# BITCOIN

# BITCOIN

**Tulio Rosembuj**
Catedrático de Derecho Financiero
y Tributario de la Universidad de Barcelona

el Fisco

Primera edición, 2015


Valls i Taberner, 14, ático 2ª
08006 Barcelona
trosembuj@telefonica.net

ISBN: 978-84-944098-0-6
Dep. Legal: B-14895-2015
Impreso por: Grafiques Rey, S.L.

**"Bitcoin gives us, for the first time, a way for one Internet user to transfer a unique piece of digital property to another Internet user, such that the transfer is guaranteed to be safe and secure, everyone knows that the transfer has taken place, and nobody can challenge the legitimacy of the transfer. All these are exchanged through a distributed network of trust that does not require or rely upon a central intermediary, like a bank or a broker.**

**What kinds of digital property might be transferred in this way? Think about digital signatures, digital contracts, digital keys (to physical locks or to online lockers) digital ownership of physical assets, such as car and houses, digital stocks and bonds and digital money."**

**Marc Andreessen**

# ÍNDICE

# CAPÍTULO I
# BITCOIN. DE LA MONEDA DIGITAL A LA MONEDA VIRTUAL

El dinero señala tres funciones comunes: unidad de cuenta; medio de intercambio e instrumento de ahorro e inversión. La unidad de cuenta o de medida sirve para asignar valor económico a los bienes o servicios; el medio de cambio indica los bienes o servicios que se cambian por dinero, o sea lo que se denomina moneda y, finalmente, como instrumento de ahorro o inversión para procurarse un rendimiento en términos de beneficios, incluidos los intereses.

El dinero es una creación jurídica y, asimismo, de consenso social, de confianza social. El dinero de curso legal goza del respaldo público y es el medio general de pago admitido y aplicado y sus clases acomunan, dinero metálico, dinero corriente y dinero bancario. A esto se le añade el dinero electrónico y, asimismo, el dinero fiduciario, comunitario, digital o virtual.

## 1. Dinero Electrónico

La Directiva 2009/110/CE define como dinero electrónico»: todo valor monetario almacenado por medios electrónicos o magnéticos que representa un crédito sobre el emisor, se emite al recibo de fondos con el propósito de efectuar operaciones de pago y que es aceptado por una persona física o jurídica distinta del emisor de dinero electrónico.[1]

1. Directiva 2009/110/ce del parlamento europeo y del consejo de 16 de septiembre de 2009, art.2, 2).

De modo que el concepto de dinero electrónico está compuesto por tres elementos: valor monetario almacenado electrónicamente; emitido a la recepción de los fondos en una cuantía no inferior al valor monetario emitido; aceptado como medio de pago por otras partes distintas al emisor.

El dinero electrónico se configura como un bien digital de transferencia de valor cierto, atado al respaldo de una moneda de curso legal (dólar, euro, yen) y bajo la dirección central de la misma autoridad monetaria que supervisa la moneda y los sistemas de pago de billetes u otros formatos de dinero en efectivo. Y, lo que es más importante, con garantía legal de reembolso en todo momento por su valor nominal.[2]

La moneda digital y virtual no es asimilable al dinero electrónico, excepto en que ambos son bienes digitales, porque no resulta emitida al recibo de fondos para las operaciones de pago, vinculadas a una moneda de curso legal. *Bitcoin,* por ejemplo*,* es una moneda descentralizada, no sometida a la autoridad monetaria , cuya unidad de cuenta no es una moneda de curso legal, sino los propios *Bitcoins, y* cuya producción tiene generación matemática(por obra de los *mineros)* en beneficio de la comunidad de usuarios, persona a persona, en red, que la aceptan para sus transacciones.

Desde una perspectiva meramente imaginativa, no obstante, nada impediría que la moneda digital o virtual pudiera devenir dinero electrónico en el futuro, en el caso que pudiera adquirir respaldo legal de la autoridad monetaria pública, supervisión de sus operaciones y obligaciones de transparencia en materia de riesgos de blanqueo de capitales y financiación del terrorismo, como aparece en las propuestas del Reino Unido.[3]

A la inversa, el dinero electrónico, por su propia definición, es imposible que evolucione, en sus términos actuales, hacia el ámbito de la moneda digital o virtual: la moneda digital o virtual no es digitalización de la moneda de curso legal. Es una moneda alternativa y complementaria a la *fiat currency*, susceptible de reconocimiento si, por caso, su regulación legal cuenta con el soporte

2. Fondo Monetario Internacional, Bitcoin versus Electronic Money, Brief, january 2014.

3. V. punto 7.1.

de la autoridad monetaria como medio de pago, unidad de cuenta, adicional a los existentes.

Por último, el dinero legal, y obviamente el electrónico, es dinero territorial, geográficamente determinado; mientras que la moneda digital o virtual nace extraterritorial, ajena a fronteras físicas o perímetros distintos a los que su comunidad de usuarios postule: local, estatal, global: es un bien digital de transferencia de valor monetario por internet. [4]

## 2. La criptoanarquía. Descripción de Bitcoin

*David Chaum* es uno de los iniciadores de la criptografía aplicada a los pagos, firmas ciegas para pagos ilocalizables, imposibles de rastrear. Un sistema que, por un lado, no permite a terceras partes la determinación del perceptor, el tiempo o el importe de los pagos hechos por otra persona; importante en términos de intimidad y privacidad; por otra, la capacidad de los individuos para proveer una prueba del pago o informar de la identidad del perceptor bajo circunstancias excepcionales. [5]

Entre 1992 y 1994 se difunde la criptografía como manifestación de un movimiento denominado criptoanarquÍa: un medio para tutelar la privacidad y la libertad individual en la red: "...una criptografía potente puede causar la declinación del poder del estado y quizá aún colapsarlo. Creemos que la expansión en el ciberespacio con comunicaciones seguras, *moneda digital,* anonimato y seudónimos y otras interacciones criptomediales cambiaran profundamente la naturaleza de las interacciones económicas y sociales."[6]

"La informática está al borde de proporcionar la capacidad a individuos y grupos de comunicarse e interactuar entre ellos de forma totalmente anónima. Dos personas pueden intercambiar mensajes, hacer negocios y negociar contratos electrónicos, sin saber nunca

4. J.J. Doguet, The nature of the form: legal and regulatory issues surrounding the bitcoin digital currency system, 73 Louisiana. L.Review, 2013, p.1143.

5. D.Chaum, Blind signatures for untraceable payments, Department of Computer Science University of California, Santa Barbara, 1983.

6. Timothy C.May, Cifernomicon. Manifiesto criptoanarquista, 1992."Un espectro acecha el mundo contemporáneo, el espectro de la criptoanarquía".

el Nombre Auténtico, o la identidad legal, de la otra. Las interacciones sobre las redes serán intrazables, gracias al uso extendido de re-enrutado de paquetes encriptados en máquinas a prueba de manipulación que implementen protocolos criptográficos con garantías casi perfectas contra cualquier intento de alteración. Las reputaciones tendrán una importancia crucial, mucho más importante en los tratos que las calificaciones crediticias de hoy en día. Estos progresos alterarán completamente la naturaleza de la regulación del gobierno, la capacidad de gravar y de controlar las interacciones económicas, la capacidad de mantener la información secreta, e incluso alterarán la naturaleza de la confianza y de la reputación".

*Wei Dai* declara su fascinación por el manifiesto de *Tim May*: en la criptoanarquia el gobierno no es temporalmente destruido sino permanentemente prohibido y permanentemente innecesario. En ello basa su propuesta de un protocolo monetario sin gobierno ni autoridades financieras. "Es una comunidad donde la amenaza de violencia es impotente porque la violencia es imposible y ello porque sus participantes no pueden ser conectados a sus nombres verdaderos o localizaciones físicas".

"Debemos asumir la existencia de una red ilocalizable, imposible de rastrear, donde los ordenantes y los receptores son identificados por seudónimos digitales (v.g. claves públicas) y cada mensaje está firmado por el remitente y encriptado a su receptor."[7]

El fundamento es que la criptografía ofrece una libertad individual irrestricta sin peaje al derecho a la intimidad, sin perjuicio de reconocer que dentro de ello todos los males públicos globales se verán potenciados. Pero, es el coste de la libertad de todos: un mercado líquido que eliminará las fronteras de la propiedad intelectual.

La primera motivación de *Bitcoin* es ideológica. Por un lado, anular la necesidad de confianza en terceras partes por encima de los participantes y, por otra, minimizar el control centralizado de la moneda y el sistema de pago. El origen de Bitcoin tiene sus raíces en la criptoanarquía.[8]

---

7. Wei Dai, B-Money, 1998., proponiendo un protocolo monetario sin necesidad del gobierno o entidades subordinadas.

8. Introduction to Bitcoin, Lam Pak Nian, D.LEE Kuo Chuen, p.11 en D.LEE Kuo Chuen, Handbook of Digital Currency. Bitcoin, innovations, financial instruments and

## **2.1.** LIMITACIÓN DE LA INTERMEDIACIÓN FINANCIERA

La premisa es que el comercio electrónico reposa casi exclusivamente en terceras partes de confianza –las instituciones financieras– para el proceso de los pagos electrónicos.

"Lo que se necesita es un sistema de pago electrónico basado en la prueba criptográfica en lugar de la confianza, permitiendo la transacción directa entre dos partes que la quieran celebrar entre sí, sin necesidad de un tercera parte de confianza."[9]

El núcleo es el pago en línea directo de una parte a otra sin intervención de la entidad financiera.

## **2.2.** LIMITACIÓN DE LA AUTORIDAD MONETARIA CENTRAL

La ausencia de intermediación entre las partes propone un sistema de intercambio monetario en línea descentralizado, independiente de cualquier autoridad central, pública, ajena a la voluntad de las partes.

El sistema *Bitcoin* recupera para sí el atributo de una red completamente distribuida en la que el protagonismo total de las transacciones reside en los usuarios, con prescindencia de las instituciones financieras.[10]

## **2.3.** NODOS SINGULARES INTERCONECTADOS EN RED DE ORDENADORES

En sentido estricto esto se configura como un sistema de pago de comercio electrónico entre los que participan en la intercomunicación, una red de ordenadores entre pares (**P2P**), eslabones de una misma cadena digital iguales entre sí: *nodos* singulares que

---

big data, Elsevier, 2015, San Diego. Entre los iniciadores, los ya citados Chaum, Dai, y también Back- Hashcash-, Szabo (1999, 2002,2008, Shirky (2000).

9. S.Nakamoto, Bitcoin: a peer-to-peer electronic cash system, www.bitcoin.org., 2008.

10. C.K.Elwell, M.Maureen Murphy, M.V.Seitzinger, Bitcoin: Questions, Answers, and Analysis of legal Issues, Congressional Research Service, july 15, 2014, 7-5700

producen el intercambio directo de información del bien digital entre los ordenadores conectados.

*Bitcoin* está fundado en un protocolo de software abierto y no propietario. El software puede ser libremente descargado en cualquier ordenador que en tal modo se alía a la red en funcionamiento.

"En lugar de una autoridad central, la red *Bitcoin* consiste en ordenadores alrededor del mundo aplicando el software *Bitcoin,* que opera el protocolo para administrar las transacciones *Bitcoin*."[11]

## **2.4.** LA MONEDA DIGITAL

*Bitcoin* es una moneda digital: "una cadena de firmas digitales."[12] Una cadena de bits de transmisión electrónica, representativa de valor, de ordenador a ordenador, sujeta a estrictos protocolos de software criptográfico.

El bien digital es servicio de software, al que puede accederse remotamente, sin intervención humana, y cuyo contenido es universal (sonido, imagen, datos, hechos) transmitidos electrónicamente, que puede disfrutarse o utilizarse previo derecho de acceso u uso, oneroso o gratuito, que no tiene equivalencia o simetría con el bien material o físico que representa, salvo por aproximación.[13]

La moneda digital es más que un bien digital en sentido estricto: un bien de información intangible fundado en protocolos específicos de software libre, representativo de un valor de un bien físico o material (dinero efectivo) y, detalle significativo, en el que la creación de moneda da lugar a contraprestación por el trabajo realizado por determinado usuario o partícipe (*miner*) en la comunidad en red.[14] Pero, como se verá, va más allá del bien digital en cuanto a que su naturaleza virtual supone exclusión y exclusividad

---

11. P.Murck, Testimonio de Bitcoin Foundation ante The Homeland Security and Governmental Affairs Committee, November 18 2013.

12. S.Nakamoto, cit., p.2

13. T.Rosembuj, El impuesto digital,Barcelona,2015,p.78

14.T.Rosembuj , El impuesto digital,p.36.

del titular respecto a los otros y, asimismo, escasez, en cuanto a que su objeto monetario es limitado y agotable.

## **2.5.** LA CRIPTOMONEDA DIGITAL

La moneda digital, el bien digital, tiene su fuente criptográfica como presupuesto para la seguridad en la comunicación, tutela de la intimidad y la convalidación del tráfico digital en la red de usuarios. Por ello, frecuentemente, la definición de *Bitcoin* e instrumentos análogos es el de criptomoneda. La matemática criptográfica es el único medio para reemplazar con garantías el modelo de confianza basado en la intervención de terceros. La protección matemática es suficiente y necesaria en la creación, almacenamiento y transferencia de datos informáticos, de información acreditada y acreditable, de valor patrimonial o documental entre las partes.

Los protocolos criptográficos sirven para tutelar la información que se crea, almacenarla y proceder a la transferencia de datos, mediante algoritmos matemáticos.[15]

Las funciones de la criptográfica se pueden sintetizar en cuatro aspectos: la autenticación, la intimidad, la integridad y la irrevocabilidad. Primero, la autenticación de la propia identidad, de lo que serían sus huellas digitales por Internet, llámese, por ejemplo, la firma digital como elemento de identificación inseparable de la persona, una proyección externa de su intimidad. Segundo, conseguir que la información electrónica transcurra, como en el papel del correo tradicional, entre firmante y receptor, con la certeza que el contenido y la forma del mensaje de datos no se transforma en público y universal. Tercero, confirmar que el mensaje que se envía es exactamente el mismo que se recibe, sin alteración o modificación del original. Cuarto, una suerte de irrevocabilidad o no repudio, que permita contrastar que el remitente realmente envió el mensaje que se recibe.

---

15. C.Viegas, J.Giglio Santamaría, S.Perciavalle, M.Urquiza, Bitcoin: un desafío para la ejecución de políticas de la Banca Central. Banco Central de República Argentina, agosto 2014, p.4.

La criptomoneda utiliza la criptografía para la transferencia e intercambio de datos digitales en una modo descentralizado entre los usuarios de la red, apoyándose en cadenas alfanuméricas (*digital tokens)* aptas para su registro público en la base de datos descentralizada de *Bitcoin.* La transmisión electrónica se perfecciona sin que se requiera una tercera parte intermediaria asegurando la visibilidad de la transacción entre todos los participantes y la autenticidad de la titularidad y propiedad de quien transmite. [16]

### 2.5.1. La encriptación asimétrica

La encriptación o cifrado asimétrico es el modo utilizado de transferencia electrónica entre las partes. Cada una de ellas posee dos claves, que son exclusivas e irrepetibles. Una de las claves es susceptible de ser conocida públicamente y la otra es privada. La clave pública es la dirección o billetero *Bitcoin,* una cadena alfanumérica, números y letras, de 33 dígitos. Cada clave pública tiene su par de clave privada, que solo es de conocimiento del usuario.

Asimétrico significa que la clave pública, aún derivando de la clave privada, hace imposible conseguir la clave privada de la clave pública.

La clave pública, dirección o billetero, habilita para verificar las firmas digitales, mientras que la clave privada es la firma, la fuente real de las firmas digitales: la clave pública es compartida; mientras que la clave secreta permanece personal y privada.[17]

El proceso comienza cuando la persona anuncia a la red un mensaje de datos que significa la transferencia de un cierto valor de *Bitcoin* desde su dirección o clave pública a la clave pública del receptor. La clave privada es equivalente a la firma digital. Por tanto, cada persona en la red puede verificar que el mensaje de datos está firmado por el titular de la clave pública que dio origen a la transacción y por tanto, en principio, es válida.

---

16. E.Dourado-J.Brito,Cryptocurrency, The New Palgrave Dictionary of Economics, 2014, Editores S.N.Durlauf-L.E.Blume.

17. Introduction to Bitcoin, cit., p.21.

La clave pública y privada son cadenas criptográficas de números y letras, y funcionan en forma par y complementaria. La primera permite crear la dirección de *Bitcoin* y la segunda es la prueba de titularidad y propiedad en el registro público de operaciones. La dirección *Bitcoin,* o billetero, es el primer paso para usar la red y corresponde a una clave privada, conocida solo por el usuario.

Cada *Bitcoin* es propiedad de una dirección *Bitcoin*, que consiste en una clave pública y la clave privada indica al propietario del *Bitcoin* habilitado para realizar la transacción en la red. El remitente firma digitalmente que hay una transferencia de *Bitcoin* desde una dirección a otra. Una transmisión criptográfica firmada de fondos desde una clave pública a otra.[18]

La clave pública tiene la función de memoria histórica: permite a los usuarios enviar valor a esta dirección y trazar la huella de las transacciones precedentes transferidas a o desde esta dirección. Si el titular quiere remitir valor debe añadir una función *hash* (un algoritmo que resume un mensaje de datos en una cadena fija de bits), el importe y el que es el receptor de la clave pública.

La transacción se articula como un mensaje de clave pública entre dos direcciones. De billetero a billetero. Pero, la validez de la operación requiere la clave privada como firma digital.

"La autenticación es como la huella digital, solo puede existir un generador de transferencias con una determinada dirección."[19] La firma sirve para confirmar que la transacción tuvo su fuente en la clave pública. La firma digital es el centro del esquema de la moneda virtual.

La firma digital es irrevocable y no puede cambiarse. A partir de ese momento la transacción se transmite a toda la red. La firma certifica que el mensaje de datos es auténtico.

---

18. J.A.Kroll I.C.Davey, E.W.Felten,The economics of Bitcoin mining, or Bitcoin in the presence of adversaries, The Twelfth Workshop on the Economics of Information Security(WEIS 2013, Washington DC, june 11-12- 2013.

19. A. Blundell- Wignall, 2014, The Bitcoin Question: currency versus trust-less transfer technology, OECD Working papers on finance, insurance and private pensions, 37.

### 2.5.2. La confirmación criptográfica de la transacción. La autocertificación

*Bitcoin* propone la solución a dos problemas puntuales del dinero virtual. Por un lado, preservar la intimidad entre las partes, sin intermediarios, lo cual consigue mediante la criptografía asimétrica, clave pública y clave privada, matemáticamente vinculada: la primera, es la dirección o el billetero, pública y conocida; la segunda, es secreta y permite crear la transmisión de valor mediante la firma digital entre una dirección y otra.

La clave pública, se dice, es la dirección del buzón. Cualquiera puede usarlo para enviar su correspondencia. Pero, solo el titular del buzón tiene la llave para abrirlo y conocer su contenido.[20] La segunda de las soluciones es más ambiciosa, puesto que se propone eliminar los registros y certificaciones centralizados, sustituyéndolos por un registro público, universal, distribuido y descentralizado en la red de usuarios.

La autocertificación es el modelo *Bitcoin* y la responsabilidad es del conjunto de la comunidad de usuarios. Aquí se plantea una distinción trascendental con otros modelos propuestos de firmas digitales, v.g. UNCITRAL, que solicitan para su aplicación la existencia de terceras partes autorizadas, públicas o privadas, para certificar los servicios digitales entre las partes. Por tanto, la Cadena de Bloques deviene una seña de identidad definitiva de *Bitcoin*. Sin exagerar puede decirse que cuando se habla de innovación tecnológica la referencia no es a la criptografía asimétrica, conocida en otras esferas en línea; la diferencia es el registro público de la propiedad, del comercio, del tráfico jurídico que prescinde de cualquier convalidación ajena al propio sistema establecido por los participantes, con igual o mayor certeza jurídica que los terceros autorizados. La distribución de la red no es solo la interconexión, sino, la responsabilidad de cada uno y del conjunto.

¿Cómo se evita que cada moneda se gaste más de una vez?. La autoridad central desaparece y es la comunidad de usuarios que la sustituye verificando y comprobando que ello no ocurra: "el

20. J.Fairfield,"Bitproperty", Washington & Lee Public Legal Studies Research Paper Series.n.2014-17, october 2, 2014, p.18.

trabajo se distribuye entre miles de usuarios que contribuyen su capacidad informática para reconciliar y mantener el registro de la Cadena de Bloques."[21]

La respuesta es la cadena de transacciones, de firmas digitales, denominada Cadena de Bloques (*Blockchain)*.Cada diez minutos, los "mineros" recogen en un bloque las transacciones que se celebran y verifican sus condiciones de validez, previo a su calificación como bloque y su añadido, en orden cronológico, a la cadena de bloques: el registro público y oficial de las transacciones en el sistema.

Cada *Bitcoin* y cada usuario está encriptado con una identidad desconocida para los ajenos a la transacción, pero incorporado a un registro público de todas las transacciones de *Bitcoin* en orden cronológico (*BlockChain)*, al cual acceden todos los ordenadores en la red, sin que conozcan la información personal de las partes.

La Cadena de Bloques opera como una base de datos pública global asegurando que las transferencias ocurren en condiciones válidas y regulares, evitando problemas como el "*double spending*", la posibilidad que alguno gaste la misma unidad de *Bitcoin* más de una vez.

La Cadena de Bloques es el medio mediante el cual los usuarios pueden verificar, sin necesidad de intermediarios, que no se gastan dos o más veces los mismos bitcoins. Todas las transacciones se registran y concilian en la Cadena de Bloques, pero, lo hacen miles de nodos interconectados en la red.

"En esencia, toda la red par-a par toma el lugar de una tercera parte de confianza".[22]

### 2.5.3. El trabajo retribuido de los mineros

La representación de valor de la moneda virtual ocurre y se materializa solo en cuanto pasa a ser una entrada en el registro

---

21. E.Dourado, J.Brito, Cryptocurrency, The New Palgrave Dictionanary of Economics, 2014, Editors S.N.Durlauf, L.E.Blume…. "Nuevas transacciones son chequeadas contra la Cadena de Bloques para asegurar que los mismos bitcoins no han sido previamente gastados, pero el trabajo de verificar las nuevas transacciones no lo hace una tercera parte de confianza."

22. E.Dourado-J.Brito, cit.p.3.

público global y universal. Desde la perspectiva del espectador la transmisión de valor entre las partes inscripta viene a indicar que una cantidad de *Bitcoin* asociada con la la clave pública, la dirección o el billetero de un usuario pasa a quedar vinculada a otra clave pública, dirección, billetero, de otra parte. La transmisión es objeto de anuncio a toda la comunidad en red, y no solo a la otra parte, de modo que esta pueda convalidarse mediante los mineros y quedar publicada en la Cadena de Bloques.[23]

Cada nuevo bloque de la cadena resulta de la comprobación de las transacciones ocurridas cada diez minutos. La verificación ocurre por obra de los denominados "mineros". De su actividad depende si añadir o rechazar el bloque de las nuevas transacciones a la cadena. El minero verifica las transferencias digitales resolviendo un problema matemático cuya solución es difícil, pero fácilmente constatable. Una vez resuelto, la solución del problema se comunica a otros mineros de la red, que la confirman o rectifican. Las transacciones confirmadas bajo examen se incorporan, entonces, como nuevos bloques a la cadena de bloques.

La creación de nuevos *Bitcoins* depende de la "prueba de trabajo" de los mineros, que son usuarios que quieran o estén dispuestos a su realización. El añadido de nuevos bloques implica la solución matemática por el minero de problemas matemáticos complejos de solución pero fáciles, de verificar y que, a la vez, le suponen, si los otros mineros lo aceptan, una retribución en moneda por el esfuerzo realizado. El resultado es que una vez producida la confirmación de las transacciones en espera se comunican al resto de la comunidad de usuarios y se agregan a un nuevo bloque en la cadena.[24]

El oro de la moneda lo descubre el minero, que puede ser cualquiera de los miembros de la red, resolviendo un algoritmo matemático. El minero introduce nueva moneda *Bitcoin* en cir-

---

23. I.Mas, D.LEE Kuo Chuen, Bitcoin-Like Protocols and Innovations, p.423, Handbook of Digital Currency,cit.

24. B.Segendorf, What is Bitcoin?.Sveriges Riksbank Economic review, 2014, 2. p.75. Los mineros deben descubrir una función *hash,* convirtiendo un número o letras de extensión arbitraria en un número fijo. Cuando esto sucede el minero puede exhibir la solución y añadir el bloque a la cadena, previa aceptación del resultado por otros mineros de la red.

culación. La consecuencia es la formulación de un nuevo bloque que incorpora las transacciones recientes. Los nodos individuales conectados en la red ofrecen su consenso a la confirmación. Pero, lo que es importante destacar es que el trabajo del minero se ve recompensado en monedas *Bitcoin* o, en su caso, contraprestaciones determinadas.

Al inicio, los mineros recibían una recompensa de 50 *Bitcoins* por la solución del problema matemático. Esta recompensa se va reduciendo por mitad cada cierto tiempo y en 2012 consistió en 12 unidades. La cantidad de moneda creada por los mineros produce la caída de sus retribuciones que, definitivamente, cesará al momento en que habrá unas 21 millones de unidades en existencia: la creación monetaria no depende de la función del banco central. La oferta surge de un algoritmo predecible y de los propios usuarios de la red. El número total de *Bitcoin* será de 21 millones de monedas,.En el interín la retribución dejará de ser en moneda y se convierte en tarifas por transacciones realizadas.[25]

Todo el proceso está controlado por un algoritmo que aproxima los datos de la producción de *Bitcoin* al promedio comparable a la extracción de materias primas como el oro.[26] Es la idea de *Nakamoto*: "el agregado constante de una cantidad de nuevas monedas es análoga a la de los mineros de oro aplicando recursos para añadir oro a la circulación."[27]

La recompensa a los mineros tiene otro efecto destacado. En efecto, la moneda digital se representa como un bien digital perfecto y afronta uno de los problemas más delicados de la economía digital en general. En todos los demás ámbitos, la cooperación o cocreación de valor del bien digital carece de reconocimiento económico, es puro trabajo gratuito. La creación de riqueza aprovecha a los que explotan la actividad, pero, dejando en el camino a los usuarios que contribuyen a su generación. En cambio, la moneda criptográfica digital asume el trabajo de sus creadores como

25. R.Bohme, N.Christin, B.Edelman, T.Moore, Bitcoin, Harvard Business School, Working Paper, 15-015, july 15,2014. El año 2140 es el año que se estima que todo el bitcoin será minado e introducido en el sistema.

26. P.McLeod, Taxing and regulating bitcoin:the government`s game of catch up, ComLaw Conspectus, vol 22, 2014, p.383

27. S.Nakamoto,cit.p.4

incentivo para su propio desarrollo. La tesis de *Bitcoin* enlazaría con la superación de la idea del trabajo gratuito, reconociendo a los cocreadores la participación a la que tienen derecho por su contribución a la creación de valor económico[28].

### 2.5.4. La obtención de Bitcoins

La convalidación y creación de criptomoneda no es el único modo de obtención de *Bitcoin.* Por un lado, el usuario puede cambiar moneda legal por una tarifa en cambio on line. El precio de *Bitcoin* depende de la oferta y la demanda y la volatilidad del precio es constante. Entre julio de 2014 y marzo de 2015 la oscilación fue de 600 dólares a 250 por unidad. Por otro, el usuario puede obtener *Bitcoin* a cambio de la compraventa de bienes y servicios.

El *Bitcoin* conseguido de alguno de los tres modos puede guardarse en el billetero del ordenador del usuario, previa descarga del software, o en un servicio de billetero online.

Por último, *Bitcoin* demuestra innegable atractivo para su uso ilegal, sea en actividad criminal de tráfico de drogas, juego, blanqueo de capitales.

La localización de la dirección o billetero digital como archivo en el ordenador, controlada por el usuario, es determinante a efectos de blanqueo de capitales, así como de su eventual sujeción a impuesto sobre la renta o el patrimonio. El territorio donde el billetero digital está operando es el sitio de la fuente tanto para la congelación, decomiso o confiscación de bienes derivados de tráfico ilícito, cuanto para su sometimiento al impuesto. El control efectivo delata al usuario, o lo que es, lo mismo, el poder de acceso, de cancelar, de negar el acceso, son las credenciales de su proximidad al archivo digital. No es el lugar donde está el ordenador; sino, la entrada y salida a la cuenta.

La "pérdida de localización", obra de la tecnología de *cloud computing,* obliga a centrarse en la individualización del sujeto, del usuario, de su *poder de disposición* del billetero digital. Pero, esto no parece incompatible con la idea de territorialidad,

28. T.Rosembuj, El impuesto digital, cit.p.38.

si se asume, no como reserva de soberanía, sino como fuente de renta o de riqueza, susceptible de confiscatoriedad y/o de impuesto.[29]

## **2.6.** LA PARTICIPACIÓN DE LA COMUNIDAD EN RED

El consenso es determinante en la configuración de la red de nodos de *Bitcoin.* La red es un elemento esencial, ya señalado en el trabajo original de *Nakamoto:* Las nuevas transacciones se comunican a todos los nodos; cada nodo incorpora nuevas transacciones para su block; cada nodo puede ser minero y si resuelve la prueba de trabajo la comunica a todos los demás que deben expresar su aceptación.[30] El autor predica una red robusta en su desestructurada simplicidad. "Los nodos trabajan todos al mismo tiempo con mínima coordinación."

La fortaleza de la red es la mejor garantía contra los ataques cibernéticos de fuera, la falsedad de las operaciones o el fraude de las transacciones. El anticuerpo de *Bitcoin* es la red de nodos vinculados entre sí a través de protocolos compartidos. La única vulnerabilidad, paradójicamente, es la concentración de poder en la minería –"miner pools"– que podrían manipular la creación de moneda en función de intereses económicos que no son los de la generalidad de la red de usuarios: "cuando un grupo de mineros controla más de la mitad del poder informático total usado para crear unidades de moneda virtual, el grupo está en posición de interferir con transacciones, por ejemplo, rechazando transacciones convalidadas por otros mineros."[31]

---

29. El poder de disposición es el concepto que "vincula cualquier dato a la persona o personas que obtienen el acceso único o colaborador y ejercen el derecho para alterar, borrar, suprimir o inutilizarlo así como el derecho a excluir otros de su uso." Cloud computing and cybercrime investigations: territoriality vs. The power of disposal?, J.Spoenle, Council of Europe Project on Cybercrime, 31-8-2010.

30. S.Nakamoto, 3,8.

31. European Banking Authority,EBA Opinion on "virtual currencies",4,july 2014, p.15.Algunos autores consideran que inclusive con menos del 50% podría verificarse el supuesto de control.:…la concentración de control sobre el poder informático en las manos de pocos grupos de mineros podría permitirles aliarse y arbitrariamente reescribir las reglas de protocolo o la historia de la transacción." Bitcoin, R.Böhme, N.Christin, B.Edelman, T.Moore, working paper 15-015 july 15,2014, Harvard Business School, p.

Pero, no solo: los riesgos de la criptografía informática digital son universales, globales, lícitos e ilícitos, morales e inmorales, y la moneda virtual los comparte. El mercado líquido es incontenible y lo difícil es acentuar la innovación tecnológica, los intereses menoscabados y la disciplina legal.

