ¿Cómo las blanquean? Lógicamente no comentarán el error de convertirlas directamente en dinero de curso legal, ya que estas operaciones sí serían rastreables ni se acercarán a un cajero pues precisa la presencia física. Tienen diferentes opciones. Utilizar intermediarios, pero es de elevado riesgo pues pueden ser delatados si estos son detenidos. Una vía más segura consiste en hacer uso de los servicios de los *exchangers*que facilitan la posibilidad de cambiar bitcoins por otras monedas de curso legal, entre ellas euros o dólares, o las webs de *trading*, que permiten comprar y vender bitcoins como si fueran acciones.

REGULACIÓN

En el ámbito de las criptomonedas la falta de regulación llega al extremo de no existir ni siquiera un consenso internacional en su definición. En algunos países son consideradas mercancías (en Canadá para efectos fiscales), en otros fondos transferibles, activos financieros, etc. La realidad actual es que el tratamiento de las criptomonedas no sólo varia de un país a otro sino que dentro del mismo país tiene distintos enfoques según se analicen desde el punto de vista financiero, legal, cambiario o tributario.

El hecho de anunciar su posible regulación desencadena una bajada en su valor. En los primeros días de enero de 2018 el precio del bitcoin bajó un 14% en una sola jornada al anunciar el gobierno que está trabajando en un proyecto de ley para prohibir las transacciones con criptomonedas.

En la siguiente tabla se refleja la situación regulatoria en algunos países.

	Advertencias al consumidor	Reglas sobre Blanqueo y financiación terrorismo	Tratamiento tributario	Registro/licencias intermediarios	Proyectos internacionales blockchain
España	X	X	X	X	X
EEUU	X	X	X	X	X
Canadá		X	X	X	X
Brasil	X		X		X
Japón		X	X	X	X
Unión Europea	X	X	X	X	X
Alemania	X		X		X
Suiza		X	X	X	
Francia	X			X	X
Reino Unido	X		X	X	X
Singapur	X	X	X	X	X
Filipinas		X		X	
Chile					X
Colombia	X				

Fuente: Banco de la República de Colombia – Documentos Técnicos o de trabajo. Criptomonedas.

FUTURO

Hablar de futuro es siempre difícil y arriesgado, mucho más cuando entra en juego la tecnología. Si pensamos en los ordenadores que existían treinta años atrás, grandes salas llenas de equipos informáticos, con menos potencia y capacidad que cualquier teléfono móvil que hoy llevamos en un bolsillo.

Se anuncia una nueva era de ordenadores, la computación cuántica. No será una evolución de lo que ahora conocemos, supondrá una ruptura total. De momento son

solamente un objeto de estudio por parte de grandes compañías como IBM, universidades y Estados, pero serán capaces de hacer en unos segundos operaciones que ahora precisan mucha potencia o son imposibles de resolver. Esto afectará de forma muy directa a los algoritmos criptográficos. Serán capaces de desvelas las claves que ahora son inexpugnables.

No significa que la base tecnológica de las criptomonedas llegará a su fin porque es lógico que están también irán avanzando y adaptándose a las nuevas tecnologías.

Se supone que estos avances reducirán el consumo de energía en el proceso de minería. Con la tecnología actual llegará un momento en que no será sostenible energéticamente. Dentro de unos años, según los estudios consultados, en la producción de bitoins se consumirá tanta energía como la que consume Estados Unidos y hay quien opina que como todos los países del mundo juntos.

Otra camino que deberá desarrollarse es el regulatorio. No será tarea fácil pues exige un acuerdo a nivel internacional, pues las criptomonedas lo son. Ahora bien, ¿esta regulación no irá en contra de su propia naturaleza?

El presente es interesante y el futuro a corto, medio y largo plazo en el mundo global que vivimos será sin duda fascinante, donde las matemáticas, la física y el Derecho jugarán un papel esencial.