Dice *Tim May*: "El Estado intentará, por supuesto, retardar o detener la diseminación de esta tecnología, citando preocupaciones de seguridad nacional, el uso de esta tecnología por traficantes de drogas y evasores de impuestos y miedos de desintegración social. Cualquiera de estas preocupaciones serán válidas; la criptoanarquía permitirá la comercialización libre de secretos nacionales y la comercialización de materiales ilícitos y robados. Un mercado computarizado anónimo permitirá incluso el establecimiento de horribles mercados de asesinatos y extorsiones. Varios elementos criminales y extranjeros serán usuarios activos de la Crypto-Net. Pero esto no detendrá la extensión de la cripto anarquía. **La cripto anarquía, combinada con los mercados de información emergentes, creará un mercado líquido para cualquier material que pueda ponerse en palabras e imágenes." (**Manifiesto criptoanarquista, 1992).

## RECAPITULACIÓN

El dinero electrónico es un valor monetario almacenado en un formato electrónico, representado por un crédito exigible a su emisor, emitido por un valor igual a los fondos recibidos y convertible en dinero de curso legal al valor nominal. Es un medio de pago digital bajo la supervisión de la autoridad central y ejercido por la intermediación bancaria y financiera convencional. El *e-money* compite con la moneda virtual en ciertos de sus procedimientos y campos de actuación a través de internet, tales como *Pay Pal,* tarjetas de crédito, transferencias por teléfonos celulares u otros instrumentos; pero, es un bien digital dependiente de la autoridad central y de los intermediarios financieros. No es un bien digital autónomo y descentralizado.

Es ilusorio separar la idea de la moneda digital de la criptoanarquía. En efecto, la proyección que se pretende no se detiene en

el Estado ni en el sistema bancario o financiero, a los que aspira a poner en crisis. Esto explica, en parte, el exceso crítico vertido en su contra; al punto de opacar la innovación tecnológica que significa.

*Bitcoin* es una moneda digital cuya tecnología se apoya en la descentralización y en la ausencia de autoridad de dirección que no sea otra que sus protocolos de software. Por un lado, auspicia las transacciones en línea de persona a persona, sin terceros y, por otro, resuelve técnicamente el problema del *double spending:* cada una de las transacciones confirmadas consta en un registro público entre los usuarios( *blockchain).*[32]

*Bitcoin* es una criptomoneda digital, porque se funda en algoritmos matemáticos, que descifran las claves, pública y privada, para impedir el fraude o el abuso, y que son únicas para cada usuario. Cada usuario dispone de dos claves, una que es privada y secreta, y otra pública que se comparte en la red. la criptografía asegura la seguridad en la transacción y permite su despliegue en un block de la cadena. La transacción entre las partes es un mensaje cuyo contenido es la clave pública del receptor y la cuantía de moneda que envía. El mensaje está firmado por la clave privada del remitente.

Desde la perspectiva criptográfica digital hay servicios añadidos no financieros que, sin ser profetas, pueden superar inclusive las consecuencias de los propios servicios financieros. Me refiero, por ejemplo, al servicio digital notarial que puede calcular el algoritmo de un documento e insertarlo en la cadena de bloques, aunque no tenga valor económico en si mismo, siendo prueba de su existencia en un determinado momento, simplemente por su inserción en el registro público de la moneda virtual, lo cual indica que esto puede representar cualquier cosa o bien o contrato (*proof of existence).*

Los méritos técnicos de la fórmula no parecen cuestionables; pero, no ha dejado de notarse que, en ausencia de intermediarios

---

32. J.Brito,…"Las nuevas transacciones son comprobadas contra la cadena de bloques para asegurar que los mismos bitcoins no han sido previamente gastados, eliminando el problema del *double spending."* Global Markets Advisory Committee, 9-10-2014, CFTC.

y de autoridad central crece el protagonismo de la creación, adaptación, expansión, del código informático. Eso que *Lessig* define como *"the code is the law"* encaja en dudosa pretensión de los fundadores de autorregulación abierta y libre del sistema *Bitcoin.*

En la idea de Nakamoto, ninguno de los participantes de la red debe poseer una ventaja sobre otro. Pero, el desarrollo de monopolios mineros compromete la descentralización e igualdad entre las partes.[33]

El grupo ignorado de expertos en la formulación y reformulación algorítmica concentran un poder ilimitado en la red, sobre los participantes y en el conjunto y, aún más, la cooptación de todo el esquema por algún grupo particular de interés. Probablemente, éste es el talón de Aquiles.[34]

## 3. Bitcoin: de la criptomoneda digital a la moneda virtual

La primera aproximación de *Bitcoin* se construye alrededor de una versión de dinero electrónico análogo que debe permitir los pagos en línea de una a otra parte sin pasar por la institución financiera: un sistema electrónico de pago análogo al dinero efectivo apoyado en la seguridad ofrecida por la matemática criptográfica, en lugar de depositar la confianza en un tercero.[35]

Así, *Bitcoin* aspira a la doble función de moneda digital y red de pagos en línea distribuida, sin la intervención de intermediarios ni del respaldo de una autoridad monetaria central de gestión.

"La distribución del registro público y la base criptográfica de *Bitcoin* permite la transacción de valor entre pares sin confiar en las instituciones tradicionales. La emisión de moneda es deter-

33. M. Tarasiewicz, A.Newman, Cryptocurrencies as distributed community experiments, p.221, en D.LEE Huo Chuen, Handbook of Digital Currency,cit.

34. R.Grinberg, Bitcoin:an innovative alternative digital currency, Hastings Science and Technology Law Journal,4(1),2012: "Cualquier coalición puede tomar el control de la red de Bitcoin convenciendo a la mayoría de los usuarios de emplear una versión diferente del software", p.176.

35. S.Nakamoto, cit., p.1

minada por un algoritmo predecible… la operación no está asegurada por la norma legal sino por las leyes matemáticas de la criptografía".[36]

*Bitcoin* señala su configuración como moneda digital destinada a su uso como medio de pago, unidad de cuenta o una forma digital de depósito de valor mediante una red de ordenadores conectados a Internet "*peer-to-peer"* y almacenamiento de valor digital.[37]

Es una moneda no disciplinada por la ley ni bajo control o manipulación de gobiernos, bancos centrales o entidades financieras, cuyo formato de bien digital se basa en un modelo de distribución, en la que la responsabilidad está en la comunidad de usuarios dispuestos a su utilización y su emisión viene determinada por un algoritmo matemático preestablecido en manos de mineros encargados de convalidar la fe de las transacciones e incorporarlas como bloques en la cadena cronológica e histórica: una operación precede y otra sigue.[38]

El salto de moneda digital, de bien digital, a moneda virtual tiene que ver con su empleo: puede tratarse de una moneda despegada del mundo real, dedicada solo al mundo virtual, v.g. juegos virtuales o por su aplicación en reemplazo de la moneda legal, para la compra de bienes o servicios en la economía real.[39]

Desde la orilla de *Bitcoin,* no se evita, sin embargo, la referencia ora a la moneda digital o a la moneda digital global como señal diferenciadora de su plataforma de pagos electrónicos y transferencias de dinero, mediante software persona a persona y con la cobertura de la tecnología criptográfica y la firma digital.[40]

---

36. S.Patterson, How Bitcoin Works, october 2014, hillsdale.edu.

37. C.Viegas, J.Giglio Santamaría. Bitcoin: Un desafio para la ejecución de políticas de la Banca Central. Algunas consideraciones jurídicas frente al creciente fenómeno de las llamadas "criptomonedas", Agosto 2014, Banco Central de la República Argentina.

38. S.Gorjón, Divisas o monedas virtuales: el caso Bitcoin, enero 2014, Banco de España, Dirección General de Operaciones, Mercados y Sistemas de Pago.

39. Government Accountability Office, GAO, -13-156, Virtual Economies and Currencies: Additional IRS Guidance could reduce tax compliance risks, 2013.

40. J.Allaire, Testimony, november 18,2013, Committe on Homeland,…cit; P.Murck, the Bitcoin Foundation, Testimony, november 18, 2013, ibídem.

La denominación entre moneda digital y moneda virtual no es baladí. De una a otra hay una aproximación que no es meramente semántica. La moneda digital, el bien digital, pertenece al mundo **real** de la digitalización de la economía; mientras que la moneda virtual, puede o no, o, en cualquier caso, es fisiológicamente del mundo virtual, distante y distinto del mundo real. En verdad, la anfibología de la virtualidad está alimentada, hoy por hoy, de connotaciones negativas, como instrumento preferido de opacidad y tráfico ilícito de flujos de dinero. Quizá es conveniente apurar mejor el entredicho digital o virtual, porque de ese modo podría perfilarse mejor la idea de la compatibilidad y convivencia entre ambos conceptos.

Una moneda virtual es una unidad digital de cambio que no tiene el respaldo de la emisión legal de gobierno. [41]

La unidad digital sugiere un bien digital con sus características, que esconde otro bien distinto. El bien digital es un bien de información, intangible, basado en servicio de software, que transfiere electrónicamente cualquier tipo de elemento (datos) susceptible de almacenamiento en la memoria del ordenador, sin intervención humana, que no tiene equivalencia con el bien físico o material salvo por aproximación.

Cualquier dato que puede digitalizarse- codificarse como una cadena de bits- es información.[42]

El bien digital de información goza de los mismos atributos que los de los denominados bienes públicos: indivisible (*nonexcludable)*, de goce plural y colectivo (*nonrival)*, asumiendo restricciones propietarias a su disfrute, goce, consumo, pero, en un marco sumamente crítico y complejo por la prevalencia de la denominada "*abundancia digital*".[43]

La prédica de la tendencia de bien público del bien digital puede alcanzar dificultades máximas , siempre que el bien digital no sea solo un concentrado de información, sino, que, en contra

41. GAO, cit.p.3.
42. T.Rosembuj, cit., p.28.
43. V.Lehdonvirta, Edward Castronova, Virtual Economies.Design and Analysis.2014, Massachussets Technological Institute, p.42.

de la abundancia digital, provea un recurso escaso o cuyo disfrute, goce, por algunos impide o restringe el de los demás.

Hay otro mundo desprendido del digital, mundo virtual, presidido por la exclusión y el consumo rival. Por ejemplo, siguiendo a *Fairfield,* considere que alguien desea vender un bien digital –un *Bitcoin*–, una espada mágica en un juego, o un MP3 usado. El comprador pensará si el vendedor puede quedarse con una copia y revenderla o si el activo es escaso, cuanto le costaría al comprador conseguirlo por sus propios medios o si el bien digital deseado también es deseado por otros en el mercado.[44]

La consecuencia es que hay bienes digitales que concluyen en bienes que no son solo de información, sino de valor representativo, de propiedad singular, excluyente y de disfrute o goce basado en la escasez. Estos son los bienes virtuales: aun cuando son bienes digitales pueden fácilmente transformarse en bienes de exclusión y rivales: "derivan su valor no de la información sino de su función…"[45]

*Bitcoin* es criptomoneda digital transformada, por sus funciones de medio de pago, unidad de cuenta, depósito de valor, en moneda virtual. La paradoja es que se trata, en común de bien digital, pero con un acento insustituible en su proximidad **material** al uso y función que se le asigna. Un bien digital de coste cero, pero exclusivo y excluyente.[46]

El bien digital, bien intangible de información fundado en el servicio de software a través de Internet o red análoga, es la matriz de otros bienes digitales, que aumentan su alcance y desbordan su alcance sobre el mundo real.

Precisamente, el bien virtual siendo una aplicación del bien digital, asocia un perfil determinante de *in-materialidad: "*es sus-

---

44. Josh Fairfield,"Bitproperty", Washington and Lee University School of Law, paper No 2014-17, October 2, 2014,88 S.Cal.L.Rev (2015).

45. V.Lehdonvirta, E.Castronova, cit.p.42.; la idea original corresponde también a Josh Fairfield, Virtual Property, Boston University Law review, Vol 85,2005: "Si una persona es propietario y los controla, otros no pueden. Son persistentes. A diferencia del software en el ordenador no se van cuando uno lo apaga. Y están interconectados. Otras personas pueden interactuar con ellos.Esta clase de código yo lo llamo "propiedad virtual", p1050.

46. V.Lehdonvirta, E.Castronova, cit., p.44.

ceptible de percibirse en términos de materialidad, porque crea medios de producción."[47]

No es que el software deje su categoría de intangible; sino, que su potencia virtual supera la frontera de la fisicidad, incorporándose directamente a la materia que quiere expresar. No es una creación simbólica, sino que el bien virtual promueve la propiedad virtual de los objetos y funciones que disciplina, sin dejar de serlo.

La *in-materialidad* es discurso de una realidad que no se opone a la realidad material, sino que la ocupa con su propia tecnología .El bien virtual, desde el bien digital, ocupa la realidad física y material con los mismos efectos que el bien material que pretende complementar, sustituir, modificar. Es otra realidad, tan real como la material.[48]

La primera consecuencia, entonces, es que si de moneda hablamos, la moneda virtual es tanto como emplear el dinero efectivo de curso legal, sin que pueda tocarse. Se dice como si fuera, cuando sirve como dinero de verdad, creado y difundido desde el mundo virtual.

La referencia virtual a la moneda digital tiene como notas definitorias que carece de soporte, garantía o respaldo de ningún aparato público o de gobierno. No es, en suma, moneda legal. Pero, al mismo tiempo, reúne como atributo de la moneda sintética, que puede emplearse en la economía real fuera de los juegos del mundo virtual, sea como medio de pago, unidad de cuenta o depósito de valor.

El protocolo de la moneda virtual, el software que sirve a la interconexión y a la convalidación de las transacciones, pretende ser no solo lenguaje de comunicación de instrucciones, sino el modelo de creación de la moneda, sin intervención de otras autoridades, que las que personifican los participantes. Una moneda alternativa, desde el servicio de software, prescinde de la garantía pública para su emisión y circulación.

---

47. M.T.Schaefer, Bastard Culture: How Users Participation Transforms Cultural Production., p.64, 2009.

48. M.A.Jansen, Bitcoin: the polític "virtual" of an intangible material currency, International Journal of Community Currency Research,Vol 17(A) 8-18, 2013, p.14.

La criptomoneda digital es moneda virtual cuando entra en el territorio del mundo real, sin contar como moneda de circulación legal. El sistema de moneda virtual de flujo abierto comprende las representaciones digitales de valor que pueden usarse en la compra de bienes o servicios reales o servir para el cambio de moneda legal. La moneda criptodigital puede comportarse en mundos virtuales, pero, asimismo, trascender a los mundos reales, cosa que en verdad, no era lo propio de la finalidad originaria de la moneda virtual.

En verdad, la moneda virtual, en sentido estricto, es la que opera en un mundo virtual, v.g. *Farmville, Second Life, World of Warcraft*, o como ficta moneda en transacciones internas a las operaciones dentro de la empresa: *Starbucks, Amazon,* cosa que no es intrínseca a la criptomoneda y la digital, cuya vocación se convierte en virtual al desplegarse en el denominado mundo de la Tierra, sea en la compra venta de bienes o servicios, cambio con otras divisas legales, inversión financiera. Esa creación puramente digital, la de firmas digitales, trasciende desde su ámbito cerrado al espacio abierto de moneda equivalente, cualquiera que sea la definición que se pretenda.

*Bitcoin,* moneda virtual, por definición, aprecia en sus funciones rasgos de exclusión y de escasez, pero, debe tenerse en claro que por su naturaleza jurídica, antes que por sus funciones, la moneda *Bitcoin* es exclusiva y excluyente por razón de su fuente: las firmas digitales. En efecto, la distinción de la tecnología *Bitcoin* radica en su total sumisión a la criptografía asimétrica, a la clave pública y clave secreta que le acompaña; que ensalza un rasgo intrínseco a la persona, a su derecho esencial a la intimidad. No es por tanto, la exclusión y escasez económica la primera característica jurídica a destacar. Esta es la persona digital que se expresa a través de su firma personal digital exclusiva, excluyente y única.

## **3.1.** EL MUNDO VIRTUAL

El mundo virtual, hasta hace poco, es el mundo de los juegos, de la fantasía, de los mitos, de las sagas. Es el mundo del espacio de juego, que tiene como barrera el mundo real, el mundo de la

Tierra. La mejor teoría lo define como un círculo mágico de libertad, erigido en torno a las propias reglas internas del juego, donde es ilegal lo que el sistema de juego excluye o no permite, a partir de la propia licencia de uso del software que aplica, que puede o no coincidir con la conducta ilegal que prescribe la norma jurídica de la realidad real. En el mundo sintético uno puede ser un ladrón sin pagar con la cárcel o un especulador codicioso, sin la obligación de pagar impuestos: "en estos mundos tu puedes ser cualquier cosa que quieres ser".[49]

Las características principales del mundo virtual del juego son: interactividad, representación física del jugador, persistencia del juego que continua aunque el jugador lo use o no.[50]

El mundo virtual es un mundo online, interactivo en el que los jugadores crean una representación física, propia (avatar), que cohabita e interactúa con los otros jugadores.[51]

El verdadero mundo virtual es un espacio sintético de juego, impermeable al mundo real (*closed worlds).*La actividad de los jugadores está sometida de pleno a los términos de acuerdo del usuario con la licencia de software (*World of Warcraft).*

Pero, a la inversa, hay mundos virtuales (*open worlds),* prolongaciones de la vida real, en las que se ensombrece la separación entre la economía sintética y la economía real, *v.g. Second Life* .La línea de separación se establece cuando el proveedor del mundo virtual permite la contaminación entre moneda real y activos virtuales.

"…el mundo virtual se convierte en un paraíso fiscal en lugar de un espacio de juego si la propiedad virtual puede ser comprada y vendida por moneda real."[52]

---

49. E.Castronova, The right to play, 8, december, 2004, ssrn.com 733486.

50. E.Castronova, Virtual worlds: a first-hand account of market and society on the cyberian frontier, december, 2001, Center for Economic Studies & Ifo Institute for Economic Research, working paper no. 618.

51. Yen-Shyang Tseng, Governing Virtual Worlds: Interration 2.0, Washington University Journal of Law & Policy, 2011, Vol 35.

52. E.Castronova, The right to play, cit.: "Si los jugadores pueden comprar y vender regularmente activos del mundo sintético por dólares reales, el mundo sintético no es más, claramente distinto del mundo económico de fuera", p.204.

El mundo cerrado del juego es un ámbito de libertad estructurado y compartido por el creador y los jugadores, sometido a sus reglas desde el inicio. El mundo abierto invita a la coexistencia con el mundo real y, por tanto, sus reglas deben someterse a las normas jurídicas generales que gobiernan cualquier actividad humana.

El juego virtual en sí mismo y el esquema virtual en el que influye la búsqueda de beneficios o ganancias de los jugadores a través del comercio, apenas limitada por las reglas fijadas.[53]

La primera restricción surge desde los que niegan la autonomía (la soberanía del reino de la fantasía), partiendo de la base que todo, inclusive lo virtual está expuesto a disciplina del mundo real.

El mundo real es bidireccional: solo respeta el juego por el juego. Aquí funciona plenamente el derecho al juego en toda su dimensión, con exclusión de cualquier interferencia de la fantasía creada para la pura diversión.

Nos alejamos del círculo mágico, en el momento que con el consenso de los jugadores, desde el mundo virtual se produce la aceptación de modos y actitudes propias del mundo real: comprar, vender, alquilar, invertir o si se usan unidades de intercambio monetario que lo facilitan, por otra, el mundo real prolonga sus modos y actitudes en el mundo virtual, facilitando la actividad económica, el comercio, la ganancia

"Es imposible separar los mundos virtuales de la economía del mundo real: los individuos que entran en los mundos virtuales son reales, sus acciones dentro de esos mundos son reales y los efectos de esas acciones sobre otras personas son reales." [54]

Quizá con la matización oportuna relativa a cuando se sustituye el placer por el placer con el comercio o la voluntad de ganar (dinero).

---

53. Esto también se conoce como "juegos estructurados" y juegos "desestructurados", B.T.Camp, The Play`s the Thing: A theory of taxing virtual worlds, 59 Hastings L.J., 4,2007.

54. J.A.T.Fairfield, The Magic Circle, 14 Vand.J.Ent.&Tech L 545, 2012.

## **3.2.** LA CRIPTOGRAFÍA COMO FUENTE DE LA MONEDA VIRTUAL

La firma digital se basa en la clave pública criptográfica, una tecnología estrictamente matemática, que facilita la creación única de un par de claves, pública y privada: cadenas aleatorias de caracteres alfanuméricos que se corresponden entre sí. Cuando el usuario emplea su clave pública puede firmar los mensajes de datos con su clave privada y otros usuarios están en condiciones de verificar que la firma digital es auténtica, comprobando que se corresponde con la clave pública. La persona envía un mensaje de datos, cualquiera que sea su contenido, en este caso, moneda virtual, y previamente entrega su clave pública al receptor. La persona firma digitalmente el mensaje con su clave privada y lo envía. El receptor comprueba la firma digital con la clave pública. Solo el titular de la clave privada tiene la aptitud para originar una firma que pueda verificarse por la clave pública.

La transacción autorizada por la clave privada se transmite a toda la red de usuarios y es irrevocable. La información deviene pública, parte de la cadena de bloques, previa su convalidación por los mineros, y pasa a formar parte de la historia de las operaciones universales registradas de *Bitcoin.*

La transacción, dice *Patterson, no es asegurada por la norma jurídica sino por las leyes matemáticas en la criptografía.* Naturalmente, emergen nuevos problemas de calificación jurídica, porque el protocolo *Bitcoin* asume las funciones del Estado y los intermediarios financieros, convirtiéndose en el nuevo intermediario software a través del cual los usuarios se relacionan. La criptografía como fuente de derechos y obligaciones, autónoma de los legisladores convencionales o específicos, porque se desarrolla en espacios no regulados; problema que va más allá de la moneda virtual puesto que implica cualquier documento necesitado de firmas digitales en el tráfico jurídico mercantil o civil, sea o no monetario.

## RECAPITULACIÓN.

La moneda virtual es el estado próximo y sucesivo de la criptomoneda digital. Es la integración del mundo digital y sinté-

tico en la economía real y en las instituciones que la organizan. La inmersión en la Tierra, siguiendo la metáfora, obliga a establecer que la virtualidad, en su propia garantía, debe asimilarse a la moneda real, para su supervivencia.

La innovación tecnológica principal es la descentralización y la competencia en el mercado financiero con la intermediación bancaria. Pero, "no hay diferencia fundamental entre la "moneda virtual" y la "moneda real"."[55] La diferencia es de grado y, probablemente, vinculada al área de aplicación geográfica de cada una de ellas.

No es *Bitcoin,* sino el modelo criptográfico digital que crea un protocolo innovador en el reino absoluto de la moneda legal de curso forzoso. No es *Bitcoin*, sino la idea que del abuso de la intermediación bancaria y de tarjetas de crédito, resultan causas de exclusión social y restricciones al consumo y a la pequeña y mediana empresa. Esas contribuciones, convenientemente ordenadas no conducen a la mano invisible que niega la existencia de instituciones monetarias centrales y la libre actuación del mercado ni, tanto menos, a la competencia entre monedas(legales y virtuales). Pero, es innegable que la comunidad en red, por insignificante que fuere, incorpora un elemento olvidado por la moneda legal que es digno de proteger :la fuerza de la comunidad para afrontar las falencias derivadas de la gestión de la moneda por el sistema financiero y bancario y la tutela de la información de cada persona, o sea, la protección de sus datos personales, como valor social, en particular el exclusivo derecho a la intimidad.

Lo que parece necesario recoger es que la moneda legal y la moneda alternativa, ambas, pueden aprovechar sus sinergias, cubriendo aspectos sociales, ora maltratados por los intermediarios bancarios ora atrasados en la convalidación digital de los medios de pago, de la unidad de cuenta, del depósito de valor. El **oro es oro**, sea fiduciario o consentido, aunque no sea verdadero oro.

La fuente matemática de valor, la criptografía de las firmas digitales, individualiza la moneda virtual y su tránsito en la comunidad de usuarios. Es la abstracción digital al infinito. El intangible

55. V.Lehdonvirta, E.Castronova, op.cit., p.191.

digital al cubo. Es imposible interpretar el fenómeno *Bitcoin* sin la referencia directa a la información contenida en las firmas digitales que consienten, a la vez, establecer la certeza del envío del mensaje al destinatario y la opción del ordenante en defensa de su intimidad personal. A la vez, la específica regulación matemática sustituye la ley y propone interrogantes sobre su eficacia desprendida de cualquier otra restricción que no sea la voluntad de las partes intervinientes. Probablemente, la reacción institucional contra la moneda virtual llevará a plantear, de algún modo, mecanismos de supervisión que, respetando la neutralidad tecnológica, pueden advertir sobre los riesgos sistémicos antes que se produzcan, que es lo que se propone desarrollar el Banco de Inglaterra.

## 4. La moneda virtual en los EEUU. Conceptos

*Bitcoin* es calificada como una moneda virtual descentralizada porque no hay una autoridad administrativa central: la convalidación y certificación de las transacciones se realizan por los usuarios del sistema y no requiere una tercera parte para las actividades de intermediación y que descansa en protocolos de software criptográfico.[56] A la inversa, la moneda virtual es centralizada cuando una autoridad administrativa única emite la moneda y tiene la potestad para retirarla de la circulación; establecer normas para el uso y conservación de un registro central de pagos.

La criptomoneda digital forma parte de una categoría más amplia como una clase de moneda virtual cuyas características enfatizan la descentralización operativa y la ausencia de rango de moneda legal.

La *Financial Crimes Enforcement Network (FinCEN)* del *US Department of the Treasury* conviene en calificar la moneda virtual como un medio de cambio que opera como una moneda en

56. Government Accountability Office,GAO 14-496,Virtual Currencies.Emerging regulatory, Law Enforcement,and Consumer Protection Challenges, may 2014; US Senate Committee on Homeland Security and Governmental Affairs, november 18, 2013,"Beyond Silk Road: Potential risks, threats, and promises of virtual currencies, Jennifer Shasky Calvery, Testimony, p.3.

algunos ambientes pero que no tiene atributos de moneda real, en particular, no es moneda legal (*legal tender)* en ninguna jurisdicción. Pero una moneda virtual que se distinga como convertible puede cambiarse por moneda real, sea por equivalencia de valor o en substitución de la moneda real.[57]

El *US Department of Justice* adopta un concepto similar de moneda virtual: un medio de intercambio circulado en la red, típicamente Internet, que no está respaldada por un gobierno, que puede ser centralizado o descentralizado, como *Bitcoin.*[58]

La *Conference of State Bank Supervisors* define la moneda virtual como un medio electrónico de cambio que no tiene los atributos de las monedas reales e incluye las criptomonedas, como *Bitcoin*, que no son moneda de curso legal y no son emitidas o respaldadas por ningún banco central o autoridad gubernamental. "Las monedas virtuales tienen propósitos legítimos y pueden comprarse, venderse e intercambiarse con otros tipos de monedas virtuales o monedas reales, como el dólar…"[59]

La primera de las definiciones legales de moneda virtual puede encontrarse en un proyecto de ley en el Congreso de los EEUU que no tuvo continuidad.

"La moneda virtual es una representación de valor que funciona como un medio de cambio, una unidad de cuenta y/o depósito de valor. "[60]

La *BitLicense de New York* entiende como moneda virtual cualquier tipo de *unidad digital* que es utilizada como medio de cambio o una forma de depósito de valor digital o que está incorporada a un sistema tecnológico de pago, centralizada o descentralizada, de existencia pura en el ordenador o susceptible de manufactura.[61]

---

57. J.Shasky, cit.

58. M.Raman, Assistant Attorney General Criminal Division,US Department of Justice,Testimony,november 18,2013, Committee on Homeland Security and Governmental Affairs US Senate,cit.

59. Conference of State Bank Supervisors, North American Securities Administrators Association, Model State Consumer and Investor Guidance on Virtual Currency, april 23,2014.

60. Virtual Currency Tax Reform Act de may 7,2014, HR 4602.

61. ver.Punto 2.3.3.

La moneda virtual, entonces, que no es moneda legal, compendia los perfiles de la moneda. Puede servir como medio de cambio entre los que la aceptan; como unidad de cuenta y como eventual depósito de valor. Y ello sin que cuente con el respaldo legal público que obligue a su aceptación.[62]Pero, no solo, es una representación digital, una cadena de bits y bytes, portadora de valor.

## 4.1. LAS ADVERTENCIAS DE ORGANIZACIONES PÚBLICAS Y PRIVADAS SOBRE LA MONEDA VIRTUAL

La configuración legal de moneda virtual aparece por primera vez en el ordenamiento jurídico americano, sea como opinión, primero en organismos públicos y privados de supervisión u orientación e inmediatamente con fuerza legal en algunos de los Estados federales de los EEUU. En el primer caso, teniendo en vista los riesgos que supone para el mercado, el Estado y los consumidores y en el segundo, tratando de compatibilizar la emergencia de la nueva tecnología de pagos con los riesgos implícitos de la incertidumbre que su propia evolución crea.

### 4.1.1. Financial Industry Regulatory Authority. FINRA

La *FINRA* es una organización independiente, que no pertenece a la Administración, pero que respalda, con su crédito moral, la idea de un mercado equitativo asegurando la educación de los consumidores e inversores. Sus primeros consejos y advertencias relatan de una profunda desconfianza sobre los riesgos de especulación y de fraude que implica *Bitcoin.*[63]

Primero, la moneda digital carece de respaldo y fuerza legal

Segundo, las plataformas virtuales y los billeteros digitales pueden ser objeto de piratería cibernética.

---

62. S.Lo, J.Ch. Wang, Bitcoin as money,Current Policy Perspectives, Federal Reserve Bank of Boston, no.14-4,september 4,2014,…"La unidad de la red es referida como bitcoin, que es generalmente considerada como la más conocida moneda virtual(electrónica, digital) a la fecha.", p.2.

63.Financial Industry Regulatory Authority, Bitcoin: more than a bit risky, may 7, 2014.

Tercero, las operaciones con moneda digital pueden estar sujetas a fraude y robo.

Cuarto, los billeteros digitales no tienen garantía como los depósitos bancarios.

Quinto, los pagos son irreversibles y el reembolso solo depende de la voluntad del comerciante o cobrador para hacerlo.

Sexto, el anonimato expone a las actividades ilegales, sea tráfico de drogas, de seres humanos, blanqueo de dinero.

Séptimo, la volatilidad de la moneda virtual impide la predictibilidad sobre su cotización.

Octavo, la ausencia de transparencia propone un estímulo para la estafa.

#### 4.1.2. Conference of State Banks Supervisors. CSBS

La CSBS es la organización nacional que reúne a los administradores bancarios de todos los estados. Desde 2014 se preocupa de la disciplina que debería acompañar a la moneda virtual.[64]

La moneda virtual es la representación digital de valor que puede servir de medio de pago, unidad de cuenta y o depósito de valor. Algunas de sus actividades despiertan preocupación en las áreas de la protección del consumidor, estabilidad de mercado y conformidad a la aplicación de ley que impida actuaciones ilícitas fuera de la ley. Los mecanismos son la licencia y la supervisión.

Las actividades cubiertas son las relativas a la transmisión; intercambio de moneda real y moneda virtual o entre moneda virtual y otra virtual; servicios que facilita a terceros el cambio, depósito o transmisión de moneda virtual, v.g. billeteros, kioscos, comerciantes-compradores y procesos de pagos. Quedaría fuera de la licencia y supervisión la pura actividad de compraventa mercantil ente comerciante y usuario o los registros públicos distribuidos criptográficos de que no tienen carácter financiero.

---

64. CSBS Policy on State Virtual Currency Regulation, december 14,2014.Para llevar adelante sus objetivos se ofrece a discusión pública un modelo de regímenes reguladores de moneda virtual, que seguramente inspiró la *BitLicense* de New York.

### 4.1.3. Consumer Financial Protection Bureau. CFPB.

El CFPB es un organismo nacido de la Ley *Dodd-Frank* de reforma de Wall Street y protección al consumidor, con el propósito de ofrecer consejo y recomendaciones sobre las prácticas financieras que puedan afectar al consumidor.

En agosto de 2014 advierte sobre los riesgos que la moneda virtual supone al consumidor [65]

Los riesgos se sitúan en cuatro áreas: piratas informáticos, que pueden romper cualquier sistema de seguridad; escasa protección de los proveedores o intermediarios; coste, que pueden ser superiores al uso de cartas de crédito o dinero efectivo; estafas.

Los hackers asolan la moneda virtual y pueden quebrar sus sistemas de seguridad en cualquier momento. Si cualquiera accede al ordenador del usuario puede quedarse con las claves privadas y robar toda su moneda virtual.

Nada asegura que su intermediario o proveedor es solvente y puede asegurar el pago o cobro que se supone.

Los costes de la transacción pueden ser más elevados que los que se dicen.

Las monedas virtuales aún son experimentales y su núcleo duro es, como en *Bitcoin, la Cadena de Bloques,* cuya conservación depende de redes inidentificables dispersas en todo el mundo. Es posible que el usuario tenga la convicción que haya finalizado una transacción que aún no refleja su constancia.

Finalmente, la criminalidad organizada practica nuevas versiones de antiguos fraudes. En especial, esquemas *Ponzi*, el pago de altísimos retornos a los inversores actuales con fondos derivados de los nuevos que entran.

### 4.1.4. Securities and Exchange Commission. SEC.U.S.

La *SEC,* la organización del gobierno de supervisión del mercado de valores, mercados financieros, opciones y mercados

65. CFPB, Risks to consumers posed by virtual currencies, August, 2014.

financieros electrónicos, manifiesta su preocupación por el uso creciente de monedas virtuales que sirven para engañar a los inversores en los que estas monedas sirven para el fraude. Esto también puede implicar a las plataformas u ofertas no registradas, al amparo del anonimato y la ausencia de requisitos de licencia. [66] Está en la vanguardia del control y la denuncia de los abusos o prácticas ilícitas en el ámbito de la moneda virtual.

En 2014 la *SEC* denunció un esquema *Ponzi en Texas*, publicitada como una "oportunidad de inversión" en *Bitcoin.*[67]A los inversores se les prometía un 7% de interés semanal, que serían invertidos en fondos de *Bitcoin,* mediante operaciones de arbitraje financiero. Los primeros inversores fueron inicialmente retribuidos a costa de los que venían después*,* (*SEC vs. Shavers*). El caso es particularmente interesante, porque el Tribunal sostuvo que la inversión en *Bitcoin* puede calificarse como "contratos de inversión" y "títulos valores" bajo la ley vigente. Por tanto, la moneda virtual puede ser instrumento financiero en sentido estricto: es una inversión en dinero; que se debe a la expectativa de beneficios que sugiere; en una empresa común; que depende solamente de los esfuerzos de un promotor o un tercero.[68] En este supuesto, el tribunal constata la existencia de un esquema *Ponzi,* y ordena una ejecución sobre el responsable de más de 40 millones de dólares. La importancia de la sentencia reside en que la calificación de *Bitcoin* como título valor es una previa definición jurídica relevante.[69]

El Tribunal considera que *Bitcoin* es una moneda, cuya única restricción es que su empleo se produce allí donde otros la aceptan como tal.[70]

La SEC ya había anticipado que al margen de analizar si las monedas virtuales subyacentes son un título en sí mismos; toda vez que generan intereses para las entidades propietarias o que

66. SEC, Investor Alert. Ponzi Schemes Using Virtual Currencies, Investor Alert, (SEC Pub no 153(7/13), 23 july 2013.

67. SEC v Shavers 2013 US Dist LEXIS 11018(E.D. Texas, august 6 2013.

68. SEC v WJ Howey Co 328 US 293(1946).

69. J.Lee, A.Long, M.McRae, J.Steiner, S.Gosnell Handler, Business Law International Vol 16, 1, january 2015. Bitcoin Basics: a Primer on Virtual Currencies

70. B.Akins, J.Chapman, J.Gordon, G.Gwinnett College School of Business, A whole new world: income tax considerations of the bitcoin economy, Pittsburgh Tax review, 2015.

ofrecen beneficios fundados en dichos activos "probablemente serán títulos valores y por tanto sujetas a nuestra regulación".[71]

Ello no obsta para que la SEC, contemporáneamente, al caso *Shavers* publicara otra nueva advertencia a los inversores sobre los riesgos de inversión que implican las monedas virtuales. Sea por estafa, dificultades de reembolso, ausencia de tutela legal, volatilidad.[72]

#### 4.1.5. North American Securities Administrators Association. NASAA

La *NASAA* advierte sobre los riesgos vinculados a la moneda virtual. Por un lado, mínima regulación, falta de tutela de los depósitos virtuales, volatilidad de los precios. Por otra, los intermediarios están desregulados y son susceptibles de fraude y robo. Asimismo, los inversores deben tener la máxima precaución ante los ataques cibernéticos y el robo de sus billeteros digitales.

"Las monedas virtuales son una tendencia emergente en los pagos por bienes y servicios. Bitcoin, quizá la moneda virtual más popular, tuvo un precio de 10 dólares por unidad al inicio del 2013, y llegó 1200 dólares por unidad al final. El rápido aumento provocó un interés en el mercado de ofertas de títulos vinculados las monedas digitales. Desafortunadamente, promotores inescrupulosos intentan capitalizar esta popularidad ofreciendo ilegalmente títulos vinculados a las monedas digitales. Aún las ofertas legítimas pueden presentar considerables riesgos al inversor incluyendo riesgos relativos a la volatilidad y demanda por las unidades, el anonimato asociado con el uso de ciertas monedas digitales, y los amenazas que suponen los hackers que usan software malicioso para comprometer la red de seguridad de los sistemas.".[73]

Sin embargo, a destacar, es que esta organización califica positivamente determinadas inversiones en monedas virtuales, que la aproximan al estado de moneda, aun sin respaldo legal.

---

71. M.J.White, Chair SEC, 30, August, 2013, carta al Committee on Homeland Security and Governmental Affairs.

72. SEC, Bitcoin and other virtual currenciy-Related investments, Investor Alert, 7, may, 2014.

73. NASSA, North American Securities Administrators Association, New Products in classic schemes identified as top investors threats, november 12, 2014.

La moneda virtual puede usarse en el comercio como inversión del mismo modo que el oro o cualquier otra materia prima(*commodities);* las monedas virtuales, como las materias primas o mercancías, o acciones, puede constituir un fondo de valor cotizable en los mercados bursátiles; la moneda virtual puede servir de activo subyacente de un derivado(sean, futuros, swaps, bonos convertibles).Estas indicaciones apuntan a una equivalencia, pese a las obvias diferencias, entre la moneda real y la moneda virtual, entre la moneda legal y la criptomoneda digital, a la sazón moneda virtual.[74]

## RECAPITULACIÓN

El escepticismo o la desconfianza es la posición más o menos unánime de las Administraciones Públicas y agencias vinculadas. El énfasis en los riesgos no es exagerado, pero, lo que sí lo es el rechazo extremo ante una experiencia tecnológica con rasgos innovadores en la orientación de la moneda. Las críticas se centran en la ausencia de fuerza legal de *Bitcoin,* que se funda en la aceptación voluntaria como medio de pago; en la ausencia de garantías que aseguren los depósitos en las billeteras digitales y en la facilidad que el anonimato(aun relativo) proporciona al tráfico de fondos ilícitos, sean drogas, contrabando, blanqueo de capitales o evasión fiscal. Menos convincente es la acusación sobre la susceptible piratería en las plataformas o en las billeteras digitales de *Bitcoin o* el peligro de fraude o robo por los intermediarios de moneda virtual. Es cierto que la moneda virtual, aun sin definición legal precisa, auspicia más actividad de riesgo que la moneda de curso legal. No obstante, hay que recordar, que, si algo trajo la crisis financiera y bancaria de 2008 es que la estafa, engaño, robo, blanqueo, evasión fiscal, no tiene necesariamente como protagonista a la moneda virtual; sino, al contrario al sistema financiero y bancario gestor de la moneda legal.

La moneda legal estuvo lejos de impedir los reproches, públicos y notorios, que hoy se dirigen a la moneda virtual. No fue

74. NASSA, North American Securities Administrators Association, What`s in your e-Wallet?, april 2014

menos perjudicial para el ciudadano el riesgo sistémico provocado por el sistema financiero regular, que el potencial apuntado contra la moneda virtual, aun sin regular. Tampoco es desatinado pensar que fue el fracaso de las grandes entidades bancarias lo que impulsa, curiosamente desde 2008, el camino de las monedas alternativas.

Sin perjuicio de lo dicho, también cabe apuntar que algunas de las agencias preservan un tono de justa prudencia sobre la caracterización de *Bitcoin*. Así, afloran problemas de calificación de compleja resolución jurídica, en este momento, tales como, la aplicación de la disciplina de títulos valores, o la naturaleza de mercancía(intangible) de la moneda virtual, generadora de derivados financieros.

La inversión en fondos *Bitcoin* podría ser asimilada a cualquier otra en títulos valores con el encuadramiento legal que esto implica o la volatilidad ínsita de la moneda virtual podría consentir la demanda de un mercado de derivados ,que pueden permitir limitar los riesgos de la inversión contra las fluctuaciones.

## 5. La disciplina legal

### 5.1. FINANCIAL CRIMES ENFORCEMENT NETWORK. FINCEN. TREASURY. EL BLANQUEO DE CAPITALES

El *FinCEN* es un organismo del Tesoro dedicado a la observación y dirección de la integridad y transparencia del sistema financiero americano, en particular, impedir el blanqueo de capitales y la financiación del terrorismo.

Desde julio de 2011 el organismo incorpora las monedas virtuales convertibles a los servicios monetarios empresariales, a los servicios de transferencia de monedas. En marzo de 2013[75] se establecen guías de interpretación sobre el ámbito de la intervención del *FinCEN*. Por una parte, alcanza a las personas que crean, obtienen, distribuyen, intercambian, aceptan o transmiten monedas

75. FinCEN Application of FinCEN`s regulations to persons administering, exchanging or using virtual currencies, FIN-2013-G001, march 18 2013.

virtuales. Los administradores o cambistas deben registrarse ante el *FinCEN* cumplir con determinados requisitos de conservación contable e información.

Las medidas están dirigidas solo a los que se dedican a servicios de transferencia de moneda: cualquiera que acepte y transfiera una moneda virtual convertible o compra o vende moneda virtual convertible

El cambista es la persona empeñada en el cambio de moneda virtual por moneda real, fondos u otras monedas virtuales. El administrador es la persona empeñada en la emisión de moneda virtual y que tiene la potestad de retirarla de la circulación.

Probablemente el efecto más importante es la calificación de la actividad mercantil en *Bitcoins* servicio monetario puesto que abre la puerta a la licencia Estatal para su ejercicio, desde que su objeto necesariamente es la transmisión de moneda, cuyo primer exponente es la *BitLicense* Nueva York.

## **5.2.** CALIFORNIA. LA MONEDA ALTERNATIVA

El Código de Sociedades de California prohibía a las sociedades o personas físicas la emisión o circulación de cualquier otra moneda que no fuera moneda legal en los Estados Unidos (Section 107).

La Ley AP-129, de junio 2014, deroga la prohibición, aceptando la emisión y circulación de moneda alternativa a la legal y oficial (*fiat currency)* dentro del Estado.[76]

De modo que decae el monopolio público de la obligación exclusiva y única de aceptación de una moneda legal para el pago de las deudas y se declara que la emisión y circulación de moneda puede basarse en la voluntad y consenso de las partes, de los participantes, de los miembros de una comunidad o de un barrio. Esto es lo que la ley de California, denomina monedas alternativas, que se expanden más allá de los pagos en dinero legal o por carta de crédito.

76. California Assembly Bill no.129 Chapter 74, june 28 2014.

La moneda alternativa es una categoría que reúne distintas variedades de moneda: puntos, cupones, la moneda digital, moneda virtual u otros objetos de valor monetario cuyo uso no viola la ley en la compra de bienes o servicios o transferencia de pagos.[77]

Primero, los modelos de puntos que compensan a los consumidores en ciertas empresas, v,g, el gasto de una cierta cantidad de dólares y que, a la postre, funciona como una moneda.

Segundo, asimismo, comprendería las denominadas "comunidades de moneda", que consisten en la creación por miembros de una comunidad junto con los comerciantes de una asociación para aceptar una moneda alternativa, v,g, para estimular el pequeño comercio de las ciudades o aumentar la cohesión social del barrio o, inclusive ,a modo de protesta política. Son clubs de permuta, cambio, de bienes o servicios, cuantificables en una moneda representativa.

Tercero, la moneda digital o criptomoneda, entre las que destacan a *Bitcoin,* pero no solo: *Litecoin ,Ripple ,Peercoin ,Namecoin, Dogecoin, Primecoin*. O moneda de empresa: *Amazon coin; Starbuck star.*

La emisión y circulación de otras monedas, fundado en la voluntad de los participantes, supone el reconocimiento amplio de moneda, como medio de pago, unidad de cuenta, depósito de valor, a cualquier experiencia solvente o tecnológicamente innovadora, aun cuando, carezca del respaldo de aceptación legal obligada. Esto no supone una alternativa desregulada, sino, al contrario, abre el camino para la disciplina del sector, sea en el ámbito mercantil, financiero, fiscal, penal, que pueda establecer los criterios generales de transparencia, protección de consumidores, evitación de tráfico ilícito de flujos económicos y evasión fiscal. Todos estos elementos estuvieron presentes en la Asamblea de California, pero, pese a las dificultades actuales que esto supone, avanzaron, acompasándose a la realidad de monedas alternativas que se difunden y se aceptan voluntariamente entre los ciudadanos y cabe reconocer.

77.M.Farouk Analysis, California Assembly Third Reading, january 23,2014.

## **5.3.** NUEVA YORK. LA BIT LICENSE

El Departamento de Servicios Financieros del Estado de Nueva York está a punto de aprobar la **BitLicense**, reguladora de las empresas dedicadas a l comercio de monedas virtuales. La disciplina contiene reglas de protección del consumidor, de antiblanqueo de dinero, de ciberseguridad.y de conservación del capital suficiente para su responsabilidad.[78]

El significado de moneda virtual es cualquier tipo de *unidad digital* que es utilizada como medio de cambio o una forma de depósito de valor digital o que está incorporada a un sistema tecnológico de pago. La moneda virtual puede configurarse en sentido amplio para incluir unidades digitales de cambio que o tienen un depositario o administrador centralizado o son descentralizadas y carecen de depositario o administrador centralizado y que pueden crearse por ordenador o manufactura.

La moneda virtual no incluye las *unidades digitales* que son usadas exclusivamente dentro de plataformas de juego en línea, sin mercado o aplicables fuera de dichas plataformas de juego. Tampoco, comprende unidades digitales que son utilizadas exclusivamente por el usuario como parte de programas de recompensas y se aplican solamente como pago por las compras con el emisor u otros comerciantes, pero que nunca serán convertibles o reembolsables por moneda legal (*fiat currency)*.

Quedan fuera de la normativa determinadas actividades. Por una parte, el desarrollo de software para el uso personal del consumidor. Por otro los programas de recompensa o regalos denominados en moneda legal .Tampoco quedan incluidas las actividades de los "mineros" en el sistema *Bitcoin* y de las compras por personas físicas como inversión. El eje de la regulación es la intermediación financiera de moneda virtual.[79]

---

78. New York State.Department of Financial Services proposed New York codes, rules, regulations. Title 23.Department of Financial Services.Chapter I.Regulations of the Superintendent of Financial Services. Part 200 Virtual Currencies.proposal, july, 23, 2014.

79. Superintendent Lawsky`s remarks at the Bipartisan Policy Center on Regulating Virtual Currencies and Payments Technology, Washington DC, December18, 2014.

La *BitLicense* perfila un marco jurídico de moneda virtual centrado en la unidad digital. No hay moneda virtual sin núcleo digital. Esto viene a significar que se entiende por virtual, la digitalización de las funciones de la moneda ( bien digital), sea como medio de pago, depósito, o comercio electrónico .Es otro tipo de moneda que carece de respaldo público y no es ni. está vinculada a ninguna *fiat currency* (dólar, euro, yen).

El eje de la disciplina propuesta, por ser una experiencia primera y contenida, está destinada a tener un efecto determinante en el tratamiento de la moneda virtual.[80]

El sujeto de la disciplina es la actividad de empresa dedicada a la moneda virtual y tiene por objeto someterla a licencia para el dicho ejercicio, cumpliendo con las normas y programas relativos a antiblanqueo, ciberseguridad, conservación del capital y protección del consumidor.

Las actividades reseñadas sometidas a licencia son:

- Recepción y transmisión de moneda virtual.
- Depósito, tenencia o custodia o control de moneda virtual por cuenta de otros.
- Compra y venta de moneda virtual para su consumo de empresa.
- Venta al detalle de servicios de cambio, incluyendo la de moneda legal por moneda virtual, o moneda virtual por moneda legal, o cambio una moneda virtual por otra.
- Control, administración o emisión de moneda virtual.

Específicamente, vale la pena mencionar las disposiciones de protección al consumidor, por su compromiso y claridad. (*Section 200.19).*

La disciplina de New York es sensible a la preocupación expuesta por otras entidades públicas reguladoras[81].El riesgo se basa en la ausencia de obligación de aceptación de la moneda

80. Gibson Dunn, BitLicense 2.0: New York moves closer to comprehensive virtual currency regulation, february 15, 2015.

81. Consumer Financial Protection Bureau, Risks to consumer, cit.

digital como forma de pago; la falta de garantía de los depósitos y la irreversibilidad de los pagos; la fragilidad ante los ataques cibernéticos, el fraude y robo de la moneda; la volatilidad de los cambios; el riesgo de participar sin información en tráfico ilícito de fondos.

La empresa licenciada debe informar al consumidor de los riesgos materiales que asume. Por un lado, que la moneda virtual no es moneda legal, ni goza de particular tutela o protección pública; los cambios legales o las actuaciones públicas pueden afectar el uso, transmisión, cambio y valor de la moneda virtual; puede existir un riesgo incrementado de fraude o ciber ataque; cualquier dificultad tecnológica puede impedir el acceso del usuario a sus cuentas. Por otro, dirigido a los consumidores de monedas *Bitcoin* o similares, que las transacciones son irreversibles y las pérdidas por fraude o accidente no son recuperables; el registro de la operación en la Cadena de Bloques puede no coincidir temporalmente con el momento en que el usuario inicia la transacción; el valor de la moneda virtual derivado del cambio entre moneda legal y moneda virtual por la voluntad de los participantes de mercado puede conducir, a la pérdida total de valor de la moneda virtual o a su desaparición completa del mercado; la volatilidad del precio de la moneda virtual en relación a la moneda legal puede suponer una pérdida significativa u obligaciones tributarias en el corto plazo; nada asegura que la persona que acepte un pago en moneda virtual continúe habitualmente haciéndolo.

Cabe reconocer que las preocupaciones son legítimas, pero, porque hasta ahora las monedas virtuales carecían de disciplina pública legal. Es evidente que la *BitLicense* es un paso importante de regulación de la actividad monetaria digital y, en la medida, que su modelo se extienda y profundice, gran parte de los riesgos entrarán dentro de la previsibilidad de una actividad económica ordinaria sometida a disciplina legal, donde se pueden producir situaciones catastróficas, pero de forma diferente a las que observamos aún se producen en el sistema financiero oficial, pese a su superior desarrollo institucional e histórico. En materia de blanqueo de capitales, evasión fiscal, por ejemplo, la banca, los fondos de inversión, las empresas aseguradoras no tienen nada que envidiar a la moneda virtual y sí mucho que enseñar.

*Bitcoin* no hace sino confirmar que la desregulación de la actividad financiera, cualquiera que sea su signo, apareja la paralela presencia del tráfico ilícito de fondos. Por tanto, si bien es cierto el riesgo que supone la moneda virtual, no lo es menos que hasta ahora campa por sus fueros la completa desregulación de su actividad en los mercados, por lo que no tiene nada de extraño que abunden las patologías derivadas.

Otro tema, bien distinto, es imputarle conllevanza con su proyecto tecnológico innovador en materia de limitación de intermediarios bancarios o la descentralización operativa propugnada. La conclusión es obvia: adoptar precauciones en orden a la tutela de los consumidores, inversores, frente a la piratería informática, la evasión fiscal y el blanqueo de capitales.

## RECAPITULACIÓN

*FinCEN (Financial Crimes Enforcement Network .US Treasury)* produjo una de las primeras disciplinas reglamentarias de "moneda virtual como medio de cambio que opera como una moneda en algunos ambientes pero que no tiene los atributos de la moneda real."[82] Su preocupación es la moneda virtual convertible, que puede cambiarse por moneda real, sea bajo una dirección centralizada o descentralizada, como *Bitcoin*.

La actividad empresarial implica servicios de transmisión de moneda desde que hay otro valor que substituye o tiene un valor equivalente a la moneda real. Ello comprende a las personas que crean, obtienen, distribuyen, intercambian, aceptan o transmiten monedas virtuales. La transmisión de moneda requiere de cambistas y administradores. Los primeros son los que producen el cambio de moneda virtual por moneda real u otras monedas virtuales. Y los segundos son los que emiten la moneda virtual y tienen la potestad para retirarla de la circulación. Ambos protagonistas deben registrarse ante el *FinCEN,* conservar una contabilidad específica e informar sobre

82. J. Shasky Calvery, cit.,p.2

transacciones sospechosas relativas al blanqueo de capitales o financiación terrorista.[83]

El *FinCEN* está centrado, como es obvio, en el flujo ilícito de fondos y su principal preocupación son los Informes sobre Actividades Sospechosas (*Suspicious Activity Reports)*: las modalidades en que los fondos pueden entrar y salir del sistema con la ayuda de las instituciones financieras. La sospecha sobre la fuente e los recursos, sobre el uso, sobre el cambio de monedas, y el carácter secreto de la actividad desprovista de licencia o registro. El escenario comprende a los cambistas, administradores de moneda virtual, así como a entidades financieras y corresponsales bancarios, locales o extranjeros, que concurren en las distintas etapas de las operaciones realizadas.[84]

La idea que la moneda virtual puede ser un vehículo apropiado para el blanqueo de capitales no es meramente teórica. Por un lado el caso *Liberty Reserve*, basado en monedas virtual centralizada y descentralizada, integra un esquema de blanqueo superior a los 6 billones de dólares, al servicio de la criminalidad organizada (fraude de tarjetas de crédito, inversiones, identidades, narcóticos, pornografía infantil. Por otro, *Silk Road,* calificado como el mercado más amplio de contrabando y droga en Internet, exigía Bitcoin como medio de pago a los usuarios.[85]

La experiencia en California asume otra perspectiva, previa a la regulación particular de la moneda virtual, cual es el pleno reconocimiento de la emisión y circulación de las denominadas monedas alternativas, en paralelo a la moneda legal con respaldo público (*fiat currency, legal tender)*.[86] Es un paso trascendente porque supone la equiparación entre el dólar y otras monedas que no son sino el resultado del consenso y la aceptación entre los participantes para su empleo. Las monedas alternativas, cada una en

---

83. FinCEN, Application of FinCEN`s Regulations to Persons Adminestering, Exchanging or Using Virtual Currencies, cit;D.S.Cohen, Adressing the illicit finance risks of virtual currency, Secretary of Terrorism and Financial Intelligence, Treasury, 3/18/2014.

84. Financial Crimes Enforcement Network, Networking Bulletin, march 2013, Cryptocurrencies.

85. J.Shasky Calvery, cit., p.7.

86. *Fiat o flat money* es papel moneda sin respaldo oro o plata o que carece de valor intrínseco.

sus circunstancias de hecho y autodisciplina, cumplen objetivos análogos a los propios de la moneda legal.

Nueva York, mediante la *BitLicense,* establece una de las primeras, sino la primera, plataforma relativa a la configuración jurídica de la moneda virtual. La premisa es el reconocimiento de la innovación tecnológica, la potencialidad e inclusión de usuarios fuera del sistema bancario global, la reducción de costes de intermediación en las remesas de dinero al extranjero y, finalmente, la posibilidad de transferir un valor no solo monetario sino no monetario a la otra parte (tecnología segura y de convalidación que permite la transmisión de contratos o cosas por Internet).

Las ideas centrales tienen tres direcciones: salvaguardia de los activos de los consumidores y protección en contra del fraude y abuso; expulsión de la actividad ilegal y de blanqueo de capitales y fortalecimiento de la ciberseguridad en contra de la piratería informática.

La actividad económica de moneda virtual es parangonable a la de cualquier otro intermediario financiero. La gran diferencia es que su comercio se funda en "representaciones digitales de valor", que no dinero legal. Pero, sometidas a obligaciones de recursos propios, de contabilidad y registros, informes e información sobre actividades presumiblemente sospechosas. El sujeto debe conservar un registro general conteniendo todo activo, deuda, propiedad, capital, cuentas de ingresos y gastos, así como información identificatória de las partes en la transacción. Asimismo, los requerimientos de capital pueden constituirse no solo en dinero legal, sino también en moneda virtual y activos de inversión de alta calidad y liquidez.

La transformación de la economía virtual apunta a sostener la innovación tecnológica y la transparencia de sus agentes financieros, más o menos igual que a los que actúan en la economía real: deben conocer a sus consumidores, informar sobre transacciones atípicas, conservar sus registros y llevar contabilidad ordinaria.[87]

La identificación de los principales agentes económicos dedicados al comercio de moneda virtual y la consiguiente respon-

87. D S.Cohen, Adressing the illicit finance risks of virtual currency, 3-18-2014.

sabilidad que su legitimación integra el servicio de cambio entre moneda virtual y legal o viceversa. Esto presupone un itinerario atractivo para el desarrollo de un sistema de pagos innovador que deja en evidencia el retardo de las instituciones bancarias satisfechas en "continuar extrayendo injustificadas rentas de los consumidores".[88]

Por último, a nuestros fines, es útil acentuar el bien digital como eje de la moneda virtual: unidad digital que se emplea como medio de cambio o almacenamiento de valor digital. Efectivamente, la moneda virtual culmina la evolución del concepto de bien digital, devenido virtual por obra de la exclusión y de la escasez, que no acompaña la definición general de bien digital como bien público.

Las principales críticas en contra de la *Bit License* señalan la discriminación entre la intermediación financiera ordinaria y la que obra en moneda virtual, por mor de mayores cargas administrativas a su cargo e intervención pública en su gestión.[89] Algunas de ellas se recogen en la disciplina final, pero, otras, por ejemplo, las que tienden a la transparencia no se modifican. Primero, la necesidad de registro; la compilación de datos, documentos, información de las transacciones y segundo, "know your customer", los servicios de moneda virtual como los demás servicios monetarios deberán arbitrar mecanismos que permitan, en su caso, identificar a sus clientes.

La obligación de identificación entre las partes es otro de los puntos que suscitó críticas desde los pro-*Bitcoin* y que amenaza con ser un vicioso lugar común: el uso de seudónimos –*Bitcoin adresses*– para asegurar el uso anónimo en las transacciones. En verdad, no parece que el anonimato sea una barrera invulnerable: la cadena de firmas digitales y el empleo de moneda virtual puede ser desvelada.así,"…los perfiles de casi el 40% de los usuarios

88. Superintendent Lawsky remarks on revised BitLicense framework for virtual currency regulation and trends in payments technology, December 18, 2014; P.Van Valkenburgh, H.Geiger, B.Szoka, Comments to the New York Department of Financial Services on the Proposed Virtual Currency Framework, October 21, 2014.

89. J.Brito, Eli Dourado, Commens to the New York Department of Financial Services on the Proposed Virtual Currency Regulatory Framework, August 14, 2014, Mercatus Center George Mason University.

puede en gran medida recuperarse aun cuando los usuarios adopten las medidas de privacidad recomendadas por Bitcoin".Esto, técnicamente irrefutable, reduciría el problema del anonimato, que mayormente preocupa a las instituciones públicas, sin menoscabo del sistema de la moneda virtual. Estamos hablando casi de la mitad de los usuarios.[90]

Es comprensible que desde el ángulo público exista un ánimo precaucional que, aunque excesivo, pretende dar certidumbre al consumidor, evitando la expansión de los mecanismos de control desprendidos de la actividad ilícita. La moneda virtual sufre la misma o mayor desconfianza que la que imperó en los primeros años del comercio electrónico a través de Internet.

# 6. La moneda virtual en el ámbito internacional

## 6.1. LAS ORGANIZACIONES INTERNACIONALES

### 6.1.1. El Grupo de Acción Financiera. GAFI. (Financial Action Task Force. FATF)

El GAFI-FATF es un órgano integubernamental cuyas recomendaciones se reconocen, con la fuerza adicional que le deriva del apoyo del G 20, como standards en la lucha global contra el blanqueo de capitales y la financiación del terrorismo.

En 2014 produjo su Informe sobre monedas virtuales, preocupado por encontrar definiciones comunes y definir los riesgos potenciales en materia de blanqueo de capitales y financiación del terrorismo.[91]

---

90. E.Androulaki, G.O.Karame, MRoeschlin, T.Scherer, S.Capkun, Evaluating user privacy in Bitcoin…" Nuestros descubrimientos muestran que las medidas ordinarias adoptadas por Bitcoin no son suficientes para proteger la privacidad de los usuarios si Bitcoin fuera usada como una moneda digital en un universo determinado. "Lo que no deja de llamar la atención es que la conservación del anonimato entre las partes se vería reforzada si Bitcoin aceptara una entidad tercera de confianza- un banco Bitcoin-, lo cual entra en contradicción directa con el sistema de descentralización. ETH Zurich, 8092, 8 april 2013.

91. FATF Report, Virtual currencies.Key definitions and Potencial AML (antimoney laundering)/CFT (countering the financing of terrorism, june 2014, FATF/OECD, Paris.

El Informe reconoce la complejidad del concepto de moneda virtual y la necesidad de conceptos de comprensión común y la adopción de términos coherentes, puesto que no solo afecta los objetivos de lucha contra la corrupción o la financiación del terrorismo; sino que es necesario para la regulación de la protección al consumidor, la fiscalidad, la reglamentación financiera seria y prudente (principio de precaución) y las medidas de seguridad. El Informe sobreentiende que la prohibición o represión o restricción del tráfico ilícito no es suficiente, requiriendo una escala de principios y standards coordinados de gobernanza global, desde diversas perspectivas y áreas de experiencia.[92]

La moneda virtual es la representación digital de valor que puede digitalmente comercializarse y funciona como medio de pago; y/o unidad de cuenta y/o depósito de valor, pero carece de curso legal.

La representación digital es algo en forma de datización digital, vinculada, a través de Internet al sistema de moneda virtual.

La moneda virtual debe distinguirse de la *fiat currency* y del dinero electrónico. O sea debe distinguirse de la moneda real de curso legal y de la representación digital que procede a la transmisión electrónica de valor, fundado en la moneda de curso legal.

El Informe evita identificar moneda virtual con moneda digital, puesto que la representación digital sirve tanto a la moneda alternativa cuanto a la moneda de curso legal y, por tanto, los conceptos diferentes son moneda virtual y moneda o dinero electrónico.[93]

El GAFI-FATF establece categoría inicial de moneda virtual convertible y no convertible. La primera tiene un valor equivalente en moneda real y puede cambiarse por moneda real. La segunda, es la moneda virtual de los juegos en línea o perteneciente a los usuarios de una empresa, sin que sea idónea para el cambio por moneda real. Los riesgos derivan de la moneda virtual convertible, sin perjuicio que en el caso de la no convertible pueda surgir un mercado secundario que conduzca a su canje por moneda real.

92. FATF Report, cit, nota 4, p.13.
93. FATF Report, cit.p.4.

La moneda virtual convertible puede ser centralizada o descentralizada. Por un lado, la que tiene una administración única o la que no tiene una autoridad administrativa central.

La moneda virtual convertible descentralizada está protegida por la criptografía: la criptomoneda descansa en claves públicas y privadas para la transferencia de valor desde una parte a otra y debe firmarse criptográficamente en cada ocasión. *Bitcoin*, por ejemplo, usa un sistema de convalidación- la prueba a cargo de los mineros- de las transacciones que aseguren su veracidad y conservar la cadena de bloques.[94]

La moneda virtual convertible descentralizada, sobre bases criptográficas, o sea *Bitcoin,* es la plataforma que sirve a la descripción de los participantes en el sistema y el contraste con modelos centralizados.

En primer lugar, el cambista, quien realiza empresarialmente el cambio por moneda real o por moneda virtual y metales preciosos, por precio.

En segundo lugar, el administrador, que solo actúa en la moneda virtual centralizada, ocupado en la emisión y retiro de la circulación de la moneda virtual. Repetimos que *Bitcoin*, por definición no exige administración central o autoridad única de dirección.

En tercer lugar, el minero, que resuelve complejos algoritmos y los distribuye como prueba de trabajo entre los usuarios para convalidar las transacciones en el sistema. El desarrollo extingue gradualmente al minero individual, sustituido por *miners pool*, porque cada vez más se exigen ordenadores más potentes, alto consumo de energía y servicios.

En cuarto lugar, los proveedores de direcciones o billeteros para disponer, almacenar y transferir moneda virtual.Es una función destacada porque es en la dirección o billetero donde se hallan las claves privadas, las firmas digitales personales, imprescindibles para asignar la moneda virtual a las direcciones de la Cade-

94. FATF Report, p.5.Bitcoin fue la primera moneda virtual descentralizada y convertible y la primera criptomoneda. ”Bitcoins son unidades de cuenta compuestas por cadenas únicas de números y letras que constituyen unidades de la moneda y tienen valor solo porque los usuarios particulares desean pagar por ellas.”

na de Bloques. Esta empresa ofrece almacenamiento y seguridad, sea online *–hot storage–, u* offline *–cold storage–.*

Finalmente, el usuario que obtiene la moneda virtual y la emplea para la compra de bienes o servicios virtuales o reales o envía transferencias a otra persona o detenta la moneda virtual como inversión. El usuario puede conseguir la moneda virtual comprando con moneda real; a cambio de servicios reales o virtuales o en las actividades de minería, en la resolución de algoritmos aplicados a la convalidación de transacciones.

El uso de la moneda virtual puede estimular la mejora de los sistemas actuales de pago reduciendo costes derivados de las tarjetas de crédito y débito o pagos en línea de pequeña cuantía. Asimismo, puede facilitar las remesas internacionales y la inclusión social de millones de personas que están excluidas de los sistemas bancarios tradicionales. Pero, sometida a disciplina legal que pueda limitar sus riesgos potenciales respecto al tráfico ilícito de flujos de dinero, en modo anónimo, totalmente inmersas en el universo digital, fuera del alcance de ningúna jurisdicción.

El abuso de la moneda virtual y los episodios detectados en los casos *Liberty Reserve, Silk Road* y *Western Express International*, descubiertos por las autoridades americanas, no contribuyen a la aceptación ordinaria de la nueva tecnología de pagos. Es obvio que la criminalidad organizada puede aprovecharse de globalizar, opacando sus consecuencias. Pero, de nuevo, vale la pena, no olvidar la crisis financiera de 2008 en donde los protagonistas de la desregulación y opacidad fueron el sistema bancario y financiero global.

Por tanto, aparece urgente diferenciar la validez de la innovación y el perfeccionamiento del funcionamiento de la moneda virtual de su mal uso, porque lo mismo que se utiliza en su contra es perfectamente aplicable al mal uso de la moneda legal por los que intervienen en su gestión.

La exigencia de coordinar la gobernanza global del sistema virtual entre los distintos países es la única via para establecer criterios de transparencia que limiten los riesgos potenciales. El futuro no es la prohibición sino en principios comunes o standards de corrección mínima, que impidan en lo posible, sus desviaciones.

### 6.1.2. Oficina de las Naciones Unidas contra las Drogas y el Delito. (United Nations on Drugs and Crime).UNODC

La UNODC, es la Oficina de las Naciones Unidas cuya especialidad es la lucha contra el blanqueo de capitales, decomiso y confiscación de los resultados de la actividad criminal.

En junio de 2014 se publica un Manual Básico para la detección e Investigación del blanqueo de la propiedad de la criminalidad organizada utilizando monedas virtuales.[95]

La publicación, como es obvio, atiende principalmente las amenazas derivadas de la moneda virtual, encauzando las mismas definiciones formuladas por el GAFI-FATF. En particular: la celeridad e irreversibilidad de las transacciones; las transferencias desde la moneda de curso legal a la moneda virtual; la conversión de una moneda virtual en otra; la transferencia de moneda virtual desde una cuenta a otra; el diseño basado en el anonimato; la ausencia de registros contables o documentales; difícil identificación de las monedas virtuales empleadas; complejidad técnica deliberada de las operaciones llevadas a cabo; uso ilimitados de fondos.

Las dificultades aumentan por la falta de disciplina legal nacional y la ausencia de coordinación internacional.

*Bitcoin* comparece repetidamente a lo largo de la publicación, casi como el modelo que alimenta las suspicacias. Una, porque opera al margen de los intermediarios financieros; dos, porque sostiene el anonimato de las transacciones, aunque como se ha señalado no parece que ésto sea insuperable; y la criptografía dificulta la trazabilidad e identificación de los usos ilegales de la moneda virtual.[96]

Finalmente menciona que China y Canada prohiben o restringen el uso de Bitcoin, por los riesgos de blanqueo de capitales, su volatilidad y naturaleza especulativa. En 2014 desvela la existencia de doce monedas virtuales.

---

95. UNODC, Basic Manual on the detection and Investigation of the Laundering of Crime Proceeds using virtual currencies, june 2014.

96. UNODC, cit., p.208.

"La disociación de las cuentas de moneda virtual de las identidades del mundo real, combinada con la habilidad de cada individuo para crear un número arbitrario de cuentas significa que nuevas, y más complejas transacciones de ocultación (de dinero ilícito) son posibles."[97]

Una de las referencias más interesantes es la que hace hincapié en las dificultades para la recuperación de los patrimonios de origen criminal. A tal efecto, y en referencia a moneda virtual descentralizada del tipo de *Bitcoin* sugiere que en cuanto las transacciones internacionales se verifican entre direcciones de usuarios individuales…"bitcoins tienen una intrínseca conexión con direcciones específicas respecto a las que usuarios específicos ejercen un control efectivo."[98]

En consecuencia, añade, "en términos de aproximación jurisdiccional, bajo el derecho público internacional, la jurisdicción territorial sobre los resultados o instrumentalidades del delito en caso de criptomonedas *debe estar vinculada a la localización del billetero."*

El billetero conteniendo la moneda virtual opera en un ordenador cuya localización –el control efectivo por el usuario- determina la jurisdicción para los propósitos de congelación, decomiso y confiscación de los resultados del blanqueo de capitales. En realidad, la localización del billetero como residencia del archivo digital bajo el control efectivo del usuario, facilita su individualización. El poder de disposición de la cuenta digital como medio de señalización del billetero.

O sea, extrapolando el resultado, sería, asimismo, útil en la configuración del establecimiento permanente virtual, si ello diera lugar a efectos jurídicos tributarios: la territorialidad como fuente de la conexión de quien dispone del acceso o salida a las rentas o patrimonio de la moneda virtual.

Por último, en respeto a la neutralidad tecnológica, admite que no necesariamente la moneda virtual es, por definición, instrumento de uso ilícito, sino que puede desempeñar, aunque cueste advertirlo, modos compatibles de actividad financiera lícitas.

---

97. UNODC, cit., p.216.
98. UNODC, cit.p.141.

### 6.1.3. Autoridad Bancaria Europea. (European Banking Authority. EBA)

La ABE desarrolla su Opinión sobre las "monedas virtuales".[99] Las define como una representación digital de valor, que no es emitida por un banco central o autoridad pública ni necesariamente vinculada a una moneda legal, pero es empleada por personas físicas o jurídicas como medio de cambio y puede transferirse, depositarse o comercializarse electrónicamente.

De las características de la definición propuesta vale la pena remarcar algunas de sus apreciaciones.

La representación digital de valor es un concepto próximo al de "unidad de cuenta", pero incluye la opción de considerar la moneda virtual *como moneda privada o mercancía.*[100]

La moneda virtual se diferencia de la moneda electrónica en que carece de relación con la moneda de curso legal, emitida por los bancos centrales o la autoridad pública.

La moneda virtual es un medio de pago entre personas para conseguir bienes o servicios. *Esto evita los inconvenientes de un sistema de trueque o permuta, v, g, la coincidencia de deseos entre las dos partes implicados en la transacción.*[101]

Finalmente, la moneda virtual puede transferirse desde un usuario a otro por medios electrónicos; depósitado en un instrumento electrónico o servidor y comercializado electrónicamente.

La Opinión acentúa perfiles que pueden ser más o menos comunes a la moneda virtual.

Así, carece de status o curso legal obligatorio; puede ser centralizada o descentralizada; convertible en moneda legal o no convertible; no redimible, por lo que no implica ninguna obligación del emisor.[102]

Los participantes son plurales.

---

99. EBA European Banking Authority, Opinion on "virtual currencies",4 july 2014.

100. EBA, cit.p.11.

101. EBA,cit. p.12.

102. EBA,cit.p.13.

- Usuario: el que compra bienes o servicios virtuales o reales o envía remesas a otro o posee la moneda virtual como inversión. El usuario obtiene la moneda virtual por cambio, ejerciendo actividades específicas (promoción, informes en línea, minerías) o recepción de otros usuarios.
- Comerciante: es un empresario que acepta la moneda virtual por sus bienes y servicios.
- Cambista: es el que cambia moneda virtual por moneda de curso legal u otras monedas virtuales.
- Plataforma comercial: es un mercado de compraventa de moneda virtual.
- Proveedores de servicios de procesos: el que facilita la transferencia de unidades de moneda virtual desde un usuario a otro por medio de tecnología de información.
- Proveedores y depositarios de billeteras: el proveedor administra la cuenta virtual y ofrece el balance de sus transacciones. Las billeteras pueden almacenarse en línea o no. La última de las opciones se considera más segura para protege la billetera.

Sin perjuicio de recoger sumariamente algunos de los beneficios potenciales, la Opinión se decanta por los riesgos que implica, identificando más de 70, entre otros, riesgos para los usuarios, para los no usuarios; para la integridad financiera; para los sistemas de pagos convencionales y para las autoridades y gobiernos.[103]

En suma, el alerta de la Opinión es universal, no queda ninguno exento de los peligros de la moneda virtual. Ni siquiera la disciplina legal está en condiciones de salvar los peligros. No extraña que se recomiende a las autoridades de supervisión nacional que desalienten a las instituciones de crédito, de pago y de moneda electrónica de compra, mantener o vender moneda virtual.

103. EBA, cit, p.38.

### 6.1.4. Banco Central Europeo. (European Central Bank.ECB)

El Banco Central Europeo ha publicado dos investigaciones sobre Esquemas de Moneda Virtual.[104]

La primera de ellas define la moneda virtual como un tipo de moneda digital desregulada, que es emitida y usualmente controlada por los que la desarrollan y es aceptada entre miembros de una comunidad virtual específica.

Esto fue objeto de críticas, debido a la propia evolución de la materia. Por un lado, la regulación emerge en algunos países, v.g. EEUU y por otra, *Bitcoin* ilustra sobre un esquema descentralizado que no cuenta con una autoridad única y unitaria.

En la segunda versión, 2015, la moneda virtual es una representación digital de valor, que no es emitida por un banco central, institución de crédito o de moneda electrónica, que en algunas circunstancias puede utilizarse como una *alternativa a la moneda.*

El cambio elimina la palabra "moneda", que es excluida de la definición porque las monedas virtuales no tienen las características de un activo liquido y no tienen la aceptación asociada con la moneda. La moneda virtual, dice, no es moneda. Asimismo, elimina la palabra "desregulación" porque, en el interín, algunos países e instituciones han comenzado a hacerlo. Finalmente, también cancela la referencia al empleo de la moneda en comunidades virtuales que la reconocen. Pero, incorpora el concepto de moneda alternativa que no deja de ser una contradicción con las previas exclusiones: moneda alternativa es moneda que no se solapa a la moneda legal, pero sirve como tal para las comunidades virtuales que la recogen o las redes de usuarios que la usan.[105]

Desde una perspectiva legal, dice el ECB, la moneda virtual que no se usa ampliamente en los intercambios dentro de un país no puede ser moneda. Por una parte, porque carece de curso legal o formato físico. "Esto significa que la moneda virtual solo pueden utilizarse como moneda contractual, cuando hay acuerdo

104. European Central Bank, Virtual Currency Schemes, october 2012; Virtual currency schemes- a further analysis, february 2015.

105. ECB,cit,2015,p.25

entre comprador y vendedor en orden a aceptar una determinada monea virtual como medio de pago".[106]

Hay, no obstante, dos referencias a tener en consideración. Por un lado, que la representación digital de valor puede asumirse como unidad de cuenta, moneda y mercancía al mismo tiempo. Por otro, que las operaciones en moneda virtual se distancian del concepto de trueque o permuta.

El BCE propone tres esquemas de moneda virtual. Primero, el esquema cerrado, que no tiene vínculo con la economía real, v.g. los juegos virtuales tales como *World of Warcraft*. Segundo, el esquema con flujo unidireccional que permite la compra de moneda virtual mediante moneda de curso legal a un tipo de cambio particular, pero que no admite la conversión, de nuevo, en moneda real, v.g. *Facebooks Credits.*Tercero, el esquema con flujo bidireccional que se basa en la compra y venta de moneda virtual de acuerdo al tipo de cambio con su moneda. La moneda virtual es similar "a cualquiera otra moneda convertible con respecto a su interoperabilidad con el mundo real, v.g. Bitcoin"[107]

No es ésta la clasificación adoptada en el Informe FATF-GAFI, que reduce la triple categoría a dos: moneda virtual no convertible(cerrada) relativa a los juegos virtuales o en algunas empresas como *Amazon* y la moneda virtual convertible (abierta) que tiene valor equivalente en moneda de curso legal y puede cambiarse por moneda real, v.g. *Bitcoin.*[108] El fundamento en que se apoya es que solo la moneda virtual convertible y abierta desplaza valor dentro y fuera del sector financiero propiciando los riesgos de blanqueo de capitales y financiación al terrorismo.

La moneda virtual es diferente al dinero o moneda electrónica. El formato digital de ambas no oculta que sean diversas: la unidad de cuenta de la moneda electrónica es moneda de curso legal y su aceptación es compartida por el emisor y por el receptor como medio de pago; sin perjuicio que, por otra parte, esté legalmente regulada, garantizada y sometida a supervisión como los demás medios de pago institucionales financieros.

---

106. ECB,cit.2015,p.24
107. ECB,cit,2012,p.14
108. FATF Report, cit.n.8, p.13.

El énfasis en los riesgos supera la motivación de innovación tecnológica y la promoción de nuevos medios de pago para los consumidores. En particular, la falta de transparencia, claridad y continuidad; el anonimato; la alta volatilidad de la moneda virtual. Queda por ver su potencial futuro, sobre todo, en materia de aplicación: Bitcoin representa unas 70.000 transacciones diarias a nivel mundial sobre unas 270 millones solo en la Unión Europea.

## RECAPITULACIÓN

El GAFI-FATF exhibe, hasta ahora, una posición mesurada y constructiva sobre la moneda virtual. No propone, como se podría esperar, un escenario catastrófico o apocalíptico. Al fin y al cabo, sus funciones le habilitarían para ello, centrado como está en la lucha contra el blanqueo de capitales y la financiación al terrorismo. Es digno de encomio su esfuerzo para encontrar un lenguaje compartido, conceptos definidos y conclusiones de alcance global. No hay alternativa, parece ser el final, sin la coordinación entre países para establecer bases mínimas de regulación de la innovación financiera.

No hay duda que el actual vacio normativo es una tentación para el tráfico ilícito transfronterizo de fondos; pero, al mismo tiempo, destaca que la moneda virtual, cualquiera que sea su calificación, arroja presupuestos positivos de inclusión social, en la remisión internacional de dinero o en la reducción de costes en las tarjetas de crédito o en pagos de pequeña cuantía.

La Oficina de las Naciones Unidas contra las Drogas y el Delito (UNODC) sigue puntualmente el itinerario diseñado por el GAFI-FATF: conservar la neutralidad tecnológica, sin renunciar al combate contra su aprovechamiento ilícito. Si es válido señalar, por su utilidad tributaria, la indicación especial a la localización del billetero digital como conexión jurisdiccional para la congelación, decomiso, confiscación de los bienes y propiedades de origen ilícito. El poder de disposición del usuario para acceso, salida, cancelación de operaciones es el espacio de localización de la renta o del patrimonio ocultado y esto determina la jurisdicción territorial sobre los resultados o instrumentalidades de la moneda

virtual. No es temerario aproximar el concepto aplicable al de establecimiento permanente virtual.[109]

"El poder formal de disposición conecta cualquier dato a la persona o personas que obtienen acceso y tienen el derecho de alterar, borrar o suprimir o inutilizarlo así como el derecho de excluir a otros del acceso y uso." Así, la jurisdicción donde ello se produce está en condiciones de obtener legalmente de la persona las credenciales y claves de su combinación para establecer los extremos de sus operaciones."[110]

La Autoridad Bancaria Europea (EBA) expresa su Opinión en términos catastrofistas y apocalípticos. Es un catálogo de los infinitos riesgos que conlleva la moneda virtual y los pobres beneficios que su desarrollo podría procurar. Hay, no obstante, dos referencias a tener en consideración. Por un lado, que la representación digital de valor puede asumirse como unidad de cuenta, moneda y mercancía al mismo tiempo. Por otro, que las operaciones en moneda virtual se distancian del concepto de trueque o permuta.

El Banco Central Europeo (ECB) es aún más radical en su posición, porque parte de la premisa que la moneda virtual no es moneda o cosa que se le parezca. Los argumentos son irrisorios. El alcance geográfico no excluye otras monedas distintas a la moneda de curso legal, en la medida en que su empleo sea fruto del consenso entre los participantes, aun sin respaldo legal establecido. Esa es la naturaleza de la moneda virtual. A esto se responde, como ya se hizo, señalando que no hay fundamental diferencia entre moneda virtual y moneda real: una es moneda con un área monetaria pequeña y la otra con un área más dilatado.[111]

Por último, acentua los peligros y riesgos, solo salvados en su versión de falsa profecía, por su escasa difusión actual, que le hace soportable para la autoridad bancaria.

---

109. T.Rosembuj, El impuesto digital, Barcelona, 2015, p.105.

110. J. Spoenle, Cloud computing and cybercrime investigations: territoriality vs. the power of disposal,?,31 August 2010, Project on Cybercrime,Council of Europe,

111. V.Lehdonvirta, E.Castronova, Virtual Economies. Design and Analysis, op.cit.p.192.

# 7. Los bancos, las autoridades financieras y representativas nacionales

El debate sobre la moneda virtual no ha hecho sino comenzar. Y entre las distintas posiciones destaca el Reino Unido que está produciendo una documentación seria y solvente donde antepone los beneficios a los riesgos, con lo que altera la descripción dominante en el marco de los bancos centrales, autoridades financieras y representativas.

Es más, el diseño del Reino Unido es el que mejor articula el reconocimiento a la innovación tecnológica del tipo *Bitcoin* en los sistemas de pagos existentes sin perjuicio de prestar atención a los riesgos sistémicos, prudenciales, de conducta o comportamiento que su instalación puede provocar, bajo la enseña de la mayor competencia en interés de los consumidores y la innovación tecnológica, que trasciende el marco de los pagos.

## **7.1.** EL REINO UNIDO

Desde 2014 hay en un curso un programa de trabajo sobre los beneficios y riesgos asociados con las monedas digitales y las tecnologías subyacentes, enfatizando las pautas de disciplina legal. En noviembre de 2014 lanzó una consulta pública destinada a recoger información.

En 2015 el Banco de Inglaterra produjo un importante documento en el que expone los principales desafíos que el futuro depara al sistema bancario y financiero.[112]

"Como ejemplo, los pagos y el crédito experimentan recientes innovaciones en la forma de monedas digitales y fuentes de financiación alternativas. *Las monedas digitales, potencialmente combinadas con la tecnología móvil, deben reformar los mecanismos de pagos seguros, permitiendo transacciones directas entre los participantes.* Esto tiene profundas implicaciones para el sistema financiero cuyos mecanismos de pagos dependen de los depósitos bancarios

112. One Bank Research Agenda, Discussion paper, february 2015, Bank of England.

que necesitan crearse a través de crédito. Igualmente, la tecnología apoya la emergencia de nuevos modelos de empresas, tales como los préstamos persona a persona y el *crowfunding,* que crean fuentes de financiación alternativas para los individuos y empresas."[113]

Inmediatamente, plantea los interrogantes monetarios fundamentales que pudieran consentir que los bancos centrales pudieran usar los fundamentos tecnológicos de las monedas virtuales, v.g. Bitcoin, para su emisión.

El mérito tecnológico puro de la moneda virtual descentralizada es el sistema de cadena de bloques (*blockchain)* que resuelve el problema del "*double spending".* El sistema de pagos descentralizado fundado en un registro distribuido, a partir del cual se evita la autoridad central porque cualquier usuario puede contrastar la transacción en curso y su validez contra el registro.[114]

El fundamento de la moneda virtual, entonces, es aceptado y hay diferentes modos en que el banco central puede utilizar la moneda digital. Primero, sirve para la compensación interbancaria, para proveer a bancos. Asimismo, puede ser puesta a disposición de entidades no financieras o personas, tal como hoy sucede con los cheques bancarios; prestando atención a sus efectos sobre los depósitos de los bancos comerciales o de los que puedan derivar del *clearing* interbancario en los sistemas de pago.

Otros puntos importantes a investigar se relacionan con el tipo de tecnología a emplear, tratando de mejorar la existente, sin incurrir en ineficiencia social, por exceso de coste en la verificación de las transacciones. O, preservar que la cadena de bloques no comprometa el ejercicio de su control sobre la moneda en general y garantizar la seguridad ante ataques sistémicos. En particular, la constitución de un sistema amplio de fraude basado en el control mayoritario del poder informático de base sobre la red de mineros, creadores de moneda virtual.[115]

---

113. One Bank Research Agenda, cit, Response to fundamental change, 5, Central bank response to fundamental technological, institutional, societan and environmental change.

114. R.Ali, Jh.Barrdear, R.Clews, J.Southgate, Innovations in payment technologies and the emergence of digital currencies, Quarterly Bulletin Bank of England, 2014.

115. Un grupo de personas o un pool de mineros podrían controlar una parte sustantiva del poder, de la potencia, informática y podría ser capaz de controlar las autoriza-

Desde la perspectiva legal, la moneda virtual plantea tres interrogantes: sistémico, prudencial y de conducta.

El desafio sistémico apunta al protocolo, al gobierno del software bajo el que el sistema tecnológico funciona (*the code is the law).*El documento propone la creación de un protocolo de transferencia de valor a través de Internet próxima a la idea de la Web (Berners-*Lee*) en materia de información.

El desafio prudencial atiene a que debe establecerse la diferencia entre los operadores en moneda virtual y los bancos existentes en cuanto a los requisitos de capital y liquidez.

El desafio de conducta se refiere a la disciplina antiblanqueo y, finalmente, establecer equilibrio entre la identidad de la gestión digital y las consideraciones de privacidad.

Los puntos a investigar en el futuro son plurales:

- Costes y beneficios de una nueva forma de moneda bajo autoridad del banco central accesible a una amplia base de usuarios.
- Impacto sobre los sistemas de compensación bancaria existentes.
- En que modo se vincula la remuneración de la moneda digital emitida por el banco central y la política de tipo de interés.
- En que forma compiten los bancos ante la migración de sus fondos a la moneda digital y las consecuencias sobre la disponibilidad de crédito.
- Cuales serían los costes y beneficios de diferentes bancos centrales compartiendo una plataforma común de emisión de moneda digital y que modelo tecnológico de registro distribuido es el más adecuado si hay respaldo de un banco central.

---

ciones de pagos o, inclusive, crear transacciones falsas: "51% attack" R. Ali y otros, cit., estiman que conforme a las investigaciones realizadas, la creación de transacciones falsas pueden derivar incluso sin mayoría de poder informático.

– Como se articularían las disciplinas legales de las instituciones que ofrecen acceso a la emisión por el banco central de monedas digitales.

En marzo de 2015, finalmente, el Tesoro hizo pública la respuesta a la consulta informativa formulada a la comunidad empresarial, académica, financiera.[116]

El esquema de moneda digital ante el cual se orienta combina el sistema de pago descentralizado y la moneda vinculada, por el interés en los beneficios potenciales de la tecnología de cadena de bloques; sin perjuicio de considerar también exáminar la disciplina de monedas convertibles centralizadas, gestionadas por una entidad unitaria.

El concepto, propio de *Bitcoin* califica la novedad tecnológica por su rápida, eficiente y segura transferencia de propiedad de un bien digital en internet, con un registro permanente de lo que se hace y sin necesidad de un intermediario supervisando el proceso. Una tecnología versátil puesto que permite otras aplicaciones, por ejemplo, la transmisión de propiedad de obligaciones, acciones, títulos valores y otros instrumentos financieros o ámbitos que requieren constante actualización, autenticación o prueba de identidad.

No obstante, este acento en los beneficios de la innovación tecnológica toma en cuenta la necesidad de precaución ante la actividad ilícita -criminalidad organizada y terrorismo- y conseguir su efectiva identificación, persecución y sanción. Pero, sin dramatizar: "…la información no sugiere que las monedas digitales hayan sido ampliamente adoptadas como vehículo de pago de la más amplia comunidad criminal."[117] En verdad, el reproche al anonimato es debido a la ausencia de un régimen legal de "*know your customer"*. Estos riesgos están vinculados a la ley antiblanqueo, su aplicación y sanción a los responsables.

Los riesgos de la transferencia de valor digital a los usuarios exigen standards que ofrezcan claridad respecto a la seguridad en

116. HM Treasury, Digital currencies: response to the call for information, march 2015.

117. HM Treasury,cit.p.14

los servicios utilizados, pero, sin perturbar la innovación y desarrollo de la moneda digital.

Finalmente, son mínimos los riesgos a la estabilidad monetaria y financiera.[118]

Las Conclusiones de la consulta merecen reseñarse. Es el primero de los gobiernos que asume el compromiso con el esquema de moneda virtual, modelado en la horma de *Bitcoin.*

El punto de partida no puede ser más claro: la moneda digital lícita ofrece una opción innovadora, alternativa a la opción de pagos existentes y ofrece ventajas para los micropagos, las remesas al exterior y el comercio transfronterizo.

"El gobierno se compromete a incrementar la competencia bancaria en interés de los consumidores. Es vital alentar la innovación en los pagos. El gobierno entiende crear un ambiente de liderazgo mundial para el desarrollo de los pagos innovadores y la tecnología financiera."[119]

La moneda digital puede ser atractiva para propósitos legítimos; así como para fines ilícitos. El gobierno entiende aplicar la legislación antiblanqueo para apoyar la innovación e impedir su uso criminal.

Nótese que se distingue el efecto positivo de la moneda digital susceptible de aprovechamiento delictivo, pero, salvado el postulado de la innovación tecnológica, asumiendo, la desviación como patología evitable. No es casual que se cite el Informe del FATF-GAFi, que, a diferencia de otros, no excluye el empleo legítimo de la moneda digital.

Los usuarios están expuestos a riesgos derivados de la incipiente tecnología y de la industria; para cuya protección se deben implementar standards voluntarios de buenas prácticas, sin que ello imponga una carga administrativa desproporcionada sobre la industria.

---

118. R.Ali, Jh.Barrdear, R.Clews, J.Southgate, The economics of digital currencies, Bank of England, Quarterly Bulletin, 2014.

119. HMTreasury, cit., p.19.

La perspectiva no es análoga a las iniciativas americanas –FinCEN o New York– de las que se asume suponen elevados costes administrativos de cumplimiento y dañan al sector.

## **7.2.** FRANCIA

En 2013 el Banco de Francia avanza su posición contraria a la moneda virtual.[120]

*Bitcoin* es una moneda virtual no regulada presentada como una alternativa a la moneda legal que no ofrece ninguna garantía de reembolso. Es una concepción altamente especulativa, porque limita la cantidad máxima de moneda y, por tanto, organiza su penuria. Las plataformas de servicios proponen sin garantía alguna de precio ni de liquidez, la compra venta de moneda virtual contra las monedas de curso legal. De su anonimato derivan los riesgos de blanqueo de capital y el financiamiento del terrorismo. Asimismo, los elementos que restringen su uso como inversión radican en que el valor de la moneda virtual no representa ningún activo subyacente; es sumamente volátil; su carencia de estado de moneda legal.

”Desde que no ofrece ninguna garantía de seguridad, de convertibilidad y de valor, el *Bitcoin* presenta poco o ningún interés para una utilización por los actores económicos, más allá de los aspectos de marketing y publicitad, exponiéndolos a riesgos importantes.”[121]

En 2014 la AMF (*Autorité des marches financiers)* publica su propia valoración sobre las monedas virtuales.[122]

Su documento viene a coincidir, a grandes rasgos, con el acento en los riesgos emergentes de la moneda virtual, sin dar cuenta ni motivación suficiente sobre sus aspectos tecnológicos u operativos que podrían ser de beneficio a los usuarios y a los sistemas de pagos alternativos a la intermediación financiera.

---

120. Focus, 10- 5 décembre 2013, Banque de France.

121. Focus, cit., p.5.

122. Cartographie 2014 des risques et tendances sur les marchés financiers et pour l’ épargne, Risques et tendances n.15, juillet 2014, Autorité des Marches Financieres.

Así, enumera riesgos jurídicos y reglamentarios, porque no es moneda legal; riesgos operativos, porque no hay garantías a la calidad de los servicios, capital o procedimientos de gestión de riesgos; riesgos de contrapartida, de liquidez de no ejecución; riesgos de mercado, por su volatilidad; riesgo contable, porque no pueden calificarse como moneda o activo financiero, sino, a lo sumo, como activo físico; riesgo sistémico de inestabilidad financiera.

En junio de 2014 un Grupo de Trabajo dependiente del Ministerio de Hacienda y Cuentas Públicas, promovió un informe en contra de las monedas virtuales tendentes a prevenir sus usos para fines fraudulentos o de blanqueo de dinero.[123]

Las Recomendaciones detectan tres fuentes de riesgos: actores no regulados; ausencia de transparencia y extraterritorialidad.

Los riesgos derivados ocupan tres apartados: encuadramiento de la utilización; regulación y cooperación y conocimiento e investigación.

El primero propende a limitar el anonimato mediante la apertura desde el inicio de una cuenta en moneda virtual y la obligación de declaración de tales cuentas; limitar los métodos de pagos anónimos; limitar el intercambio entre bienes y servicios y monedas virtuales a través de su cuantía y el control de la identidad. En el segundo, tienden a la armonizació de la legislación comunitaria e internacional y la sujeción de los usuarios a las disciplinas tendentes a evitar el blanqueo y la financiación del terrorismo; control de los profesionales que intervienen o participan en las operaciones con monedas virtuales. En el tercero, propone adaptar el cuadro legal y los métodos de investigaciones y mejorar el conocimiento del sector

### 7.2.1. Informe Marini-Marc de la Comisión de finanzas del Senado sobre el desarrollo de Bitcoin y otras monedas virtuales

El Informe Marini-Marc del Senado ofrece una aproximación menos dogmatica y conceptualmente más rica que la de las auto-

123. Ministere des Finances et des Comptes Publiques, L`encadrement des monnaies virtuelles.Recommandatations visant a prévenir leurs usages á des fins frauduleuses ou de blanchiment, junio 2014.

ridades administrativas bancarias y financieras. Pero, sin llegar al atrevimiento británico que dice de una moneda virtual lo que diría de la moneda legal.[124]

De las Conclusiones y Recomendaciones del Informe conviene apuntar las siguientes.

Primero, el desarrollo de las monedas virtuales y, en particular *Bitcoin,* representa un fenómeno de largo plazo que impone importantes interrogantes económicos y jurídicos y que no deberían ser ignorados por los poderes públicos. ”Pese a sus riesgos claramente identificados, respecto a su volatilidad, a su anonimato y a su ausencia de garantía legal, *Bitcoin* es portador de múltiples oportunidades para el futuro, en tanto que medio de pago, pero sobre todo, en cuanto tecnología de convalidación descentralizada de las informaciones.”[125]

De sus méritos destacan los costes cuasi nulos de transacción; la creación monetaria que retribuye a los mineros y la seguridad en las transacciones por mor de la criptografía descentralizada. En particular, el protocolo de convalidación de las transacciones descentralizadas permite eliminar al tercero de confianza que no tiene la información completa, que aparece perfectamente verificada por la tecnología empleada.

Precisamente, la convalidación de las transferencias de valor podrían ser útiles, también, en otros campos de información no necesariamente monetarios: documentos de identidad; diplomas y otros certificados, votos electrónicos. ”El fraude sobre la autenticidad de numerosos documentos o procedimientos podría resultar considerablemente reducido.”[126]

Segundo, los riesgos señalados indican su volatilidad; la ausencia de garantías de convertibilidad en moneda real; el anonimato. Pero, es destacable, que se rechace el alarmismo, porque, en el fondo, todo viene de la falta actual de regulación legal. La

---

124. Ph.Marini-F.Marc, Rapport d´information, Commission des finances sur les enjeux liés au developpement du Bitcoin et des autres monnaies virtuelles, Sénat, n. 767 rectifié, 23 juillet 2014.

125. Les Conclusions et Recommandations de la Commission des Finances, cit.,1º , 2º

126. Rapport .cit., p.11.

regulación de las monedas virtuales, se dice, aparece hoy como una necesidad.

Tercero. Los poderes públicos deben trabajar en la puesta a punto de un encuadramiento jurídico equilibrado, impidiendo las desviaciones sin comprometer la capacidad de innovación. Al respecto, el recurso a las categorías jurídicas de derecho común aparece como la solución más razonable.

La calificación de la moneda virtual es la de una operación de trueque en versión digital. Es una visión ciertamente equivocada, pero, que es consecuencia de negarla como moneda. En efecto, si el *Bitcoin* no es moneda alternativa ni medio de pago; su entrega a cambio de otra cosa, derecho o dinero es un puro intercambio voluntario entre las partes, ajena a cualquier otra denominación mercantil más precisa: compraventa, ahorro o inversión, activo financiero en operaciones de derivados financieros, contratos de futuro, swaps.

La versatilidad de *Bitcoin* difícilmente encaja en el *barter* o, mejor dicho, no se agota en el trueque, aunque puede incluirlo. Por un lado, puede ser medio de pago para la adquisición de bienes y servicios o medio de cobro de bienes y servicios vendidos; pero, también, puede servir al cambio por moneda de curso legal o para el pago del alquiler o servicios de cualquier tipo, en la medida que la otra parte de conformidad.

En suma, la naturaleza de moneda digital, aún alternativa, impone soluciones análogas o semejantes a la moneda legal. O, si se prefiere, si se propone un estatuto legal a la existencia de la moneda alternativa; no puede diferir sustancialmente del atribuido a la moneda legal.

Finalmente, el Informe aconseja que la regulación de la moneda virtual, en su caso, no puede asumir sino un ámbito europeo o, directamente, global, habida cuenta del "carácter transnacional de las monedas virtuales".[127]Desde la perspectiva global, no obstante, el impulso virtual de los EEUU y RU recorren un camino de influencia directa sobre las expectativas de cualquier otro Estado, porque, si algo se aprende de Internet, es que las prohibiciones,

127. Rapport,cit. ,5º

por fuertes que sea, no impiden su expansión ,y esto es aplicable tanto a China, Rusia o Japón como a Ecuador.

## **7.3.** ALEMANIA.FEDERAL FINANCIAL SUPERVISORY AUTHORITY. BAFIN

BaFin califica Bitcoin como unidad de cuenta, bajo la ley alemana. Y, por tanto, es un instrumento financiero.

La moneda virtual no se identifica con el dinero electrónico ni con la moneda legal. ”El valor monetario de Bitcoin deriva del hecho que son realmente usados y aceptados como medios privados de pagos.”[128]

El punto a destacar es la afirmación que *Bitcoins* se evidencian como unidades monetarias en la medida que se caracterizan como unidades de cuenta, pero con la diferencia que no tienen curso legal. ”Esto incluye unidades de valor que sirven como medio privados de pago en operaciones de trueque (*barter*)…”[129]; lo que viene a significar que su uso comprende tanto operaciones de trueque como otras que no lo son.

La moneda virtual es comparable con divisas y puede expresarse en moneda de curso legal, a pesar que no lo sea ni, tampoco, ningún tipo de divisa. La creación y empleo de Bitcoin no exige autorización. Pero, si se hace como actividad empresarial se le califica de instrumento financiero y exige autorización previa para la actividad. Esto comprende la compraventa de instrumentos financieros por cuenta de terceros o las actividades de comisión e intermediación en la compraventa de los mismos.

El concepto de moneda privada identifica las operaciones entre particulares, asimilables a operaciones de trueque, pero aceptando que hay otras que no lo son; que si resultan de actividad de empresa supone la obligación de autorización para el comercio de instrumentos financieros.

---

128. BaFin, Annual Report 2013.
129. BaFin, Trading in Bitcoins, 17 june 2014.

El BaFin advierte sobre los riesgos existentes del comercio de moneda virtual para el consumidor o entornos de criminalidad organizada y blanqueo de capitales o la volatilidad y ausencia de garantías en la circulación de Bitcoin.

El comercio de Bitcoin está sujeto a la supervisión legal como cualquier otro instrumento financiero (acciones, derivados, divisas extranjeras,)"El propósito de la supervision es asegurar el cumplimiento de los standards financieros y organizativos en relación a los consumidores e instrumentos financieros".[130]

## RECAPITULACIÓN

El RU privilegia los beneficios sin menoscabar los riesgos, considerando que, en principio, el discurso de la moneda virtual no escapa a su definición, esto es, estamos hablando de una moneda y de su relación con la moneda de curso legal y del eventual respaldo del banco central a su circulación. De esto se desprende que el RU, a diferencia del resto de los Estados Miembros y de las autoridades bancarias de la Unión Europea, adopta una posición primera ante la moneda virtual que ni la prohíbe, descarta o excluye como ámbito de actuación futura de cualquier banco central. *Al contrario, entiende que es una oportunidad para mejorar la competitividad en el sector bancario y financiero en beneficio de los consumidores y con fundamento en la innovación tecnológica que depara menores costes y más rapidez de ejecución que los medios de pago usuales.*

La premisa del gobierno británico es que, aún reconociendo las barreras existentes, propone la importancia de la tecnología del registro distribuido como medio de innovación de los sistemas de pago y su utilidad social en micropagos, remesas de dinero o transacciones transfronterizas. Es un modo de transformación análogo al que produjo internet en la transferencia de información; esta vez localizada en la transferencia de valor.

130. BaFin, J.Münzer,Bitcoins:Supervisory assessment and risks to users, 17 february 2014

Las autoridades bancarias y financieras de Francia exhiben una disposición genéricamente negativa ante la moneda virtual, elevando a defecto lo que son las características de la moneda legal, que, por definición, no lo es. Los riesgos son sobradamente superiores a sus beneficios y su interés es meramente publicitario o de marketing. Así viene a coincidir con las posturas similares de la autoridad bancaria y financiera de la Unión Europea. La posición de la administración financiera es más estricta todavía porque solo advierte el riesgo de la moneda virtual orientada al blanqueo de capitales y financiación del terrorismo. La Comisión de Finanzas *Marini-Marc,* en cambio, expone menos dogmatismo porque valora la moneda virtual no tanto como moneda sino como instrumento tecnológico renovador. Se equivoca, sin embargo, en la calificación jurídica –operación de trueque– que es correlativa al desconocimiento de su categoría de moneda.

Alemania está próxima a la posición de Francia. Pero, es distinta, menos enfática y más abierta a la evolución de las circunstancias. No parece que Alemania ostente la misma posición que las autoridades bancarias o de supervisión financiera de la UE. Por un lado, porque entiende que la moneda virtual puede ser unidad de cuenta, como cualquier otra moneda y la individualización como instrumento financiero cuando es objeto de explotación empresarial o profesional, parangonable a cualquier otro activo financiero. Una moneda que, aunque privada, es moneda.

# CAPÍTULO II
# LA FIRMA DIGITAL

## 8. La firma digital

La firma digital es una construcción matemática que acredita la autenticidad de un mensaje de datos electrónico, La firma es la persona que la envía y que el receptor cree que es producto propio del remitente y no sufre alteración desde el punto de origen al punto de destino. La firma digital, criptográfica, del que remite usa la clave privada para cifrar el mensaje mientras que el receptor usa la clave pública del remitente para descifrar.

La definición UNCITRAL de la firma electrónica significa datos en forma electrónica, aneja o lógicamente asociada con un mensaje de datos, que debe utilizarse para identificar al firmante en relación al mensaje de datos y a indicar la aprobación del firmante a la información contenida en el mensaje de datos.[131]

La firma electrónica es un bien digital –datos en forma electrónica- que supone la identificación del que firma y su aprobación a la información contenida en el mensaje de datos. La única duda es la expresa mención al deber de identificación del firmante, no solo a la aprobación del contenido del mensaje, porque, de la propia aplicación del sistema criptográfico destaca la imposibilidad de descender de la clave pública a la clave privada, lo cual convierte en aparente el deber de identificación personal, no por ninguna inclinación ideológica, sino porque el sistema criptográfico lo restringe o evita.

---

131. UNCITRAL, cit., art. 2, a); Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por el que se establece el marco comunitario para la firma electrónica; Ley 59/2003, de 19 de diciembre, de firma electrónica.

La firma, cualquier tipo de firma, sirve para finalidades claras: identificación de la persona firmante; dar certeza del compromiso personal del firmante en el momento de la firma y, sobre todo, asociar a la persona con el contenido del documento que firma.[132]

*Bitcoin,* usa un modelo de criptografía asimétrica, en 2008, que es una réplica del Modelo de sistema de firma electrónica digital adoptado en 2001 por las Naciones Unidas, UNCITRAL*;* solo reformado en el capítulo de certificación de servicios.*[133]*

## **8.1.** LA FIRMA DIGITAL Y EL DERECHO A LA INTIMIDAD

La transacción es un mensaje, una comunicación, un compendio de información digital desde una dirección pública a otra dirección pública que el remitente firma con su clave privada para que se difunda entre la red de usuarios. Hay dos claves, una pública y otra privada, que tienen correlación matemática por lo que el software responde: la clave pública, compartida con la comunidad en red, permite verificar si el mensaje que llamamos transacción fue realmente firmado con la clave privada correspondiente. La verdad de la firma (privada) delata que el mensaje le es propio.

"La relación matemática entre la clave pública dada y la correspondiente clave privada permite a los usuarios verificar la propiedad de bitcoin (esto es, *que el propietario* detenta *la clave privada),* simplemente, comprobando la clave pública mediante el software Bitcoin."[134]

Los mineros graban y despliegan el mensaje denominado transacción en un bloque, permitiendo que la comunidad de usuarios acceda a la novedad del registro público distribuido.

Por tanto, el mensaje se perfecciona solo en tanto y en cuanto se produce su incorporación al registro público, su entrada y constancia *urbi et orbe* es la transacción, cualquiera que sea, el objeto,

---

132. UNCITRAL, cit.p.19, par.29.

133. UNCITRAL, Model Law on Electronic Signatures with Guide to Enactment, 2001.

134. Jerry Brito, Houman Shadab, Andrea Castillo, Bitcoin Financial Regulation: Securities, Derivatives, Prediction Markets, and Gambling, The Columbia Science & Technology Law Review, Vol. XVI, 2014, p.149.

contenido o finalidad. El sistema asegura que la coincidencia entre la clave pública y privada, es equivalente a la transacción, en verdad, es la transacción en términos sustantivos. El transmitente nos dice el registro público, detenta la clave privada, por tanto es legítimo propietario de lo que transfiere, cualquiera que sea su contenido o denominación y la inscripción contable en el bloque establece que se perfecciona la transmisión de la propiedad que ostentaba antes de su registro. Hay un propietario que desaparece y emerge otro nuevo y así sucesivamente, encadenados los mensajes denominados transacciones en orden cronológico.

El nucleo de *Bitcoin* es el mensaje que puede ser portador de diversos bienes digitales, sea como moneda para transmitirse de persona a persona a cambio de moneda de curso legal o para bienes o servicios, o como instrumento de inversión; la promoción de contratos programables (*smart transactions*) sin intervención de terceros o de ejecución legal; certificación de identidad; y cualquier convención, acto, contrato, negocio jurídico realizado en primera persona con otra.

"En los sistemas de monedas, el transmitente no trata de transferir otra cosa usando la unidad de criptomoneda como un símbolo de esa otra cosa. El transmitente meramente transfiere la unidad de criptomoneda transfiriendo la inscripción contable en el registro."[135]

La firma digital, entonces, es la plataforma de la moneda virtual, su exigencia necesaria e insustituible. Pero, encaminada hacia su registro público.

El mensaje, los datos, son parte de la persona y consonantes con la facultad de cada individuo en la disposición de sus datos propios. La firma es, obviamente, una de las expresiones esenciales de la situación existencial de cualquier persona. Cada firma es cada persona y cualquier persona es cada firma.

Su conversión en bien digital, radica en su elemento constitutivo de bien de información, intangible. La firma electrónica es un bien digital cuyo objeto es una situación jurídica subjetiva

135. Josh Fairfield, "BitProperty", Washington & Lee Public Legal Studies Research Paper Series, paper 2014-17, october 2, 2014.

esencial –situación existencial– tutelada por el ordenamiento jurídico, en cualquier y en todo momento de la vida de la persona. La circulación jurídica de la firma exige su control por el titular como manifestación primera de autodeterminación informativa y garantía de la intimidad.[136]

La firma digital es información en estado puro de la persona que la transforma en objeto de circulación de noticias, mensajes, en suma, dato personal a través de internet. Pero, aún más, la firma fija un perímetro de tutela del derecho de la persona y su intimidad y el ejercicio de la libertad patrimonial.

La principal característica que enseña la firma es que como bien digital no puede ser bien de información, no exclusivo ni excluyente. La firma es única y su uso impide que otro acceda a su ejercicio.

No parece, entonces, que la facultad de autodisposición sobre uno mismo, la propia vida singular y las relaciones que hacen a su vida(derecho a la intimidad) resulte ilegítimamente recortada por el interés general a evitar el blanqueo de capitales, la financiación del terrorismo, la criminalidad organizada o la evasión fiscal. No es menos cierto que la intimidad y la vida privada no pueden ponerse en cuestión si no hay un perjuicio justificado, convirtiendo en prohibido lo que es un medio de ejercicio de un derecho fundamental.

De esto derivan dos características típicas de *Bitcoin* que necesariamente deben explicarse en otro modo. Por un lado, el anonimato entre las partes firmantes y, por otra, la irrevocabilidad de la firma una vez celebrada su inserción registral o, lo que es lo mismo, la irreversibilidad del pago una vez convalidada la transacción.

El protocolo de Bitcoin impide la revocación del pago una vez confirmado, por razones de error o accidente, salvo la buena fe o disposición del perceptor, en una segunda transacción. Es una decisión estratégica del sistema porque tiende a simplificar el empleo de la plataforma tecnológica y, sobre todo, confirmar que

136. T.Rosembuj, Intercambio internacional de información tributaria, Barcelona, 2004, p.65.

la relación persona a persona no admite intermediarios centrales, de tipo bancario, cartas de crédito, financieros. La relación entre las partes es estrictamente bilateral, incluso en la equivocación y esto supone un compromiso y una garantía plena porque una vez validada, la transacción resultante es irreversible.

El anonimato es una crítica recurrente. El sentido es decididamente erróneo o equívoco. Se dice anónimo a aquello que supone la protección privada, íntima, de los datos personales, de la firma particular de cada persona, que lleva a cabo una transacción, económica o jurídica, con otra. Efectivamente, desaparece el deber de información personal al intermediario financiero usual; pero, esto ni implica en si mismo el enaltecimiento del juego anónimo, lo cual entraría en contradicción con la propia definición del sistema como una cadena pública de firmas digitales. No hay ruptura entre identificación personal y clave pública registrada en la cadena de bloques: la trazabilidad ocurre sea mediante el sitio web de la persona o en el intercambio de moneda de curso legal con moneda virtual.

Dicen *Brito-Castillo*: "Aunque *Bitcoin* es relatada como una moneda "anónima", en realidad, es muy difícil permanecer anónimo en la red de *Bitcoin*."[137] Los antecedentes de la transacción y sus efectos hacen que puede rastrearse o desvelarse la identidad del usuario, si hay motivo y ello porque, finalmente, cada transacción y la identidad encriptada de cada usuario queda inscripta en un registro público universal.Es lo que en la expresión anglosajona convierte anónimo en seudónimo.

¿Por que? Porque las operaciones no son en efectivo y siempre pueden rastrearse de una clave pública a otra. No es difícil, se afirma, con los instrumentos y medios adecuados traspasar el seudónimo. Alguna información puede capturarse por las referencias para individualizar, efectivamente, la identidad de los usuarios.[138]

---

137. J.Brito, A.Castillo, Bitcoin: a primer for policymakers, cit.: "Los seudónimos vinculados a las transacciones registradas en el registro público pueden identificarse años después que un intercambio se haya efectuado."Además, como se ha dicho, hay técnicas que permiten desvelar hasta el 40% de la identidad de los usuarios.

138. L.Pak Nian,D.LEE Kuo Chuen, Introduction to Bitcoin, cit., p.22,

No obstante, hay que evitar la confusión entre el anonimato (indeseable o riesgoso) y la intimidad.: "La privacidad es vital a la democracia. Es valiosa por propio derecho. Contribuye al "mercado de las ideas "y a la promoción de la verdad."[139]

En cambio, la *persona digital* no respeta, frecuentemente, ni el mercado de las ideas ni la promoción de la verdad. Todo lo nuestro es de conocimiento público, en manos públicas o privadas: en que gastamos el dinero, de que vivimos, cuanto ganamos y donde habitamos, cuales son nuestras ideas, religión, pensamientos.

Digamos que la reconstrucción ajena de nuestra persona, transformada en persona digital, al albur de la digitalización de fragmentos de datos, perfiles y bits, sea por dossiers digitales públicos o privados, crean una alarmante inseguridad y un cúmulo de consecuencias sobre nuestro comportamiento, que ignoramos. La persona digital es una burda aproximación a la persona. Es mérito de *Solove* reclamar que ello es producto de la ley, que no solo de la tecnología. "La protección de la intimidad en la Edad de la Información es una cuestión de diseño social."[140]

Precisamente, *Solove* destaca el valor social de la intimidad, porque la tutela individual interesa, sobre todo, a la sociedad, antes que al individuo. La intimidad no es una lucha de la persona contra los intereses sociales, sino la tutela del individuo en base a los propios valores de la sociedad."Así no puede pesarse como un derecho individual contra el más importante bien social.Las cuestiones de intimidad implican equilibrar los intereses sociales en ambos lados de la escala."[141]

La cadena de firmas digitales es un medio lícito de oscurecer la propia libertad patrimonial ante la intermediación financiera y el gobierno, dificultando su trazabilidad o localización; pero, que en un marco de regulación apropiada permite a la potestad administrativa encontrar el nexo, si lo necesita, con la identidad particular de las partes. No es nada más que una primera defensa

---

139. D.G.W.Birch, What does cryptocurrency mean for the new economy, p.511, en D.LEE Kuo Chuen, Handbook of Digital Currency, cit.

140. D.J.Solove, Digital Person.Technology and privacy in the Information Age. New York University Press, 2004, p.226.

141. D.J.Solove,"I´ve Got nothing to hide" and other misunderstandings of privacy, 2-7-2008, ssrn: 998565, p.763.

contra la interferencia en la esfera personal del individuo, que, como es obvio, no delata ilicitud sistemática. La metáfora del uso de seudónimo digital, que no de anónimo digital, no es del todo lejana a la descripción de la realidad virtual. Una forma extrema de defensa de la persona, de cada uno y su derecho esencial a que sus datos personales no se le escapen de las manos, sin su previo conocimiento y consentimiento.

## **8.2.** LA INFORMACIÓN Y LA INTIMIDAD

El bien digital, en general, tiene un claro componente de (bien) de información, de noticias, datos, que, son de uso general, no excluyente ni exclusivo. *Lehdonvirta-Castronova* acuñan la categoría de bienes digitales de información cuyo "valor se basa en la información que contiene"[142] y que tienden a ser bienes públicos, de fruición plural y donde el consumo de uno no impide el de otros (*non rival, non excludable).* Al mismo tiempo, les distinguen de los que denominan bienes virtuales, calificados por sus funciones, pero, sobre todo, porque carecen, en principio, de las características de exclusión y su uso disminuye la capacidad de disfrute de otros.

La apreciación puede aceptarse, pero requiere una particular atención cuando la referencia es al bien de información cuyo contenido es el dato personal y la transferencia de uno de sus atributos exclusivos y excluyentes cual es el derecho a la intimidad (*privacy).* El bien digital de información exclusivo y excluyente, no tanto por sus funciones, cuanto por la necesaria tutela al derecho fundamental a la protección de datos esenciales, por ejemplo, la firma digital. En suma, hay bienes digitales cuyo valor es la información, pero que reúnen atributos de los bienes virtuales.

El bien virtual de información, en la especie la firma digital, solo puede estar bajo control de su titular y no hay escisión posible entre el dato y la persona. La moneda virtual es un precipitado técnico de información e intimidad. El eje del dinero virtual es la

142. V.Ledhonvirta, E.Castronova, op.cit., p.41.

protección del dato personal de la firma digital. Sin firma digital, a ciegas, ilocalizable, no puede existir moneda virtual.

La firma digital es la información requerida para entrar en el sistema *Bitcoin* y pertenece a la persona, es única y forma parte de sus datos personales irrenunciables e indisponibles para ninguna otra persona. La firma es exclusiva y excluyente y así sucesivamente con las otras firmas.

El valor máximo de *Bitcoin* es la disposición y circulación jurídica de la firma digital. No deja de ser curioso que los datos personales que sirven de primera materia para los proveedores de bienes digitales, sin reconocimiento de ninguna clase; resultan, en lo específico, la condición esencial de funcionamiento de la moneda virtual.[143]

El ejercicio del derecho a la intimidad no es consecuencia de la propiedad. Es difícil referirse a la intimidad como una suerte de mercancía regulada por su valor de cambio en el mercado. La intimidad es parte del derecho fundamental de cada persona y, por tanto, está fuera de las normas del mercado. Esto en ningún caso impide que la información íntima, firma digital, puede estar en el tráfico jurídico; pero, no como mercancía, sino como expresión de la persona de autenticidad, de validación, de responsabilidad final por los actos de comercio que puede emprender. La mercificación de la firma llevaría al absurdo de mercificar a la persona por cualquiera de las determinaciones en sus relaciones en el mercado.

Por eso, las decisiones de la persona en la moneda virtual son irrevocables, fruto de su voluntad; y confidenciales (seudónimas) para amparar su privacidad. Lo que no significa que no deba distinguirse entre intimidad (firma), mercancía y moneda virtual.

## **8.3.** LA CRIPTOGRAFÍA COMO MONEDA

*Bitcoin* es un objeto criptográfico (*fixed-value cryptographic object o digital token),*representado por una cadena de firmas digitales, cuya información reparte y descentraliza como moneda

143. T.Rosembuj, El impuesto digital, cit., p.34.

fiduciaria virtual en forma segura y convalidable, respecto a los documentos en que se emplea; sin perjuicio, que otros documentos distintos de la moneda virtual puedan aprovechar su sistema criptográfico.[144]

Bitcoin es un bien digital fundado en la criptográfica asimétrica: se trata de un sistema basado en dos clave, público y secreto, en el cual dos partes pueden entablar una comunicación segura en un canal de comunicación no seguro sin compartir la clave secreta. El sistema, en palabras de sus creadores *M.Hellman y W.Diffie, en 1976,* emplea dos claves que están matematicamente relacionadas aunque el conocimiento de una de ellas no permite a cualquiera determinar fácilmente la otra clave. Una clave se usa *para* encriptar el texto y la otra para desencriptar el texto cifrado. No importa cual clave se aplica primero, sino que se requiere la aplicación de ambas. La clave pública puede comunicarse ampliamente cuanto su titular quiera. La clave secreta no es revelada nunca a la otra parte. La persona encripta datos, letras o números, usando la clave pública de otra. El receptor descifra el texto mediante su clave privada, el método permite la prueba del remitente del mensaje de datos, porque si la persona encripta con su clave privada; el receptor que lo descifra mediante la clave pública del remitente, puede tener la certeza de quien lo envía y éste nunca podrá desmentir que lo ha hecho(*non-repudiation)*

A ello se añade el uso de funciones *hash (message digest)* que aseguran la integridad de los archivos, para evitar la intrusión de terceros: algoritmos que impiden cualquier cambio en el contenido del mensaje porque trae como consecuencia que el receptor calcula un valor *hash* diferente que el colocado en la transmisión por el remitente y no es probable que dos mensajes diferentes compartan el mismo valor *hash.* [145]

La criptográfia asimétrica, en suma, se basa en dos claves matemáticamente relacionadas, en la que el conocimiento de una de

144. J.A.Kroll, I.C.Davey, E.W.Felten, The Economics of Bitcoins mining, or Bitcoin in the presence of adversaries, Princeton University, The Twelfth Workshop on the Economics of Information Security, (WEIS 2013), june-11-12-2013; E. Dourado, J. Brito, Cryptocurrency, The New Palgrave Dictionary of Economics, Online Edition, 2014, edited by S.N. Durlauf y L. E. Blume.

145. Gary C.Kessler, An overview of cryptografphy, 21, january, 2015.

las claves no permite conocer la otra clave. Una clave se usa para encriptar el mensaje de datos y la otra para descifrarlo. Una persona envía un mensaje de datos y lo encripta usando la clave pública del receptor. El receptor descifra el texto mediante su clave privada. Esto sirve para probar quien envía el mensaje. Si el ordenante encripta el mensaje con su clave privada; el receptor puede descifrar con la clave pública del ordenante, quien lo envía y así evitar que lo repudie o revoque.

En la firma digital uno cifra su mensaje de datos mediante su clave privada, mientras que el receptor usa la clave pública del remitente para descifrarlo .La irrevocabilidad o el no repudio del mensaje de datos se logra mediante el uso de la clave pública del remitente, mientras que éste emplea su clave privada para la firma digital.

Las firmas digitales usan la criptografía para transformar los mensajes en forma aparentemente inintelegibles y su posterior retorno a su forma original. Para ello se usa la criptografía de la clave pública que crea mediante algoritmos matemáticos dos claves relacionadas. Por una parte, la clave pública crea una forma digital o transforma los datos en formas aparentemente inintelegibles y la otra, la clave privada, verifica la firma digital o se emplea para que el mensaje vuelva a su forma original.[146]

Los criptosistemas asimétricos se basan en que el remitente y el receptor tienen dos claves criptadas cada uno de ellos. Una de las claves es pública, susceptible de hacerse pública sin restricciones – la clave pública en *Bitcoin* es una cadena de números y letras que consta de 33 dígitos. La otra clave es privada conocida solo por el que la emplea. El remitente del mensaje criptado usa la clave pública del receptor para que sea formalmente inintelegible y puede descifrarse solo por el receptor mediante el uso de su clave privada. El receptor es el único que puede retornar la forma del mensaje a su contenido original. Si el remitente usa su clave privada para encriptar un mensaje, solo podrá descifrarse mediante su clave pública. El receptor, entonces, tendrá la seguridad que el mensaje fue enviado por el remitente, porque ningún otro tiene

146. UNCITRAL Model Law on Electronic Signatures with Guide to Enactement 2001,cit. p.22

acceso a su clave privada. La clave privada equivale a la firma personal.[147]

La firma mediante clave privada ratifica que el mensaje originado está confirmado por el titular de la clave pública y, por tanto, que es un mensaje auténtico. La transmisión de *Bitcoins* implica que el ordenante firme el mensaje con su clave privada y comunique la clave pública del receptor. Así puede comprobarse que el contenido del mensaje viene de quien dice venir y su contenido es autenticable. La firma impide la alteración del mensaje una vez emitido.[148]

Si el diseño del sistema es correcto… "es virtualmente imposible derivar el conocimiento de la clave privada del conocimiento de la clave pública".[149]Esto es la importancia del derecho a la intimidad, respetado por la criptografía. Evidentemente, el límite es el orden público económico que hace inadmisible su abuso ilícito; pero, no puede ignorarse que si hay un valor a destacar de la firma digital es que el mensaje solo puede leerse por el remitente y el receptor.

El proceso UNCITRAL de firma digital ilustra, comparativamente, la equivalencia con la criptografía de *Bitcoin.*[150]

- El usuario origina o recibe un único par de claves.
- El firmante prepara un mensaje, por ejemplo en la forma de un pago de unidades de moneda virtual, en el ordenador.
- El firmante prepara un "resumen del mensaje" (*message digest)* aplicando una función *hash*, que impide la alteración o cambio.Si el resumen del mensaje enviado coincide con el que recibe la otra parte, éste podrá asegurarse que no existen modificaciones entre ambos resúmenes. La función del algoritmo *hash* sirve para transformar la información en un formato y tamaño fijo o, texto o números de ar-

147. B.Segendorf, What is bitcoin?, cit., p.74.

148. S.Gorjon, Divisas o Monedas virtuales. El caso Bitcoin, Dirección General e Operaciones, Mercados y Sistemas de Pago, Banco de España, enero 2014.

149. UNCITRAL, cit.p.23; P.Murck, Testimonio, Bitcoin Foundation, Homeland Security and Governmental Affairs Committee, November 18, 2013, p.4.

150. UNCITRAL, cit., p.31.

bitraria longitud en un número de longitud fija que impide que el contenido o extensión del mensaje de datos pueda recuperarse. Es lo que se denomina *digital fingerprints* del contenido del archivo, para impedir que pueda ser alterado, en tutela de la integridad del archivo.

- El firmante encripta el resúmen del mensaje con la clave privada, que utiliza un algoritmo matemático para su aplicación.
- El firmante adjunta su firma al mensaje.
- La parte receptora usa la clave pública del firmante para verificar su firma digital. La verificación asegura que el mensaje viene del firmante.
- El receptor crea un resúmen del mensaje usando la misma función *hash.*
- El receptor compara los dos resúmenes de mensaje para comprobar que sean idénticos y que no ha existido modificación del mismo después de su firma.

Es una moneda virtual o sea un bien digital que va más allá de la información porque la transferencia de valor tiene un fin exclusivo y excluyente de un recurso escaso entre los participantes; aun cuando, insisto, el valor de la intimidad da contenido al valor de la información igualmente importante. El valor de la moneda virtual no es otro que el de las firmas digitales. Al punto que su ausencia declara la inexistencia o irrelevancia del *digital cash* .Esta es una de las contribuciones originales de *Bitcoin.* La otra, a diferencia del Modelo UNCITRAL es la autocertificación, también criptográfica, de las operaciones entre firmas digitales: *Bitcoin,* asumiendo su herencia de la criptoanarquía, rechaza la certificación externa de su funcionamiento sea por autoridad pública o privada.

Si esto se acepta resulta que el nudo gordiano de la moneda virtual no es la criptografía asimétrica o su plena aceptación de la firma digital entre las partes; en el bien entendido que el derecho a la intimidad es un valor no de mercado digno de tutela. El verdadero conflicto está entre la autocertificación o la certificación externa de los servicios, donde el origen de *criptoanarquia de Bitcoin* aparece con toda intensidad.

## **8.4.** LA CERTIFICACIÓN DE SERVICIOS

UNCITRAL define el certificado como el mensaje de datos que confirma el nexo entre un firmante y la firma de los datos creados. El proveedor del servicio de certificación es una persona que emite certificados y puede suministrar otros servicios relativos a las firmas electrónicas.[151]

La verificación de la firma digital es el proceso de comprobación de la firma digital con referencia al mensaje original y una clave pública dada, determinando si la firma digital fue creada para el mismo mensaje usando la clave privada que corresponde a la clave pública de referencia.[152]

El software de verificación, alta tecnología matemática criptográfica, confirma la firma digital si la clave privada del firmante fue usada para firmar digitalmente el mensaje, que es el caso si la clave pública del firmante fue usada para verificar la firma porque la clave pública del firmante verificará solo una firma digital creada con la clave privada del firmante.[153]

El verificador necesita acceder a la clave pública del firmante para comprobar la firma digital y asegurarse que corresponda a la clave privada del firmante. "De cualquier modo, el par de claves pública y privada no tiene asociación intrínseca con ninguna persona: es simplemente un par de números."[154]

El proveedor del servicio de certificación es un tercero, público o privado, cuya función es asociar un firmante identificado con una clave pública específica. La actividad trata comprobar que el usuario de la clave pública se corresponde con el usuario de la clave privada y utiliza técnicas criptográficas fundadas.[155]

El proveedor del servicio de certificación emite un certificado que firma, que asocia el par de claves con un firmante. "La princi-

151. UNCITRAL, cit., art.2,b),e).
152. UNCITRAL, cit, (v) Verification of digital signature, par.43, p.24.
153. UNCITRAL, cit., par.44, p.24.
154. UNCITRAL, cit., par.45, p.25.
155. UNCITRAL, cit., par.50, p.26.

pal función de un certificado es vincular una clave pública con un firmante particular".[156]

La tecnología *Bitcoin,* basada en la criptografía asimétrica, el valor de la firma digital; rechaza la necesidad de confiar la certificación de los servicios a terceros. La convalidación del tráfico de firmas digitales, sea en valor monetario o documental, es cosa endógena de la comunidad de usuarios. En especial, depende del registro público distribuido. El nuevo paradigma está constituido por la cripto firma digital y el registro público. La Cadena de Bloques es una base de datos universal, con acceso abierto a todos los usuarios del sistema.

La Cadena de Bloques es una cadena de transacciones u operaciones, que pueden o no ser de índole monetaria, ya que cualquier acreditación documental es susceptible de transmitirse mediante mensaje de datos y firmas digitales. El registro público facilita que se pueda comprobar, en la moneda virtual, que los pagos no han sido duplicados o gastados en otra operación ignorada y recupera para cada transacción su memoria de modo que cada operación tiene su cronología (origen, desarrollo, perfeccionamiento), perfectamente visible y transparente.

Las transacciones son recogidas cada diez minutos por los mineros, cuya función específica es la verificación de la transacción y su añadido, si se cumplen los requisitos, como nuevo bloque a la Cadena de Bloques. La Cadena de Bloques contiene la historia, la cronología, de todas las transmisiones ocurridas, desde el propio inicio hasta el momento actual. Cualquiera de las transacciones realizadas exhibe su origen, creación de moneda, y su seguimiento aparece reflejado en el registro público distribuido.

El descubrimiento y convalidación de los nuevos bloques es una tarea que corresponde a los mineros. Cualquier usuario puede llegar a serlo, pero, en la práctica, es necesaria una potencia informática, de energía, de tiempo, que seleccionan, la calificación entre algunos de la red, que no todos. Los mineros garantizan la emisión de *Bitcoin* resolviendo problemas matemáticos complejos

156. UNCITRAL, cit, par.53, 54, p.27, 28.

(*proof-of-the-work)* de simple comprobación, una vez resueltos (*hash function).*[157]

El descubrimiento del *hash* permite añadir el nuevo bloque. Es la prueba de trabajo del sistema. Todos los nodos aceptan el bloque si todas las transacciones son válidas y los *Bitcoins* no han sido ya gastados.[158]

No hay certificaciones por terceros; sino que el trabajo se distribuye entre los usuarios, algunos de los que desempeñan el papel de mineros.

Los mineros reciben una recompensa por el hallazgo del nuevo bloque. Originariamente la recompensa era de 50 bitcoins, pero, se reduce a la mitad aproximadamente cada cuatro años. Ordinariamente es de 25.El proceso replica el agotamiento en la extracción del oro. Además, reciben contraprestaciones por la verificación de las operaciones en la red. La minería tiene 2140 como fecha de extinción.

## RECAPITULACIÓN

*Nakamoto*, en su seminal trabajo, define *Bitcoin como una cadena de firmas digitales*. Una serie de bits y bytes de firmas, persona a persona, convalidables en un registro público descentralizado y global, cuyos efectos son mensajes de datos de transferencia de valor, sin intermediación financiera ni autoridad bancaria central.

La firma es un bien de información digital, pero excluyente y exclusivo. La genialidad de *Nakamoto* es que la cadena de firmas digitales condena a la moneda virtual, a *Bitcoin,* al ámbito de la protección de datos, el derecho a la intimidad y la libertad patrimonial del individuo, sin perjuicio de la interferencia pública que impida su abuso, los actos ilícitos o la criminalidad organizada. En

157. La *hash* function convierte la longitud de un texto o número arbitrario en un número de longitud determinada. Bitcoin usa Hashcash SHA256, que transforma el mensaje en un resumen de 256-bit-. La importancia del *hash* es que impide la adulteración, aunque mínima de los mensajes de datos y que sean invenciones.

158. Nakamoto, cit., p.3

suma, condena a la moneda virtual a ser una prolongación digital de la persona.

El bien virtual de información, en la especie la firma digital, solo puede estar bajo control de su titular y no hay escisión posible entre el dato y la persona. La moneda virtual es un precipitado técnico de información e intimidad. El eje del dinero virtual es la protección del dato personal de la firma digital. Sin firma digital, a ciegas, ilocalizable, no puede existir moneda virtual. Por tanto, si bien es cierto que el bien virtual califica la exclusión, por valor de mercado; es más importante la exclusión por el valor no de mercado. Precisamente, la intimidad.

La criptografía asimétrica consiente que la intimidad quede fuera del mercado, del mensaje de datos, del comercio de la moneda virtual.

La criptomoneda virtual supone una moneda independiente del Estado y del sistema bancario y financiero, cuya fuente es la criptografía asimétrica. Las firmas digitales son el contenido fiduciario de la moneda: no hay ningún otro valor intrínseco de la moneda virtual que las firmas digitales. El oro de la moneda virtual deriva exclusivamente de la confianza entre las partes y la seguridad de su realización, sin terceras partes, solo en base al establecimiento del protocolo criptográfico.

La tecnología *Bitcoin,* basada en la criptografía asimétrica, el valor de la firma digital; rechaza la necesidad de confiar la certificación de los servicios a terceros. La convalidación del tráfico de firmas digitales, sea en valor monetario o documental, es cosa endógena de la comunidad de usuarios. En especial, depende del registro público distribuido. El nuevo paradigma está constituido por la cripto firma digital y el registro público. La Cadena de Bloques es una base de datos universal, con acceso abierto a todos los usuarios del sistema. La innovación es esencial porque, de su arquitectura, resultan expulsados los terceros intermediarios, dado que la confianza está en el funcionamiento del propio sistema, sin que sea necesaria la acreditación o certificación desde fuera de los actos, contratos, transacciones celebradas entre las partes.

El tráfico o circulación la propiedad digital encuentra su encauzamiento más allá de la moneda virtual.

El desarrollo de la tecnología de la Cadena de Bloques va más allá de la moneda virtual. Podría servir para la gestión documental, civil, mercantil, penal, fiscal, ejercicio del derecho de voto, identificación y antecedentes personales. No solo una plataforma para la creación de criptomoneda, sino una plataforma para el "*cripto derecho*".[159]

La idea de los *smart contracts* entiende que la Cadena de Bloques puede ser útil para complementar o sustituir partes enteras del orden jurídico, aquellas que necesitan de una tercera parte para su convalidación. En lugar de incumplimiento de contrato que debe ejecutarse mediante acto judicial; puede pensarse en obligaciones automatizadas por el software, verificadas por la Cadena descentralizada de Bloques o, la *smart property* que implica la transmisión de cualquier forma de propiedad.[160]

## 9. BitProperty. La propiedad digital como protocolo de información

Cualquier dato que pueda digitalizarse –codificarse como una cadena de bits- es información. El bien digital es un intangible de información, de goce plural, sin que la satisfacción singular impida la contemporánea satisfacción de los otros.[161]El bien digital virtual añade a su calificación la restricción de la escasez, de donde resulta que la exclusión comparece junto a la pura información.[162]Asimismo, hay bien digital con atributo virtual, como ya se dijo sobre la firma digital. La reproducción infinita de la copia, característica del bien digital, debe cohabitar, de algún modo, con procedimientos que impidan su devaluación automática. Si uno puede duplicar el bien digital o gastar dos o más veces la misma unidad de moneda virtual amenaza su supervivencia. La

159. G.Wood, A.Buchanan, Advancing Egalitarianism, en D.LEE Kuo Chuen, Handbook of Digital Currency, cit., p.400…" Esto se implementa distribuyendo a todos una copia de toda la información en el sistema y usando criptografía para proveer una via para ser abierta y privada, rompiendo la contradicción prima facie."

160. P.Vigna, M.J.Casey, The Age of Cryptocurrency.How Bitcoin and Digital Money are challenging the Global Economic Order, New York, 2015,p.224.

161. T.Rosembuj,El impuesto digital,cit.,p.27

162. V.Lehdonvirta, E.Castronova, Virtual economies, cit., p.44.

duplicación y el doble gasto son fenómenos que afronta la tecnología *Bitcoin,* en forma descentralizada y distribuida entre los usuarios, sin intermediarios que actúen como garantes del sistema.

*Fairfield* se interroga sobre la actuación de la propiedad en el ámbito digital y virtual. Su punto de partida es que la propiedad es un procedimiento, antes que un conjunto de atributos o una finalidad. La propiedad, para este autor, es un procedimiento para comunicar información sobre la relación de una identidad a un recurso. La propiedad es un protocolo de comunicación e información y almacenamiento: "La identidad personal no es el corazón de la propiedad. Los activos no son el corazón de la propiedad…En cambio, los datos consistentes en *quien* debe adoptar *cual acción* con respecto a *que activo* y los procedimientos para comunicar y cambiar los datos, llega al hueso. Cuando a una transacción sigue otra, formando una cadena de titularidad, creamos una cadena de datos relativos a cada transacción respecto a la próxima. El sistema de propiedad reside en los procedimientos de seguimiento, transmisión y verificación de esa información. Si un sistema persigue habilitar las transmisiones, lo hace por el transporte de la información respecto a quien ahora es propietario de que."[163]

No puede ignorarse que *Fairfield*, que en el mismo ensayo, cultiva las excelencias técnicas del registro público universal y la cadena de bloques de *Bitcoin,* termina por extender esa lógica al sistema de propiedad digital. La información es el vehículo que ofrece sustancia al sistema de propiedad, porque la cadena previa, actual y posterior, de la transacción permite individualizar al titular del dominio del bien que es su objeto. La propiedad es un sistema de información, antes que uno sobre cosas o mercancías, activos, identidad personal o derechos de uso.

La información es propiedad y se traduce en protocolos que establecen el formato de los datos, los procedimientos para comprobar y corregir errores en la recepción de los datos y procedimientos para el almacenamiento seguro de los datos para su retransmisión una vez recibidos.

"En lugar de tratar la identidad del propietario, los atributos del objeto o la naturaleza de la relación que el individuo sostie-

163. J. Fairfield, The BitProperty, cit., p.54.

ne sobre el activo como el nucleo de la teoría de la propiedad; el protocolo simplemente fija como cada uno debería formatear, transferir, comunicar, actualizar, verificar, almacenar y asegurar esa información."[164]

Primero, el sistema de propiedad y el sistema de información son fungibles, son equivalentes. La información permea la institución de la propiedad, antes que sus efectos tradicionales, en modo que no hay propiedad sin información.

Segundo, la información indica el verdadero propietario, solo enmendado por la emergencia de mejor información, mejores datos, que lo altere. El flujo de información se propaga como "olas en un lago, desde el punto de origen".[165]

Tercero, la propiedad digital es una categoría de información .El hecho que un bien digital sea exclusivo o escaso supone información crítica. Pero, obviamente, hay información que no cuenta con la exclusividad o escasez para construir derechos de propiedad digital. Por un lado, no debe extenderse el sistema de propiedad intelectual sobre bienes digitales que no sean exclusivos ni escasos. Por otro, no resulta eficaz aplicar reglas de propiedad tradicional a recursos digitales que son exclusivos o escasos.

Cualquier bien digital, desde un *e-book* hasta música, aplicaciones, películas, está controlado por el registro central de los proveedores de los servicios: no es un registro descentralizado y distribuido, público para todos, lo cual termina por estimular la duplicación.

## **9.1.** LA CRIPTOPROPIEDAD

La criptografía asimétrica y el registro público universal encauzan el discurso de la firma digital como fuente de derecho de la propiedad digital. La firma digital, personal, única, inseparable, intransmisible, es el elemento esencial de la circulación civil, mercantil, penal, fiscal y financiera en el ciberespacio. La construcción jurídica de la moneda virtual, por ejemplo, no puede des-

164. J.Fairfield, The BitProperty, cit.p.62.
165. J.Fairfield,The BitProperty, cit. p.70

pegarse del tráfico de la firma digital, del tráfico de la intimidad de la persona, del tráfico del valor patrimonial o documental del acto, contrato, negocio jurídico, puesto en práctica.

La firma digital, la clave pública y la clave secreta, es una expresión de cada persona. Al principio y al final del circuito hay una persona. La dirección, billetero o identidad sirven para hacer mención a que no puede existir firma sin persona que sea su titular y a través de su reconocimiento ponga en marcha su voluntad de acto o hecho jurídico digital.

La firma digital es única, no hay matemáticamente, dos iguales: es el equivalente de la huella digital. Cada persona solo es titular de una y no más firmas.

La firma digital es inseparable de su titular, una manifestación del derecho de personalidad, como el nombre, en cuya virtud no es exagerado elevarla a derecho esencial, sobre todo, porque su disciplina ciberjurídica no puede alejarse de la importancia que le concede la criptografía asimétrica.

La firma digital, por último, es intransmisible, sustraída a la libre disposición del titular, irrenunciable e imprescriptible y, particularmente, enlazada al derecho a la propia intimidad, extramercado y extrapatrimonial.

La moneda virtual es un bien de información del titular. Por tanto, reúne las primeras calificaciones de bien digital; pero, asimismo, del bien virtual enrocado en el derecho de propiedad, con características propias relativas a su carácter exclusivo y excluyente y su escasez.

"Cuando los bitcoins son transferidos desde A a B, nada resulta materialmente transferido, entre sus billeteros; en cambio, una cantidad de bitcoins que previamente estaban asociados con la dirección pública de A en el registro ahora pasan a ser asociadas con la dirección pública de B. A anuncia esta transmisión a todos los nodos en la red de *Bitcoin,* no solo a B, de modo que la red pueda colectivamente validarla a través del proceso de los mineros y queda así recogida dentro de la Cadena de Bloques". [166]

166. I.Mas, D.LEE Kuo Chuen, Bitcoin-Like Protocols and Innovations, en Handbook of Digital Currency, cit., p.423; J.Fairfield, The BitProperty, cit., p.30... *"El trans-*

La formalización de la propiedad sucede, entonces, en cadena de firmas digitales, asociando un importe de moneda virtual o documentos a una dirección, billetero o clave pública en el registro que queda asociada a otra dirección, billetero o clave pública, que se comunica a todos los usuarios de la red, para su convalidación por los mineros, previa a su inscripción en la Cadena de Bloques.

El tráfico mediante moneda virtual exime al derecho a la intimidad de la persona, usuaria de la clave secreta, que permanece voluntariamente en una discreta segunda línea. Las claves, pública y privada, están vinculadas matemáticamente; pero, es imposible deducir la clave privada de la dirección o billetero de *Bitcoin* .La clave pública sirve para comprobar las firmas digitales en las transacciones, mientras que la clave privada es la firma en sentido auténtico –la que tutela su intimidad-, que permite que se materialicen las firmas digitales. O lo que es lo mismo, sin firma privada no hay compromiso personal y solo puede existir dicho compromiso con la tutela de la privacidad, como derecho esencial de la personalidad.

## **9.2.** LA PERMUTA O TRUEQUE

La permuta es un contrato "por el cual cada uno de los contratantes se obliga a dar una cosa para recibir otra" (art. 1538 Codigo Civil).No se entrega dinero (precio) por una cosa, sino una cosa por otra. La permuta, se dice, es una fórmula de cambio directo o de cosa por cosa. El *barter* es el equivalente de la permuta en el derecho anglosajón: el cambio de una cosa por otra *sin el uso de dinero.*

El difícil encaje jurídico de *Bitcoin* impulsa determinado tipo de conclusiones que, a la postre, son insostenibles. No puede afirmarse que la transacción en base a moneda virtual significa permuta, trueque o *barter,* de cosa por cosa, sin dinero de por medio. Al contrario, negando la premisa mayor se termina por crear una confusión insuperable. La permuta o trueque es cambio directo, de cosa por cosa, sin dinero. Aquí hay dinero, digital o virtual,

---

*mitente* meramente *transfiere la unidad transfiriendo la entrada al registro."*

que es precio de compra o venta, de pago o de cobro, de cambio por moneda legal, o de inversión. Es una moneda, sin fuerza legal ni obligatoria, pero, cuyas funciones no sirven al cambio por otra cosa. O sea, no se entrega la cosa *Bitcoin* por otra.

Primero, el usuario de la red puede conseguir *Bitcoin* por la venta de bienes o servicios, como cuando un comerciante los acepta del comprador por la venta de su producto.[167]

Segundo, el usuario puede cambiar moneda legal (dólar, euro, yen) por *Bitcoin,* pagando una comisión al cambista o, a la inversa, puede cambiar moneda digital o virtual por moneda legal. Hay un mercado que fija el precio de cambio de *Bitcoin,* aún aceptando su elevada volatilidad, que comporta imprevistas apreciaciones o depreciaciones de valor.

Tercero, la creación de *Bitcoin* ocurre mediante *mining,* proceso criptográfico completamente ajeno a la transacción que sirve para convalidar. La oferta de *Bitcoin* crece en la cuantía de 50 cada diez minutos. El número se reduce a la mitad cada cuatro años. En 2140, la emisión de *Bitcoin* se cierra en 21 millones. Ahora, se crean 25 cada diez minutos.

No convence, tampoco, establecer como permuta la retribución a los mineros en "dinero no legal y eventual medio de pago (*Bitcoin).* Entender que la moneda es una cosa a cambio de otra altera la función del minero en el sistema: la retribución es una contraprestación por su prestación a la resolución del problema matemático complejo que permite convalidar la transacción propuesta entre las partes. Y cuya naturaleza o es ganancia de capital (nueva riqueza que viene de la nada con la creación de nueva moneda) o es comisión, si no obtiene moneda virtual a cambio. El minero es un comprobador calificado, cuyo cobro en moneda virtual es ganancia de capital o, en su caso, compensación de servicios, si no la recibe.[168]

Cuarto, la versatilidad de *Bitcoin* permite su difusión como moneda de curso legal, en el sentido que su aplicación es univer-

---

167. C.K.Elwell, M.M.Murphy, M.V.Seitzinger, Bitcoin: questions, answers and analysis of legal issues, cit., p.2.

168. C.Gomez Jimenez, El bitcoin y su tributación, Contabilidad y Tributación, 380, noviembre 2014, p.93.

sal, a cualquier tipo de bien o servicio, previo consenso de la otra parte. Una persona puede pagar su alquiler o comprar alimentos con *Bitcoin*, en la idea de su previa aceptación.[169]

## RECAPITULACIÓN

La conclusión general de *Fairfield* es que los registros públicos universales, públicos, en la línea *Bitcoin (trustless technologies)* proponen a la creación y seguimiento de cualquier clase de derechos con certeza y seguridad, sin centralidad ni intermediación, sea para la moneda virtual, como para los intereses hipotecarios, títulos valores, propiedad de acciones o cualquier forma de propiedad digital. Propiedad es información: quien es el propietario de que.

La fuente de la propiedad digital, de la criptopropiedad digital, es la información, representada por las firmas digitales, cuya extensión matemática adecuada consigue constituir y movilizar el valor, económico y no económico, derivado de su aplicación. La moneda virtual, primero es la firma digital y después su valor económico como consecuencia de la aceptación y convalidación en el registro público distribuido entre los usuarios.

El tráfico jurídico debe preservar la tutela de la intimidad, corporizada en la clave secreta, verdadero derecho de la persona, y encauzar a su través los actos o contratos, los negocios jurídicos de disposición económica que el titular pretende celebrar: si es moneda, será la creación de bitcoins , el intercambio con otras monedas legales o virtuales, la adquisición de bienes o servicios, la inversión o el ahorro; y no siéndolo, a la perfección de cualquier documento, prescindiendo de terceras partes, en un sistema matemático de convalidación.

La arquitectura de la permuta o *barter* resiste solo y en cuanto se rehuse la calificación de moneda virtual, moneda alternativa a la moneda legal, pero, sobre todo, moneda. El concepto se debilita y desaparece desde el momento en que progresa el reconocimiento

169. P.McLeod, Taxing and regulating Bitcoin: the governments game of catch up, CommLaw Conspectus, Vol 22,2014.p.389.

a la autonomía del concepto de la moneda digital. La moneda no es cosa que se cambie por otra, sino un medio de pago, de unidad de cuenta, de inversión, sea con fuerza legal o con fuerza real.[170]

El IRS extiende los principios de la permuta o *barter,* a la moneda virtual.[171]

El *barter*, intercambio de bienes o servicios, sin dinero, no resulta fácilmente adaptable al sistema *Bitcoin*; pero, sobre todo, pese a lo que se diga en contrario, porque es una moneda que hace las veces de dinero, aunque no sea moneda legal de fuerza obligatoria. Puede discutirse si el dinero *Bitcoin* equivale al dinero en efectivo; pero, no puede discutirse, a esta altura, que se trata de dinero privado digital, que permite la transmisión de valor sin intermediación financiera.

La disposición de moneda virtual, sin carácter empresarial, se conjuga mejor en la categoría de disposición de propiedad digital, criptopropiedad, que sirve de fuente a ganancias o pérdidas de capital: disposición con renta o disposición sin renta.

## 10. Calificación jurídica. El bien digital y virtual

La datización (*datification*) es de la esencia digital, sin datos no hay algoritmo y sin algoritmo difícilmente se puede hablar de bien digital. El valor de los datos reside en su infinita reutilización. El primer dato personal digitalizado, convertido en una cadena de bits, es susceptible de eternidad, de reiteración, repetición, aplicación continua y sistemática y es un dato que pertenece a alguno que, desde ese momento pierde o puede perder la huella de su identidad primera**.**

---

170. C.R.Baros, Barter, Bearer and Bitcoin, The likely future of steless virtual money, University of Miami Business L.rev, 201,2014: "Sin embargo, los usuarios y compañias aceptan pagos en Bitcoin por bienes y servicios, significando que aunque no sea oficialmente calificada como una moneda, todavía, funcionalmente opera como una moneda.", p.220.

171. Internal Revenue Service, Internal Revenue Bulletin 2014-16, april 14 2014, Notice 2014-21, IRS Virtual Currency Guidance.

La trascendencia de los datos, por pequeños o incidentales que sean, propone una cadena de valor en la que el protagonista es el consumidor final. La interacción digital y datos pueden ser del mayor peligro para la persona.

La identidad prestada contribuye a la creación de la *persona digital,* que se reconstruye a fragmentos, por piezas de las verdadera persona y que, como bien dice *Rodotá,* amenaza que la identidad de la persona sea contruida por los otros: identidad hipotética e incluso distorsiva, o sea el menoscabo de la autodeterminación informativa de la persona al uso o recorrido de sus derechos fundamentales a sus datos personales, íntimos, privados**.**[172]

El bien digital emerge de la recogida, transmisión, almacenamiento de los datos personales. El bien digital, en su estado puro, es información, al que puede accederse en modo remoto, sin intervención humana y cuyo contenido es universal: todo número y letra transmitida electrónicamente es apto de digitalización (sonido, imagen, datos, hechos, software).

*Bitcoin* es un bien digital, con particularidad virtual, admitiendo que tiene el acento en la exclusión y en la escasez. La moneda virtual encarna y representa la propiedad digital. Pero, al mismo tiempo, contando como elemento diferenciador la tutela del derecho a la intimidad, la tutela última del dato personal, la difusión de un valor *extrapatrimonial* en el mercado. La moneda virtual es propiedad digital limitada en su tráfico por la privacidad, o, lo que es lo mismo, por la firma digital. No es paradógico que la tutela de los datos personales sea mejor garantizada en el sistema de la moneda virtual, que en el sistema institucional, financiero, asegurador, bancario.

No puede ser una mercancía plenamente comercializable en el mercado ni, tampoco, un bien digital de uso plural o múltiple. Lo primero, porque no es estrictamente una mercancía y la intimidad, la firma digital, no es comercializable. Lo segundo, porque es una manifestación de propiedad digital exclusiva y excluyente.[173]

---

172. T.Rosembuj, El impuesto digital, cit.p.34.
173. T.Rosembuj, El impuesto digital, cit., p. 43,52.

La moneda virtual se acomoda a la calificación de bien digital: producto codificado digitalmente y transmitido electrónicamente por Internet o red análoga.

La primera diferencia es que no se trata de un bien digital ordinario –programa de software, texto, video, imágenes, grabaciones de sonido–, sino un servicio de firma digital creada para transferir entre las partes valor mercantil o no mercantil, monetario o no monetario, mediante la transmisión electrónica criptográfica; al amparo del derecho a la intimidad.

La segunda diferencia es que es moneda fiduciaria cuyo valor depende de la recíproca aceptación entre las partes como unidad de cuenta, medio de pago o de ahorro o inversión. Un servicio digital que reposa en la confianza y seguridad de los protocolos de software libre y abierto.

La tercera diferencia, apuntada por *Vigna, Casey,* apareja la captura de la información de las manos de los monopolios financieros y "crea una mecanismo descentralizado para que la sociedad juzgue la validez de esa información."[174]

Hay información que forma parte de cada persona y que no corresponde ceder a organizaciones de datos personales que extraen de su uso una utilidad infinita, sin que su titular lo sepa o aunque lo sepa no puede hacer nada por evitarlo. La persona digital no es la persona y el derecho a la intimidad es de la persona.

## **10.1.** MERCANCIA DIGITAL. HÍBRIDOS FINANCIEROS Y SINTÉTICOS

La mercancía digital no sigue el mismo itinerario que la mercancía ordinaria: la diferencia es que la mercancía es, por definición, física y material. Pero, no obstante, el bien digital o virtual, la cadena de bits o firmas digitales, concurre en el concepto de mercancía en cuanto su carácter de artículo de comercio: la mercancía es un bien que se vende en el mercado de calidad uniforme y valor universal. No obstante, sería simplificador, entender que

174. P.Vigna, M.J.Casey, op.cit.p.310.

mercancía digital excluye su calificación como moneda, y se reduce al software. El bien digital, la mercancía digital es un bien digital, es más que el software, que siendo esencial es solo uno de sus elementos componentes.[175]

Como cualquier otra mercancía tradicional –afirma *Kaplanov-,* la moneda claramente se coloca como bien de calidad uniforme dado que no importa el dólar negociado puesto que su valor está vinculado a su poder de compra y no a la calidad del papel o la tinta.[176]

*Bergstra y Weijland* clasifican *Bitcoin* como un tipo de mercancía informacional como moneda.[177]

La premisa es la referencia a *Bitcoin* en términos de mercancía, en particular, una mercancía cuya substancia es la información. La información privada que es propiedad de la persona. O sea, la intimidad. Los datos personales orientan la mercancía informacional. La intimidad (privacy) indica que esas mercancías deben ser propiedad de un propietario con el efecto que todas las formas de acceso de los no propietarios son una quiebra de los derechos que el propietario goza en virtud de su propiedad. El uso de la mercancía informacional se justifica porque hay un mercado para tal información, aún si la privacidad pretende regular y constreñir ese mercado.[178]

La mercancía informacional, cuyo contenido es la intimidad, significa su aptitud para ser regulada por las leyes del mercado, donde pueden ser objeto de intercambio por dinero. La clave para considerar una casi moneda a *Bitcoin* reside en ser ese tipo de mercancía informacional regulada por las fuerzas del mercado que disponen su valor de cambio.

La intimidad o privacidad se manifiesta en la firma digital y es un valor que está fuera del mercado o limitado jurídicamente en su

175. N.M.Kaplanov. Nerdy Money: Bitcoin, the private digital currency, and the case against its regulation, ssrn.com 2115203, p.27; A.Bal, Stateless virtual money inthe tax system, European Taxation, july 2013, p.353.

176. N.M.Kaplanov,cit.,p.27

177. J.A.Bergstra, P.Weijland, Bitcoin: a money-like informational commodity, Informatics Institute, University of Amsterdam, february 20, 2014.

178. Bergstra, Weijland, cit. p.16.

ámbito. Es cierto que la sustancia de *Bitcoin* es la intimidad; pero, no lo es menos que la clave privada es la que autoriza el gasto del dinero. La firma digital permite a los otros que el gasto en dinero ocurre con la autorización del propietario o titular de la clave privada. La transferencia de bitcoins supone un mensaje de datos que contiene la clave pública de la otra parte y el remitente firma con su clave privada, sin referencia a su identificación personal que permanece en el ámbito de la privacidad. La autorización de la transacción con la clave privada se transmite al conjunto de la comunidad en red.

Bitcoin es un bien digital o virtual, intangible, de aplicación uniforme y valor de mercado, cuyo elemento destacado es la propiedad de la información personal extramercado. Esto significa que la tutela de la firma digital está construida para evitar o restringir la invasión de terceros en la identidad de las personas, que lo emplean en el mercado.

"El público puede ver a alguno mandando una cantidad a otro, pero sin información que vincule la transacción a ninguno"[179]

Por tanto, si esto fuera cierto, *Bitcoin es* moneda virtual creada y tutelada por la criptografía y que se perfecciona en la firma digital. El respaldo oro de la moneda virtual es la matemática y la confianza que la gente deposita en el sistema. La fuente de *Bitcoin* es la constatación criptográfica de las firmas digitales, en particular la clave pública y la clave privada, certificadas en la cadena de bloques públicos y universales. [180]

La clave privada, inseparable de la clave pública, exhibe una componente ideológica totalmente intransferible e incomparable con el dinero electrónico o, inclusive con el dinero efectivo: su función es la protección de la persona, de su intimidad, de su derecho a que le ignoren.

---

179. Nakamoto, cit., nota 20.

180. B.Akins, J.L.Chapman, J.M.Gordon, A Whole New World: Income tax considerations of the bitcoin economy, Pittsburgh Tax review, 2015. "A diferencia de la clave pública, la clave privada está oculta y es solo conocida por el poseedor. La clave privada es usada para autorizar la transacción tanto para el remitente como para el receptor. La transacción es firmada con la clave privada del remitente, la cual no está incluida en la, cadena pública y permanece anónima…La autorización de la transacción mediante la clave privada permite su distribución a toda la red persona-a-persona".

Podría decirse que esto también se comparte con el dinero efectivo, pero, no es cierto, porque, en todo caso, el efectivo puede identificar la vocación de anonimato de la transacción y de las partes, pero, sometido a su hipotética trazabilidad concreta y, sobre todo, a la ausencia de cualquier compromiso ideológico con el derecho a la intimidad.

El rasgo que transforma la criptomoneda en algo más que bien digital es no solo la transferencia de valor o, en su caso, de documentos; sino la preservación matemática del secreto de la firma digital, secreto de la persona que es libre de hacerla pública o no; pero, que el sistema no le exige hacerlo.

Es la firma ciega de *Chaum.*

El punto delicado es la financiarización de *Bitcoin* que puede arrojar efectos opuestos al sistema, sus objetivos y caer preso, precisamente, de la intermediación financiera, que pretende evitar.

*Andy Yee* formula algunas sugerencias sobre la arquitectura de regulación de *Bitcoin*, por él denominado el *Internet del dinero,* dignas de ser tomadas en cuentas.[181]

El objetivo de la disciplina legal deben ser los intermediarios que conectan la comunidad técnica con la economía real. Y que permiten el acceso del público a las aplicaciones de la moneda virtual, v, g, servicios a no mineros de cambio entre bitcoins y monedas reales o servicios de dirección o billetero y de garantía que permitan el almacenamiento de moneda virtual en forma segura.

Los reguladores financieros tradicionales están mal preparados para entender la arquitectura de Internet y actúan en base a sus propios prejuicios culturales, organizativos y prácticos: *"Esto es complicado por el hecho que Bitcoin no encaja con las definiciones legales existentes de moneda, mercancía o red de pago."*

Las definiciones legales actuales comprometen su aplicación a la moneda virtual. De la mercancía digital se pretende el servicio a los derivados financieros, más o menos, en los mismos términos

181. A.Yee, Internet architecture and the layers principle: conceptual framework for regulating Bitcoin, 2014, Internet Policy Review, 3(3)DOI:10.14763/2014.2.289.

que los aplicados a los híbridos financieros y sintéticos dominantes en el sector financiero.

La aproximación del bien digital a la mercancía digital provee argumentos a los que defienden la semejanza entre cualquier mercancía, sea cual sea su configuración, y la moneda virtual como activo subyacente de derivados –swaps, futuros, opciones- atraídos por la regulación sectorial que les atiende, v.g. *U.S. Commodity Future Trades Commission.* Hay mercancías agrícolas, metales, energía, títulos del Tesoro, índices de tasas de interés, índices de mercados bursátiles, monedas, electricidad.

Así se afirma que *Bitcoin* es una mercancía digital escasa que cae dentro de la definición legal americana de mercancía. El sistema es más que una moneda digital o un mecanismo de pago. La segunda ola de *Bitcoin* atañe a los *smarts contracts*, instrumentos financieros, derivados y títulos.[182]

El uso de derivados puede contribuir a limitar los riesgos de la volatilidad para los comerciantes y cambistas de moneda virtual y, por otra parte, el sistema de registro público distribuido universal podría servir eficientemente a los mercados financieros.

La CFTC no es ajena a considerar los derivados de *Bitcoin* como mercancía digital. Primero recoge la demanda de los comerciantes para limitar sus riesgos por las fluctuaciones de la moneda virtual. Segundo, que la tecnología de pago de *Bitcoin* puede ser útil a los mercados de derivados y otros servicios de confianza. Sin embargo, asegura su voluntad de vigilancia en la integridad de los mercados, para impedir la manipulación y el fraude.[183]

*Bitcoin* como activo subyacente en las operaciones con instrumentos financieros, swaps, futuros, opciones, supondría un impulso determinante para que la mercancía digital denominada fuera la propia moneda virtual y, por tanto, caerían gran parte de los

182. H.B.Shadab, Regulating Bitcoin and Block Chain Derivatives, Commodity Futures Trading Commission Global Markets Advisory Committee Digital Currency Introduction-Bitcoin, October, 9,2014; J.Brito, H.Shadab, A.Castillo, Bitcoin Financial Regulation: Securities, Derivatives, Prediction Markets and Gambling, The Columbia Science & Technology Law review, V.XVI, 2014.

183. Commissioner M.Wetgen, The Global Markets Advisory Committee Open Meeting, 9.10.2014; Chairman Timothy G.Massad before the US house Committee on Agriculture, Washington DC, february 12, 2015.CFTC.

prejuicios existentes como moneda en su contra. La criptomoneda no es oro ni tiene respaldo legal o público alguno, por tanto, su mero reconocimiento como activo subyacente no puede ser sino a título de moneda virtual.

El problema, en todo caso, implicaría la propia configuración de los derivados financieros virtuales, puesto que la crisis financiera de 2008 enseña que los instrumentos financieros estuvieron tendencialmente orientados a crear más incertidumbre que estabilidad.

Si la filosofía *Bitcoin* pretende la desafortunada réplica de los derivados financieros, sea en orden a la especulación sobre los precios cuanto a la inversión a corto en *Bitcoin* sin su disposición **real, sin la disposición efectiva por obra de las firmas digitales del usuario**, ya puede anticiparse el fracaso. En verdad, los derivados financieros son una bomba de profundidad, porque, por otra parte, incurrirán en titulización , esta vez anónima, con lo cual se pierde uno sino el principal de los atributos de la moneda virtual, cual es la legítima defensa del derecho a la intimidad. Nada hace suponer que los híbridos sintéticos o financieros basados en la moneda virtual sean distintos a los que se utilizaron y utilizan actualmente. Por tanto, serían objeto de interés institucional de la intermediación financiera, bancaria, aseguradora convencional, empleando los mismos instrumentos, *Special Purpose Vehicles,* y jurisdicciones fiscales no cooperativas. (No es casual que las primeras propuestas lleguen de Chipre, las Islas Vírgenes, Gibraltar, Hong Kong, Singapur).

Los derivados digitales, precisamente porque lo son, no pueden sujetarse a las mismas reglas que los derivados financieros conocidos y los agentes que intervienen deben obligatoriamente intermediar en moneda virtual, con garantía suficiente, transparencia y fuera del ámbito financiero tradicional.

Esto exige otro sistema *Bitcoin*, otros criterios de actuación. Primero, la intervención financiera, de fondos de inversión y *shadow banking* conspira contra la idea de transparencia porque la titulización lleva a una opacidad automática, que significa anonimato, que no derecho a la intimidad, que es la primera materia de la moneda virtual. Segundo, la negociación de moneda virtual

que no se posee, invalida la creación originaria de la minería, alimentando moneda en la sombra que no añade ningún valor a la integridad de los mercados. Se entra en una pura realidad virtual, como si se tratara de un juego, que no la economía real, aunque los daños lo soportarían, finalmente, las personas.

Por tanto, retomando la idea de *Yee,* el foco de la disciplina legal de *Bitcoin* son los intermediarios del propio sistema Bitcoin, incluidas las organizaciones públicas que en este momento se encargan de la materia, con el propósito de evitar riesgos sistémicos que pueden facilitar daños online y evitar, al mismo tiempo, interferencias en la innovación del Internet del dinero. Esto significa otro concepto de híbridos financieros o sintéticos, que enfatice solo sobre la seguridad en el riesgo asumido, prohibiendo operaciones de especulación o sin propiedad de moneda virtual, *off-the-counter,* mediante negociación en mercados abiertos. La financiarización de Bitcoin, tal como la que conocemos, conduce la experiencia a su catástrofe anunciada. La pretendida segunda ola, será, ciertamente, la última.

La moneda virtual comparte rasgos próximos a la mercancía, si bien, en cuanto bien digital cuyo comercio está sometido a las reglas de mercado y la preservación del derecho a la intimidad del usuario, manteniendo, como intangible la crucial diferencia con la mercancía física. Que esto suceda no significa que la moneda virtual deba encauzarse en el ámbito del comercio de las mercancías, sobre todo, a tenor de lo dicho, respecto a los deletéreos efectos del recurso a los derivados financieros tradicionales que asoma como inevitable si así fuera.

Nada excluye que la moneda virtual puede compartir aspectos de título o valor en materia de inversión, lo cual atraería distintas competencias sobre la materia. La primera idea es que la moneda virtual puede acomodarse como mercancía digital, excepto su utilidad como activo subyacente de derivados, y, así tambien su calificación como título o valor, obligaciones de inversión (*security).*[184]

184. R.Grinberg, Bitcoin: An Innovative Alternative Digital Currency, Hastings Science & Technology Law Journal, Vol. 4:1, Winter, 2012, p.199, la diferencia entre mercancía y título es que éste confiere un recurso que la primera no concede: reclamar contra el emisor, sus beneficios, gestión o activos.

## **10.2.** TÍTULO O VALOR. INVERSIÓN EN BITCOIN

En agosto de 2013 el Tribunal de EEUU de *Eastern District*[185] *de Texas* sostuvo su competencia sobre un posible fraude en inversiones adquiridas con *Bitcoin,* en base a que las inversiones realizadas eran títulos o valores (*securities).*

El Tribunal se declaró competente puesto que se trataba de un fraude de inversión con *Bitcoin* y dicha inversión eran títulos, obligaciones, bonos. El demandante era la *Securities Exchange Commission (SEC)* y sostuvo la violación a la legalidad vigente en materia de títulos y, especial, un esquema *Ponzi* destinado al engaño de los inversores.

El demandado, *Trendon T. Shavers,* fundó y dirigió la *Bitcoin Savings and Trust*, promoviendo las ventajas a ahorristas para invertir en oportunidades vinculadas con *Bitcoin*. El demandado decía que se dedicaba a la venta de moneda virtual y prometía pagar al inversor un 1% de interés diario hasta que el retirára sus fondos o hasta que la compañía no pudiera generar beneficios suficientes.

Los inversores perdieron entre 1.8 y 23 millones de dólares.

El demandado se defendió argumentando que las inversiones realizadas no eran títulos o valores bajo la legislación americana porque Bitcoin no es moneda y no está regulada por los EEUU. Al negar la premisa mayor, no se trataba de títulos, valores, obligaciones, tampoco era competente el Tribunal. La SEC, a su vez, decía que los contratos de inversión implicaban títulos o valores, obligaciones.

El Tribunal encaja como contrato de inversión, las inversiones de compra de *Bitcoins* y por tanto, títulos, valor u obligaciones. La jurisprudencia exige que hay contrato de inversión cuando se cumplen tres condiciones: inversión en dinero; en una empresa en común y con la expectativa de beneficios por los esfuerzos del promotor. La clave es determinar si "los inversores son atraídos exclusivamente por las perspectivas de retornos de sus inversiones."[186]

---

185. Securities and Exchange Commission v. Shavers, Nº 4:13-CV-416(E. D. Tex. 6 2013)

186. SEC v W.J.Howey & Co, 328 US 293, 300,1946.

El Tribunal no duda en afirmar que *Bitcoin* es "moneda o forma de moneda", porque es empleado para la compra de bienes o servicios y aún para pagar los gastos necesarios de personas (en este caso los gastos del demandado) y los inversores entendieron su realizar una inversión en dinero. Es moneda, con la única restricción que *Bitcoin* solo puede emplearse en lugares que lo acepten como moneda. Asimismo, se trataba de una empresa común porque los inversores dependían de la experiencia del demandado en los mercados de moneda virtual y se había comprometido a conspicuos retornos. Ello cubría el tercero de los requisitos: la expectativa de obtener beneficios de la inversión.

La decisión del Tribunal acepta que, cumplidos los requisitos de *Howey,* nada impide que, en aplicación del principio de la substancia sobre la forma, se pueda considerar como un medio de cambio reembolsable en dinero y susceptible de reclamación al emisor.O sea, una obligación en sentido estricto.

La referencia no es caprichosa, porque, previamente, el Tribunal considera que estamos ante una moneda fiduciaria, una forma de moneda.

Finalmente, y no menos importante, que ello ocurra es a instancias de la organización pública encargada de velar en el mercado de los títulos. La SEC desarrolla, como ya se ha visto, una decidida campaña advirtiendo, sobre todo, los riesgos de inversión de moneda virtual y su autoridad para disciplinar materias relativas. Pero, al mismo tiempo, valora que pueden suscitarse otras cuestiones, que merecerían su respuesta: "sin perjuicio de si la moneda virtual subyacente es en si misma un título, los intereses planteados por entidades que tienen monedas virtuales o proveen retornos basados en activos tales como las monedas virtuales probablemente deberían ser obligaciones y por tanto sujetas a nuestra disciplina."[187]

Vale la pena demorarse en la importancia de esta sentencia. Primero, la moneda virtual, como tal, no figura en el elenco o catá-

187. J.Lee, A.Long, M.McRae, J.Steiner, Sth. Gosnell Handler, Bitcoin Basics: a Primer on Virtual Currencies,Business Law International,Vol.16, nro. 1, january 2015, p.31, citando a Mary Jo White, la Administradora de la SEC 30 August 2013, Senate Committee on Homeland Security and Government Affairs.

logo legal de instrumentos financieros definidos como títulos, valores u obligaciones. No solo; excluye expresamente a la moneda como tal. Segundo, califica la moneda virtual como una forma de moneda fiduciaria. Tercero, la aplicación de *Bitcoin* en inversión supone su reconocimiento como instrumento financiero, como título, valor u obligación.

## RECAPITULACIÓN

La moneda virtual encarna y representa la propiedad digital, en el sentido de su contenido informacional. Pero, al mismo tiempo, contando como elemento diferenciador la tutela del derecho a la intimidad, la tutela última del dato personal, la difusión de un valor *extrapatrimonial* en el mercado. Por eso no puede identificarse pura y simplemente con una mercancía en el mercado. Es un bien digital mercantil, con el velo de la privacidad, cubierto con el *burka* de lo que pertenece al derecho fundamental de la persona.

Bitcoin es un bien digital o virtual, intangible, de aplicación uniforme y valor de mercado, cuyo elemento destacado es la propiedad informacional, lo que se pretende comunicar, diferenciado de, de la información personal extramercado, que no se quiere comunicar. Esto significa que la tutela de la firma digital está construida para evitar o restringir la invasión de terceros en la identidad de las personas, que lo emplean en el mercado.

La moneda virtual comparte rasgos próximos a la mercancía, si bien, en cuanto bien digital cuyo comercio está sometido a las reglas de mercado, pero, insistiendo que la preservación del derecho a la intimidad del usuario comporta una reserva de circulación desde el origen de la identidad propia de la persona y de su voluntad de ponerla o no en conocimiento, manteniendo, además, como intangible la crucial diferencia con la mercancía física.

La financiarización de Bitcoin, servir de soporte a operaciones financieras estructuradas mediante híbridos financieros o sintéticos, conduciría la experiencia a su catástrofe anunciada. La pretendida segunda ola, será, ciertamente, la última. Esto significa pensar otro concepto de híbridos financieros o sintéticos, que enfatice solo sobre la seguridad en el riesgo asumido, prohibiendo

operaciones de especulación o sin propiedad de moneda virtual, *off-the-counter,* mediante negociación en mercados abiertos. La moneda virtual en la alquimia financiera se transforma, entonces í, en un puro juego virtual en manos de los especuladores e intermediarios financieros.

La moneda virtual, como tal, puede figurar a título propio en la enumeración de instrumentos financieros definidos como títulos, valores u obligaciones. La posición del caso *Shavers* y de la propia SEC permiten una correcta configuración de la moneda virtual como una forma de moneda fiduciaria, un instrumento financiero que es apto para el ahorro o la inversión. De este modo la aplicación de *Bitcoin* en inversión supondría su reconocimiento como instrumento financiero, como título, valor u obligación (*security)*, bajo la específica disciplina del sector.

# CAPITULO III
# LA MONEDA ALTERNATIVA.

## 11. La moneda alternativa

La principal propiedad del dinero es que sirva como medio de pago unidad de cuenta y reserva de valor, entre una serie indeterminada de personas, sea en una marco territorial o en dimensiones más reducidas, locales, comunitarias, empresariales. O, también, en un ámbito extraterritorial de alcance personal indefinido, como sería el caso, de la moneda digital.

"Una cosa se convierte y es moneda a través de un proceso de equilibrio social. *Es moneda cuando nosotros estamos de común acuerdo que lo es."*[188]

La referencia más reciente viene, como se ha visto, desde California donde se elimina una prohibición vigente impidiendo a personas jurídicas o personas físicas, la emisión y circulación dentro del Estado de moneda distinta a la moneda legal de los EEUU.

La denominación de California comprende todo y cualquier tipo de moneda: moneda virtual de empresa; moneda comunitaria y moneda digital; tratando de englobar un escenario que es un relato de la realidad del territorio poblado de moneda de empresa –*Amazon coin, Starbucks Star*–; moneda digital –B*itcoin* y otras similares– y moneda comunitaria enraizada con las economías locales- *Bay Bucks ,San Francisco, Davis Dollars , Davis, Santa Barbara Hours, Santa Barbara , Berkshares, Massachussets, Ithaca Hours, New York.*

---

188. E.Castronova, Wildcat Currency.How the virtual money revolution is transforming the economy. Yale University Press, 2014, p.99, 100: "Si un proceso social unge a la moneda virtual como moneda, será moneda. Hay alguna evidencia que esto está sucediendo."

## **11.1.** LA MONEDA COMUNITARIA. CONCEPTO

La categoría más notoria de moneda alternativa es la moneda comunitaria.

*Lietaer* define la moneda comunitaria como complementaria de la moneda nacional, que no substitutiva: un acuerdo dentro de una comunidad aceptando una moneda no nacional como medio de pago, incentivante de reciprocidad y cooperación.[189]

Sería un error restringir la existencia de la moneda comunitaria a unos pocos casos en los EEUU. En el Reino Unido pueden citarse, *Transition Town Pounds, Time Banks, Bristol Pounds, Bristol, Local Exchange Trading Systems y en Brasil, Banco Palma, Curitiba, Tauschring, Chiemgauer, Bremer Roland, en Alemania, Graine de Sel, en Francia, etc.*[190]

En 2003 se calculaban más de 4000 monedas complementarias: Italia, Francia, Alemania Reino Unido; Japón; Canada; Nueva Zelanda; México; Australia; Brasil. Monedas locales o regionales, con propósito de fortalecimiento de la actividad comercial, ambiental, laboral, o, en general.[191]

La moneda comunitaria, complementaria, es una construcción histórica: no es extraño que desde hace cientos sino miles de años se puede constatar la creación de monedas por los individuos, con fines y propósitos diferentes y ámbitos geográficos más o menos definidos, a nivel de ciudades o regiones. Sus funciones son idénticas a la moneda legal, salvo que carecen de fuerza obligatoria y respaldo legal público y no se aceptan para satisfacer obligaciones públicas tributarias, cotizaciones a la Seguridad Social, sanciones. Pero, asimismo, la moneda alternativa da respuesta a desafíos y funciones que la moneda convencional no puede cumplir. Y lo que es más importante, desmiente la existencia de una moneda nacional única en estado de monopolio.[192]

---

189. B.Lietaer, cit.p.180.

190. B.Lietaer, The future of money: Creating new wealth, work and a wiser world, London, january, 2001, p.31; Ver aquí California y la moneda alternativa, pag.32 y sigts.

191. L. Laubisch, Debate about alternative monetary systems- Silvio Gesell, John Maynard Keynes, Irving Fischer, Thesis Master of Science in International Finance, Berlin School of Economics and Law, École Supérieure de Commerce Extérieur Paris, 15, july 2013, p.45.

192. M.Shubik, Simecs, Ithaca Hours, Berkshares, Bitcoins and Walmarts, Discussion Paper nº. 1947, Cowles Foundation for research in economics, Yale University, may 2014.

La moneda comunitaria surge en momentos de crisis económica, como una respuesta a la inestabilidad financiera o como un instrumento de cohesión e inclusión social en momentos de incertidumbre política, un modo de resistencia y de organización social. La moneda alternativa aspira la circulación local de la riqueza; facilitar a las empresas y miembros de la comunidad el intercambio de bienes y servicios esenciales; promover la cohesión comunitaria y facilitar la inclusión de los menos favorecidos.[193]

No es, sin embargo, solo el efecto de un factor geográfico: la moneda en su versión comunitaria, es un medio de cambio de bienes y servicios, en la idea de facilitar las actividades económicas de sus usuarios, sin intermediación financiera o bancaria ni pública; desplazando el poder desde las instituciones a las personas, a los grupos, a la comunidad de usuarios.[194]

La moneda alternativa, en el sentido de la ley de California, incorpora la moneda digital, criptográfica, la cual obviamente tiene un horizonte más amplio, indefinido y genérico que la moneda comunitaria. *Bitcoin y* análogos se ofrecen como moneda alternativa digital, criptográfica, destacando por su extraterritorialidad, más allá de los ámbitos geográficos determinados, sean locales, regionales o de finalidad específica y su versatilidad tecnológica es superadora de su aplicación exclusiva a la moneda. Ambas comparten el consenso de los usuarios, la circulación sin respaldo público ni fuerza legal, y la eliminación de los intermediarios.

## **11.2.** LA MONEDA ALTERNATIVA DIGITAL CRIPTOGRÁFICA INFORMACIONAL

La criptomoneda alternativa es, utilizando la precisa terminología de la disciplina legal de New York, cualquier tipo de unidad digital. Un bien digital intangible, una cadena de bits, de firmas digitales, que se desplaza en Internet, como medio de cambio o forma de depósito de valor digital o que integra un sistema de dinero electrónico.

193. Sustainable Economies Law Center, 2015, Community Currencies Program, California.

194. PosNote, 475 August 2014, Houses of Parliament, Parliamentary Office of Science & Technology, Alternative Currencies.

La representación digital de valor califica la moneda virtual, porque, su naturaleza, a diferencia del bien digital ordinario, es exclusiva y excluyente y finalmente escasa.

La mejor definición de moneda virtual es la que ofrece *Nakamoto:* una cadena de firmas digitales. La firma electrónica es la **unidad** de la unidad digital y su significado es trascendente porque apunta a datos personales asociados al mensaje de datos que identifican al que lo envía y, al mismo tiempo, supone su aprobación a la información que transmite.[195]

La firma digital acredita la autenticidad de un mensaje de datos electrónico. La firma es la **persona** que la envía y aprueba y que el receptor sabe que es producto propio del remitente y no sufre alteración desde el punto de origen al punto de destino.

El sistema de *Bitcoin* reparte y descentraliza la **información** en la red de forma segura y convalidable, sea como valor monetario fiduciario virtual o, también, como distribución de información jurídica -propiedad, contrato, documentos de información personal, en forma segura y convalidable. [196]

La circulación de la información es genérica y universal, excepto la difusión de los datos personales de pertenencia de la firma digital, amparados por el **derecho a la intimidad**, un verdadero derecho de la personalidad, que no entran en el tráfico de valor o de propiedad, contrato, datos privados, a no ser que la persona decida lo contrario.

La información no es ni la intimidad ni el secreto de comunicación; sino el objeto ordinario del tráfico jurídico de la moneda: bienes y servicios, depósito o inversión. La información de la persona, la identificación, queda fuera del circuito informativo, lo cual propone una consideración dual: hay información que es de la persona y no sale de su ámbito, a menos que quiera y otra, que sirve para que la firma digital sea constitutiva de efectos jurídicos y económicos. La Cadena de Bloques recoge la información activa, dedicada al comercio. Podría decirse que hay un capital

195. UNCITRAL, cit., art. 2, a).

196. J.A.Kroll, I.C.Davey, E.W.Felten, cit.; E. Dourado, J. Brito, Cryptocurrency, cit.

humano informacional que no trasciende y una información que alimenta el flujo de la actividad del capital humano, de la persona, con autonomía de su fuente, salvo transgresión o violación del ordenamiento jurídico objetivo.

Por eso *Bitcoin* no es mercancía informacional, salvo en sentido amplio e impreciso, de tráfico jurídico y económico bajo las reglas del mercado, porque la unidad digital preserva la identificación y aprobación, la firma digital, en modo automático (criptográfico) de la circulación genérica y universal. La firma es la persona, **su capital humano informacional**, y la persona está fuera del comercio.

### 11.2.1. El derecho de personalidad. Intimidad y comunicación. La firma

"Los derechos de la personalidad, dice Ferrara, son los derechos supremos del hombre que garantizan en él, el goce de sus bienes personales. Frente a los derechos sobre los bienes exteriores, los derechos de la personalidad garantizan el goce de nosotros mismos, aseguran al individuo el señorio sobre su persona, la actuación de sus propias fuerzas físicas y espirituales."[197]

Extraemos: el goce de la persona partiendo del señorío sobre si mismo. La persona como objeto de su derecho de la que es sujeto.

El derecho de la personalidad incluye el derecho a la intimidad y la comunicación y el derecho a la identidad personal, para cada individuo.

El derecho a la esfera íntima de la persona significa que toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia (Convenio Europeo de Derechos Humanos, art.8.1; C.E., art.18). La protección de la privacidad es el ámbito reservado de vida de cada uno, frente a la intromisión injustificada de los poderes públicos o particulares, en contra de su voluntad. El derecho a estar solo y que lo dejen en paz. Esto siempre que no se cuestione ni la legalidad, legitimidad o necesidad democrática para la realización de su finalidad.

197. De Cossio, A., Instituciones de Derecho Civil. To I. Parte General, Madrid 1988, p.187

El secreto de las comunicaciones tiene un alcance rigurosamente formal, que está separado de su contenido: la comunicación, cualquiera que sea su contenido, debe vallarse de ingerencia de terceros, salvo ley o autorización judicial.

La firma es una especificación del derecho al nombre, una de sus formas de expresión, sea manual o electrónica. Es la identificación de la persona que envía el mensaje de texto y la evidencia que su contenido merece su aprobación, que el mensaje de texto es veraz y propio. Criptográficamente, se añade, es inmodificable una vez que se envía.

La firma, entonces, constituye un derecho de la personalidad, integrado en el derecho al nombre, cuya característica esencial es que es inseparable de su titular y carente, en si misma, de cualquier valor patrimonial.

La firma de la persona puede nutrir un derecho que se identifica con su privacidad, intimidad, y cubierto por el respeto al secreto de la comunicación. Es una expresión de identidad y voluntad que es inescindible de su titular. La intromisión de terceros o la ingerencia, en sin causa que lo justifique, significa una lesión al derecho humano tutelado.

El ámbito de la intimidad y el secreto en la comunicación solo cede ante indicios de uso ilegal, v.g. blanqueo de capitales, evasión tributaria, criminalidad organizada, terrorismo; pero, en ningún caso se impone la postergación en el tráfico fisiológico, jurídico o económico: "…la mayoría de la gente no querria vivir en una sociedad que permite anonimato para todo, menos para las pequeñas transacciones. Quieren vivir en una sociedad que provee el *nivel apropiado de privacidad.* Si todas las transacciones fueran anónimas los ricos y poderosos no podrían ser controlados."[198]

La criptografía asimétrica concede valor a la **información** intrínseca y extrínseca de la persona que genera datos en forma electrónica .Cualquier dato que pueda digitalizarse, codificarse como una cadena de firmas digitales es información. La información intrínseca es la clave secreta – quien firma- y la extrínseca es

198. D.G.W.Birch, What does cryptocurrence mean for the new economy, cit., p.511.

la clave pública –que es lo que se firma–. La información transita en Internet en modo secreto y en modo público, dirigida a la inscripción en el bloque y su posterior incorporación en la Cadena de Bloques.

En sentido jurídico, es información que propone *Bitproperty, Smart contracts* o documentación individual, curriculum vitae, datos de identidad.

La información intrínseca es la traducción del derecho de la personalidad: algo inherente a la persona y que no es idónea para ninguna valoración patrimonial separada, como, por ejemplo, sería el derecho sobre la imagen de la persona ni, obviamente, susceptible de alienación. La persona firmante es el creador de la firma digital, de la información intrínseca, aunque puede actuar en nombre propio o a través de la persona que representa.

La firma digital, como la manuscrita, sirve de indicación del nombre de la persona que hace propias las declaraciones del acto, negocio jurídico, contrato que firma. Por un lado, la individualización entre el mensaje y el remitente y, por otra, la autentificación, que expresa conocimiento, consentimiento y responsabilidad del envío.

La firma digital es la persona que crea la información cuyo contenido no puede alterarse o repudiarse mediante la aplicación de la criptografía asimétrica, claves públicas y privada.[199] Esa persona es la que realmente tiene en mente el sistema *Bitcoin.*

## RECAPITULACIÓN

California aporta el nuevo concepto de moneda alternativa. El adjetivo es definitivo. La alternativa al dólar, cualquiera que sea su configuración, modelo, alcance, finalidad, es moneda. Es obvio

199.El art. 3 de la L.59/2003 de firma electrónica dice: *"**La** firma **electrónica avanzada** es la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control".*

que no es moneda legal, de fuerza obligatoria y respaldo público; pero, es moneda. Cuando una persona compra o vende con alguna de esas monedas no está realizando un trueque o permuta, si no que paga y cobra, porque la otra parte así lo acepta.

La moneda comunitaria integra uno de los aspectos de la moneda alternativa.

Es una moneda que puede emplearse complementariamente a la moneda legal, de libre aceptación y común acuerdo entre sus usuarios, en un ámbito geográfico determinado.

*Bitcoin* es un objeto **criptográfico** (*fixed-value cryptographic object o digital token)* fundado en la asimetría criptográfica de la firma digital: el remitente usa la clave privada para cifrar el mensaje mientras que el receptor usa la clave pública del remitente para descifrar. La moneda digital es el otro componente importante de la moneda alternativa, basada en el tráfico jurídico de la información intrínseca de la persona y la información extrínseca encerrada en la firma digital.

La firma digital asociada a un mensaje de datos declara la identidad del firmante, información intrínseca, y ofrece su consentimiento voluntario al contenido en el mensaje de datos, información extrínseca.

*Bitcoin* reivindica el derecho al nombre, derecho de la personalidad, al amparo del derecho a la intimidad y en salvaguarda del secreto de la comunicación electrónica.

# CAPÍTULO IV
# LA IMPOSICIÓN DE LA MONEDA VIRTUAL

## 12. La imposición del mundo virtual

La doctrina coincide, en general, en que no existen argumentos fundados para que la disciplina de la actividad en el mundo virtual no sea equivalente a su similar en el mundo real. El beneficio, es el mismo, se obtenga en el medio virtual o en el real.[200] La gran diferencia está entre "*game worlds" (World of Warcraft)* y *"unscripted worlds (Second Life*),o sea, entre juegos que no están contaminados por el comercio y otros que alientan a sus participantes a hacerlo. El jugador que consigue moneda real de su deambular virtual debería quedar sujeto al impuesto. Esto puede o no suceder en el juego-juego, pero es inevitable que ocurra en los juegos que estimulan la imaginación comercial de los jugadores.[201]

La moneda virtual puede salir al mundo real, mediante cambio y ello producir un beneficio económico al perceptor-jugador. Desde que esa moneda virtual puede transformarse en moneda real, dólar, euro, yen, la oportunidad del beneficio debería gravarse cuando se consigue.[202]

---

200. N.A.Beckman, Virtual Assets,real tax:The capital gains/ordinary income distinction in virtual worlds,The Columbia Science and Technology Law review, 11, 2010. RMT (*real money trading)…"*Por ejemplo, la moneda de Second Life, denominada Lindens, es fácilmente canjeable por moneda real, lo cual significa que no hay diferencia real entre pagar por objetos con moneda real o pagarlos con Lindens…" p.158

201. L.Lederman, Stranger tan fiction: Taxing virtual worlds, New York Unviersity Law review, 2007, 82.

202. S.Chung, Real taxation of virtual commerceVirginia Tax review, Vol 28, 2008, p.146.

La manifestación de capacidad contributiva que se grava es la capacidad del jugador de procurarse dinero en efectivo. La renta virtual puede estimarse y los participantes pueden realizarlo por lo que no cabría distinción respecto a la renta derivada de una actividad real.[203]

El mundo virtual del juego, del entretenimiento puro y duro, tiene sus propias reglas, generalmente, establecidas desde la aceptación por el participante de las condiciones fijadas por la licencia de uso del software. Es razonable suponer que el dominio del placer prevalece sobre cualquier otra consideración. En cambio, los juegos virtuales, desestructurados o sin guión, sometidos a la improvisación creativa del participante, y cuya arquitectura promueve el comercio virtual no se conservan como espacios lúdicos, sujetos como están a las normas jurídicas del mundo real.

Dice *Castronova*, que los mundos abiertos no son sino "extensiones mundanas de los territorios de la Tierra"*: "*Como mundos que importan, estos mundos abiertos deberán recibir exactamente el mismo tratamiento legal como recibe el mundo real. Por ejemplo, toda la actividad económica dentro de los mundos abiertos deben ser tratadas como equivalentes a la actividad económica en el mundo real."[204]

*Bitcoin* pertenece al mundo virtual abierto y así como no parece fundado negarle su calidad de dinero virtual; al mismo tiempo, obliga al legislador a su regulación como moneda alternativa a la moneda real, de curso legal. No es un mero espacio de juego, sino un objeto de valor representativo digital al servicio del comercio de bienes y servicios, al depósito de valor, al ahorro o inversión.

La diferencia entre la moneda comunitaria y la moneda digital o virtual consiste que la primera no desmiente ni contradice la base de permuta o trueque de las operaciones que acredita. Todo lo que es comercio intracomunitario es trueque, intercambio de bienes o servicios recíprocos, representados en créditos o débitos, cuyo contenido es mudable o variable, pueden ser horas, sellos, actividad profesional propia. En cambio, la moneda virtual, pese

203. A.Chodorow, Tracing Bias through Virtual Spaces, Cornell Law review, Vol.95, 2, january 2010.

204. E.Castronova, cit, The right top lay, p.205.

a las tentativas de formulación, excede el marco del trueque. El valor digital representa, en si mismo, un número, una cantidad, un importe, que puede ser transversal a la transacción: compra o venta; cobro o pago; pero, asimismo, ahorro o inversión.

La moneda virtual en el mundo real es tan real como la moneda legal. De ello se deduce que su disciplina jurídica y, sobre todo, fiscal, debe prescindir del concepto de trueque, que no le sirve; para ajustarla a la noción, primero, de propiedad digital –información intrínseca e extrínseca– y, segundo, que su calificación de renta o patrimonio, aún intangible digital, responde a los mismos criterios que inspiran la renta o patrimonio físico o material.

## **12.1.** LA CAPACIDAD CONTRIBUTIVA Y EL BIT

La firma digital dirigida a la información electrónica segura y fiable de mensajes de textos es la persona en acto y su derecho al uso de sus datos personales específicos: la identidad y la voluntad de actuar en un sentido u otro. La unidad de medida del mensaje de texto es el número de bits y bytes.

Dicho esto hay que reparar en la importancia de la firma digital como índice del capital humano informacional, que es el fundamento de la moneda virtual y preguntarse cual es su función en y con respecto al sistema tributario.

La firma digital es, en si misma, un indicador de capacidad contributiva. El mero envío, recepción, del mensaje de texto, en las condiciones del sistema *Bitcoin* revelan el contenido de bits empleados, el bien digital es una cadena de bits, y la moneda virtual es una cadena de firmas digitales. El bit emerge como el primero de los elementos susceptibles de valoración económica de sujeción fiscal.

El presupuesto de hecho de la fiscalidad digital, en general, es el bit y su cuantía se determina en los elementos digitales de la transmisión electrónica. Pero, la unidad, no es decisión de la oferta y la demanda, sino fruto de la autonomía política del legislador, como la Tobin Tax o la Carbon Tax.

Consecuentemente, la primera y decisión política fiscal es la discusión y adopción de la *Bit-Bitcoin Tax.*[205]

El sistema de registro público y universal, que es una de las virtudes de la tecnología *Bitcoin*, acomoda perfectamente el bit a la transacción inscripta. Pero, aún más, si se quisiera, la *Bit-Bitcoin Tax* podría ser el prólogo a la aceptación formal de la moneda virtual en el cumplimiento de las obligaciones tributarias relativas a su empleo.

El bien digital de camino a la moneda virtual, cuyo nucleo es la unidad digital, podría, incluso ser el pretexto de convertir al propio *Bitcoin:* la *Bit-Bitcoin Tax* incardinaría el cumplimiento de las obligaciones ordinarias derivadas de las transacciones llevadas a cabo mediante la moneda virtual: la moneda virtual como instrumento de pago de la *Bit Tax.*

El escenario de la moneda virtual, moneda siempre, es conflictivo porque su origen y desarrollo es la cadena de firmas digitales, la unidad digital, y como tal, es información que incorpora en Internet el valor monetario de transacciones o el valor patrimonial de otros documentos que no son monetarios. La criptopropiedad es propiedad Bit, parafraseando a *Fairfield,* dominio creado especialmente para la operación de cambio que se cede a otro que lo acepta a cambio de un precio en moneda virtual. La convalidación de la cual es su inscripción contable en el registro público universal.

La unidad digital en el comercio es el bit, cuyo consumo exhibe la primera indicación de capacidad contributiva en movimiento. La *Bit-Bitcoin Tax* afronta el gravamen adecuado a través de la tecnología del sistema *Bitcoin:* hay un hecho imponible cuya base imponible declarada es el precio, medido por intensidad de bits. Los sujetos pasivos son los cambistas, intermediarios y proveedores de servicios del sistema.

## **12.2.** LA CALIFICACIÓN DE LA MONEDA VIRTUAL NO FUNCIONAL

El dinero virtual, el bien digital representativo de valor como dinero, no es material o tangible, como el dinero efectivo. Pero,

205. T.Rosembuj, El Impuesto Digital, cit. p.194.

aunque ajeno a la contabilidad del intermediario financiero o bancario, pretende cumplir exactamente con las mismas funciones, desde un signo o marca –la firma digital– que nutre el mensaje de texto criptográfico. "objeto de información cifrada en la red."[206]

Los resultados del tráfico mercantil mediante el uso de *Bitcoin* no son diferentes al que se desprende de la aplicación de medios de pagos ordinarios y convencionales, conforme a la transacción aplicada: *Smart contracts,* compraventa, préstamos, créditos, servicios conexos, que son la fuente de salarios, beneficios, dividendos, intereses, ganancias de capital o pérdidas o a su inversión o ahorro como título valor.

La renta de empresa afecta a los sujetos dedicados al intercambio de moneda virtual entre si o respecto a monedas legales, a los intermediarios del sistema, los proveedores de servicios, excepto la particularidad del tratamiento de los mineros constituidos o no en unidades económicas estables y habituales; así como a la empresa que de cualquier modo interviene en operaciones liquidadas mediante moneda virtual por la cesión o adquisición de bienes y servicios.

La renta de trabajo dependiente es la contraprestación recibida como salario en moneda virtual por la actividad cumplida.

Finalmente, la valorización o desvalorización de la moneda en su cambio cotidiano, en la medida que proceda como activo financiero, como capital, provoca ganancias o pérdidas de capital conforme a su valor de mercado al momento de su realización. La renta de propiedad deriva del empleo de la moneda como instrumento financiero o de inversión y ahorro. La moneda virtual como título valor. Un bitcoin contiene un millón de bits.

Hay una cierta coincidencia en considerar como compensación de servicios la actividad del minero. No está claro, porque la ganancia del minero puede ser concebida, asimismo, ganancia de capital no derivada de transacción previa, v.g. descubrir un teso-

206. M.A.Jansen, Bitcoin: the political "virtual" of an intangible material currency, cit.p.17, donde su crítica a la asimilación entre dinero efectivo y virtual se basa en la inexistencia de las previas relaciones de deuda con la contabilidad bancaria. Bitcoin se postula como independiente en su creación y predistribución como transacciones sin fuente.

ro u obtener incremento patrimonial del azar o la casualidad. El minero que verifica una transacción no recibe siempre una compensación por sus servicios, porque los servicios que presta no siempre llevan al resultado de la contraprestación, a menos que, sea el primero, en realizar la prueba de trabajo con efecto positivo: la creación de nuevos bloques en la Cadena. No es un mero servicio; debe producirse un resultado, que no es ni más ni menos que la creación de nueva moneda y se encarna en la recompensa al minero por conseguirlo. El minero obtiene una retribución automática del sistema, que podrá realizar cambiando la retribución por moneda legal o comprando bienes y servicios, instantes en los que deviene contribuyente. Esa contraprestación accidental y excepcional revela atributos de ganancias de capital, antes que de compensación de servicios. Sin perjuicio, que pudiera conseguir retribución adicional por sus servicios específicos, que le confieren el derecho a una determinada cantidad de dinero legal o similar, lo cual le sirve de compensación, en ese particular. Este es el ejemplo de los *mining pools* que coordinan y aumentan su poder informático para mejorar sus oportunidades de hallar nuevos bloques. La recompensa por el bloque se divide entre los que contribuyen a su búsqueda y solución, menos una comisión si el operador del pool hace un cargo por el servicio.

"Puesto que las monedas virtuales actúan en muchos sentidos como moneda en el mundo real, deberían gravarse como divisas extranjeras (non *functional currency).* Si la recepción de moneda virtual es gravable debería depender si el receptor consigue una ganancia económica en el mundo real…Una ganancia económica se logra cuando la moneda se convierte en moneda real y debería gravarse en ese momento."[207]

En verdad, la moneda alternativa digital es moneda, que no propiedad en sentido estricto. Cualquiera que use moneda legal para la compra de bienes o servicios no puede calificarse como realizador de ganancias o pérdidas de capital sobre la moneda virtual en si misma. El uso de *Bitcoin,* si se caracteriza como propiedad, daría siempre origen a ganancias o pérdidas patrimoniales.

---

207. S.Chung, Real Taxation of virtual commerce, Virginia Tax Review, Vol.28, 2008, p.147.

Al contrario, si *Bitcoin* atiende a su naturaleza propia de moneda alternativa a la moneda legal, es obligado calificarlo como una **moneda no funcional**, distinta a la moneda legal (*non functional currency)*. La moneda no funcional es la moneda virtual respecto a la moneda legal dominante. La consecuencia de ello es que su empleo provoca renta ordinaria o pérdida en lugar de ganancias o pérdidas patrimoniales.[208]

La moneda virtual, no funcional, comparada con la moneda legal, funcional, merita un tratamiento equivalente, en el bien entendido, que se acepte su carácter de moneda: medio de cambio, unidad de cuenta, instrumento financiero.[209]

## **12.3.** LA EXPERIENCIA EN EL REINO UNIDO

La Administración Tributaria del Reino Unido explicita su posición sobre la fiscalidad de *Bitcoin*..[210]

La línea de reflexión es de absoluta coherencia con la disciplina *Bitcoin.* Es una moneda virtual no funcional, cuya disciplina tributaria admite su consideración como tal para la aplicación de las normas tributarias generales con referencia a los principales impuestos. La moneda virtual es dinero, medio de pago o depósito de valor, como el dinero legal y a eso debe ajustarse el impuesto, y al efecto es dinero no funcional como si fuera una divisa extranjera.

---

208. Taxpayer Advocate Service- 2013 Annual Report to Congress-V.One, p.249."Por ejemplo, un residente en EEUU generalmente no reconoce ganancia o pérdida cuando usa dólares para comprar bienes o servicios. Como resultado, algunos pueden quedar sorprendidos que el uso de bitcoins en la compra de bienes o servicios origina ganancias o pérdidas de capital gravadas sobre los propios bitcoins.", p.253.

209.H.Wiener, J.Zelnik, I.Tarshish, M.Rodgers, Chomping at the Bit: US Federal Income Taxation of Bitcoin Transactions, Tax Notes International, january 27, 2014, Vol 73-4, p.353. Las operaciones en divisa extranjera se gravan bajo la Section 988 del Internal Revenue Code de los EEUU que considera los rendimientos como renta positiva o negativa ordinaria. Lo primero a determinar es si la transacción implica una moneda, sea funcional, v, g, dólar, o no funcional, v.g. euro. No hay definición legal de moneda.

210. Revenue and Customs Brief 9(2014, Bitcoin and other cryptocurrencies.GOV.UK.

### 12.3.1. IVA

La renta recibida por las actividades mineras de *Bitcoin* está fuera del ámbito del IVA en base a que la actividad no constituye una actividad económica para los fines del IVA, porque hay un vínculo insuficiente entre los servicios facilitados y cualquier contraprestación recibida.

Efectivamente, no puede concebirse como prestación de servicios una actividad de resultado aleatorio e impredecible, que no está ligada a la dicha actividad, sino a su resultado final eventual.

La renta recibida por los mineros por otras actividades, tales como la provisión de servicios en conexión con la verificación de transacciones específicas para las cuales se prevén cargos específicos, están exentas del IVA (Artículo 135 (1) (d), de la D.EU IVA, porque caen en el ámbito de la definición de "efectos comerciales" similares a la entrega de dinero, "transacciones, incluida la negociación, concerniente depósitos de fondos y cuentas corrientes, pagos, giros, créditos, cheques y otros efectos comerciales, con excepción del cobro de créditos."

Sirve el ejemplo del *miners pool* al cual se hizo referencia por los cargos que efectua el operador a los demás participantes. El concepto jurídico es que se trata de "efectos comerciales", que otorgan un derecho a una determinada cantidad de dinero, similares a la propia entrega del dinero.[211]

Cuando Bitcoin es cambiado por esterlinas o divisas extranjeras, tales como euro o dólar, no se adeuda IVA sobre el valor de los propios Bitcoins.

---

211. En el mismo sentido la consulta V1029-15 de la SG de Impuestos sobre el Consumo, Agencia Tributaria, 3-3-2015, compraventa de moneda electrónica Bitcoin: "Por tanto, de la sentencia Granton Advertising se puede concluir que el concepto de «otros efectos comerciales» del artículo 135.1.d) de la Directiva 2006/112/CE está íntimamente ligado a **instrumentos de pago que permiten la transferencia de dinero** y que como tales operaciones financieras deben quedar exentas del Impuesto.Las monedas virtuales Bitcoin actúan como un **medio de pago** y por sus propias características deben entenderse incluidas dentro del concepto "otros efectos comerciales" por lo que su transmisión debe quedar sujeta y exenta del impuesto."

### 12.3.2. Impuesto sobre Sociedades

Están sujetos a impuesto los beneficios o pérdidas de las operaciones de cambio entre divisas. El tratamiento fiscal de las monedas virtuales es objeto de las reglas generales sobre cambio con divisas extranjeras y relaciones de préstamos. Los movimientos de cambio para las empresas se determinan entre la moneda funcional que emplea, v, g, esterlinas, y la otra moneda en cuestión. El análisis se aplica si hay un tipo de cambio entre Bitcoin y la moneda funcional.

### 12.3.3. Impuesto sobre la renta

Deben reflejarse en la contabilidad los beneficios y pérdidas de una empresa individual respecto a las transacciones Bitcoin, gravables conforme a las normas ordinarias del impuesto.

### 12.3.4. Impuesto sobre ganancias de capital

Si se verifica un beneficio en un contrato de moneda que no está incluido en los beneficios empresariales queda sujeto al impuesto como ganancia de capital o puede deducirse, en su caso, como pérdidas.

## 12.4. LA EXPERIENCIA EN LOS EEUU

La experiencia americana, a diferencia de la británica, clasifica la moneda virtual como propiedad, en lugar de moneda, como si fuera una divisa extranjera. *Bitcoin*, como cualquier divisa, es medio de pago, porque se acepta como pago de bienes y servicios; puede cambiarse con otras monedas o aplicarse como como inversión en títulos valores.[212]

La Administración americana tiene un punto de partida distinto y, a la postre, equivocado. Su experiencia en anteriores episo-

212. C.G.Warley, Federal Tax Policy Committee, Texas Society of Certified Public Accountants, en carta dirigida al John A.Koskinen, Comisionado del Internal Revenue Service, sobre Notice 2014-21 Virtual Currency Guidance, september 22,2014.

dios relativos a la economía de trueque y, probablemente, monedas comunitarias que lo respaldan, le llevan a concluir que *Bitcoin* no es sino el mero intercambio entre propiedades distintas, sin moneda de por medio; operación de *barter.*

El *Internal Revenue Service* (IRS) define la permuta relativa a cualquier persona u organización que contratan entre si para el intercambio de propiedad o servicios. Usualmente, no hay cambio por dinero efectivo.[213]

La permuta consiste en el cambio de un producto o servicio por otro, sea en modo informal, caso por caso o a través de una sociedad dedicada al intercambio entre sus socios.[214]

La preocupación de la Administración reside en las sociedades cuyo objeto es el cambio entre sus socios o clientes de bienes o servicios. El trueque usa "unidad *barte*r", que no es dinero efectivo, que sirve para acreditar o debitar unidades de crédito a los miembros por los bienes o servicios proveidos o recibidos. El socio o cliente cambia por 1 a otro algo que le hubiera significado 1 dólar. El otro cambia al primero por 1 algo que le hubiera significado 1 dólar.

El valor razonable de los bienes o servicios recibidos mediante el trueque se considera renta imponible. La unidad *barter* es idéntica a los dólares reales a efectos de información tributaria. O sea, cada uno de los participantes en el trueque deben incluir el valor razonable de mercado de lo que recibieron en su renta íntegra.

La finalidad de obligar a las sociedades dedicadas a la permute a aflorar sus actividades les impuso deberes amplios de comunicación tributaria.

El IRS extiende los principios de la permuta o *barter,* a la moneda virtual. La diferencia es que la moneda virtual es convertible en moneda legal, cosa que no sucede con las unidades de barter.[215]

---

213. IRS Bartering Tax Center, 2-10-2014;J. Isom,As certain as Death and Taxes:Consumer Considerations of Bitcoin Transactions for when the IRS Comes Knocking, December 9,2013, donde se señala que la calificación como barter fue siempre una de las opciones del IRS, p.15, ssrn.com.2365493

214. S.Pareja, It Taxes a Village: the problema with routinely taxing barter transactions, Catholic University Law review, vol.59, 2010.

215. Internal Revenue Service, Internal Revenue Bulletin 2014-16, april 14 2014, Notice 2014-21, IRS Virtual Currency Guidance.

La Administración americana tiene un punto de partida distinto y, a la postre, equivocado. Su experiencia en anteriores episodios relativos a la economía de trueque y, probablemente, monedas comunitarias que lo respaldan, le llevan a concluir que *Bitcoin* no es sino el mero intercambio entre propiedades distintas, sin moneda de por medio; operación de *barter*.

El IRS califica a *Bitcoin* como propiedad, no como moneda, para los fines de impuestos federales. De ese modo los principios generales que se aplican a las transacciones de propiedad se aplican a las transacciones que usen moneda virtual convertible. Entre propiedad y moneda, elige la primera. Las consecuencias son determinantes.

*Bitcoin* como propiedad supone, además del desconocimiento de su configuración como moneda, la identificación puntual y permanente en cada operación si se trata de un activo (acciones, obligaciones) o rendimiento ordinario en las manos del contribuyente (inventarios y bienes afectados a la actividad de la empresa). La calificación de la propiedad conduce a una compleja individualización en cada operación y que lleva al gravamen sobre ganancias o pérdidas de capital o al de renta ordinaria.

No es por otra razón que se dice que el tratamiento solo sirve para los inversores a largo plazo; pero, perjudica a los comerciantes o individuos que aceptan o usan la moneda virtual como pago de bienes y servicios, que quedan obligados a establecer valores cambiantes sobre cada transacción diaria, que, inclusive, cambian en el decurso del mismo dia.[216]

*Bitcoin* como moneda, como si fuera una divisa no funcional (extranjera) no es susceptible como regla sino de generar renta positiva o pérdida ordinaria por el cambio de la moneda por dinero, otros bienes o servicios.; y excepcionalmente, para los individuos, ganancias de capital por actos singulares, sea por inversión o, en mi opinión, por la actividad minera.[217]

---

216. C.G.Warley, Federal Tax Policy Committee, Texas Society of Certified Public Accountants, cit.

217. N.Mirjanich, Digital Money: Bitcoin`s Financial and Tax Future Despite Regulatory Uncertainty, De Paul Law Review, Vol.64, 2014; J.Isom, cit., la compra de divisa por un individuo se trata como la compra de un activo y su venta posterior puede resultar en ganancia de capital, dependiendo del tipo de cambio al momento, p.18.

La moneda virtual es una representación digital de valor que funciona como medio de cambio, unidad de cuenta o depósito de valor. En algunos ambientes se acepta como si fuera moneda real, legal, de fuerza obligatoria. Siguiendo la definición del *Financial Crimes Enforcement Network (FinCEN)* usa el concepto de moneda virtual convertible, de valor equivalente en moneda real o que actua como su reemplazo y que puede comprarse o cambiarse en dólares, euros, etc.[218]

El contribuyente puede obtener ganancias de capital o renta ordinaria de la venta o cambio de la moneda virtual por otra propiedad. Lo primero, cuando la moneda virtual es activo, capital, en sus manos, por ejemplo, asimilable a acciones, obligaciones, inversiones. Lo segundo, renta ordinaria, cuando se trata de inventarios, o propiedad dirigida a la venta a clientes en la actividad económica que se realiza.

El contribuyente que recibe *Bitcoin* se ve abocado a incluir el valor razonable de la moneda, al momento de la recepción, para calcular su renta íntegra, tanto si lo recibe a cambio de bienes o servicios o por actividad de minería. Inmediatamente, se exige el cálculo de la ganancia o pérdida de capital, que obliga a definir si el activo es o no un activo de capital.[219]

El cambio de moneda virtual por otra propiedad origina ganancias o pérdidas de capital; lo cual presupone su consideración como activo, como capital, obviamente, intangible por sus características. La transmisión de moneda virtual supone realizar ganancias o pérdidas de capital intangible, que no renta ordinaria; a menos que la actividad económica sea la de comercio en o con moneda virtual. O sea, la moneda virtual no siempre se califica como ganancia o pérdida de capital y ello sucede si es una actividad que no sea de empresa habitual.[220]

---

218. V.pag.36.

219. B.Akins, J.L.Chapman, J.M.Gordon, A Whole New World: Income tax considerations of the Bitcoin Economy, Pittsburgh Tax Review, 2015. Los autores fundamentan que las transacciones que implican el cambio de bitcoin por moneda legal, bienes o servicios debería calificarse como ganancia o pérdida de capital; mientras que la creación o minería debería calificarse como renta por compensación de servicios, con lo que discrepo: hay una pura ganancia o pérdida de capital .Y, respecto a la primera, también: es renta ordinaria.

220. N.Antonikova, Real Taxes on Virtual Currencies: What does the IRS Say?, Virginia Tax Review, 34, 3, 2014, p.11.

El que cobra en moneda virtual debe integrarla a su renta, al valor razonable de mercado de la fecha de recepción.

El tipo de cambio de la moneda virtual debe ser razonable, calculado en dólares, a la fecha de su recepción

El pago a un contratista independiente en moneda virtual es una renta de trabajo autónomo. El pago a un trabajador en moneda virtual es salario. La contraprestación a una actividad económica regular supone renta regular, ordinaria.

Hay deber de información de los pagos realizados por encima de determinados importes y de retención y sanciones en caso de incumplimiento. No deja de reprocharse a la Administración que el tratamiento dispuesto supone una pesadilla para le contribuyente, porque le obliga a seguir cada unidad de moneda virtual y las ganancias o pérdidas en cada transacción, como por ejemplo, beber un cafe.

El contribuyente que recibe la moneda virtual como pago por bienes o servicios debe incluir en su renta íntegra el valor razonable de mercado de la moneda a la fecha del recibo. Las transacciones que usan moneda virtual deben documentarse en dólares. Si la moneda virtual cotiza en un mercado, el valor de mercado razonable será determinado mediante su conversión en dólares al tipo de cambio.

En suma, de la calificación de propiedad queda excluida la designación de la moneda virtual como tal y, consecuentemente, las operaciones en las que se emplea reciben el tratamiento genérico de la permuta o *barter.* Por tanto, si hay bienes o servicios que se entregan o reciben, sin dinero, será por cambio directo entre las partes. No es, desde luego, la mejor solución, que, obviamente, sería la consideración de la moneda alternativa como otra divisa, lo cual facilitaría la gestión tanto para el contribuyente como para la Administración.[221]

221. N.Antonikova, cit., p.34: la moneda virtual tipo Bitcoin asemeja una divisa extranjera en la forma que opera como medio de cambio.

### 12.4.1. El minero

El minero obtiene renta íntegra por la recompensa de *Bitcoin* como retribución de servicios. La actividad económica de minero genera renta de trabajo autónomo sujeta a impuesto. Es una compensación de servicios. Es un error, porque la creación de moneda virtual no puede ser gravada como servicio, sino como adquisición de ganancia de capital que no deriva de transacción. O, como también, sería razonable, no puede gravarse un producto por su producción, sino en el momento en que se realiza, se vende.[222]

El IRS entiende que el minero debe incluir la moneda virtual por su valor razonable de mercado a la fecha de la recepción. La posición interpreta que el minero realiza un servicio por lo cual recibe la recompensa en *Bitcoin.*

El minero convalida la transacción mediante la creación de un nuevo bloque, que le supone una recompensa determinada, porque evita el *doublé spending.*

La crítica de *Lewis* es que no hay servicio, sino creación de propiedad. ”No es que Usted reciba un pago por proveer servicios a alguno, sino que esto pasa porque Usted está creando propiedad, Bitcoins, a través de un esfuerzo de capital intensivo, solucionando problemas matemáticos con costosos ordenadores “La actividad del minero es como la del panadero horneando el pan y el panadero es gravado cuando vende el pan, no cuando el pan está en el horno. El autor sostiene que el gravamen debería verificarse cuando el minero realiza su beneficio, por ejemplo, vendiendo las monedas virtuales que obtuvo o adquiriendo bienes o servicios.

Coincido que no hay servicio, como asimismo es la posición de la Administración británica. La diferencia es que, podría interpretarse que la recompensa al minero es adquisición patrimonial sin transacción, susceptible de calificarse como ganancia patrimonial, como si halla un tesoro o por azar.

222. W.Lewis, Why the IRS is wrong on the taxation of bitcoin mining, march 27, 2014, The Global law & Business perspective.

### 12.4.2. New York. California

El Estado de Nueva York explica su política de impuesto sobre las ventas a las transacciones que usan moneda virtual convertible. Su posición coincide en lo fundamental con la definición del IRS: la moneda virtual es una propiedad sometida al trueque o *barter*.[223]

El uso de una moneda virtual convertible por un consumidor para el pago de bienes o servicios se considera una transacción de permuta. Pero, a tener en cuenta, siendo la moneda virtual un intangible y por lo tanto no sujeta al impuesto sobre ventas, queda también no sujeta la moneda virtual que recibe una de las partes. Sin embargo, si a cambio del pago en moneda virtual se reciben bienes o servicios sujetos, la parte queda sujeta al impuesto por el valor de mercado de la moneda virtual a la fecha.

Un ejemplo lo clarifica: El cliente compra artículos de decoración a un comercio online a cambio de moneda virtual. El cliente debe pagar el impuesto por el valor razonable de mercado de la moneda virtual en dólares y el comerciante no debe impuesto por la moneda virtual recibida a cambio de sus productos.[224]

En California el *State Board of Equalisation* explica el modo de aceptación de la moneda virtual como un método de pago, en la misma línea de reflexión impulsada por el IRS.[225]

Si un restaurante vende comida a un cliente por un menú de 50 dólares y recibe 0.065 bitcoin; la base imponible en el impuesto sobre las ventas es de 50 dólares. Inclusive, si el pago de bitcoin es superior al precio del menú en dólares, este prevalece.

El organismo manifiesta, asimismo, que no acepta la moneda virtual como método de pago de impuestos.

---

223. New York Department of Taxation and Finance, Technical Memorandum TSB-M-14(5) C, (7)I, (17)S, December 5, 2014.

224. A.Nellen, Sales Tax and Bitcoin (or other virtual currency), December, 19, 2014, Sales Tax Support.com, apunta algo interesante al ejemplo del comerciante decorador y es que él está aceptando la moneda virtual como equivalente al dinero efectivo con la consecuencia que si convierte el dinero virtual en efectivo será gravado de nuevo.

225. California State Board of Equalisation, Accepting Virtual Currency as Payment Method, june 2014.

## RECAPITULACIÓN

La moneda virtual en el mundo real es tan real como la moneda legal. No deja de ser moneda porque no tenga el respaldo público ni el soporte bancario.

De ello se deduce que su disciplina jurídica y, sobre todo, fiscal, debe asumir que es otra moneda, complementaria o sustitutiva de la moneda legal, una moneda no funcional, equivalente. El trueque o la permuta sirven, en extremo, para la explicación de la moneda comunitaria, pero es totalmente artificiosa en el caso de la moneda virtual. Es necesario un esfuerzo en torno a la bit propiedad –información intrínseca y extrínseca y que su calificación como medio intangible de pago acepta el compromiso de renta o patrimonio en base a los mismos criterios que inspiran las transacciones mediante moneda legal. La moneda no funcional es la moneda virtual respecto a la moneda legal dominante, La consecuencia de ello es que su empleo en operaciones monetarias provoca renta ordinaria o pérdida en lugar de ganancias o pérdidas patrimoniales.

La unidad digital en el comercio es el bit, cuyo consumo exhibe la primera indicación de capacidad contributiva en movimiento. La *Bit-Bitcoin Tax* afronta el gravamen adecuado a través de la tecnología del sistema *Bitcoin:* hay un hecho imponible, firmas digitales, cuya base imponible declarada es el precio, medido por intensidad de bits. Los sujetos pasivos son los cambistas, intermediarios y proveedores de servicios del sistema.

El encuadramiento jurídico mejor logrado es el del Reino Unido. La premisa es que *Bitcoin* constituye una moneda virtual semejante a la moneda no funcional y su disciplina debe ser análoga a la que se establece para los rendimientos en el Impuesto sobre Sociedades y en el Impuesto sobre la Renta. Asimismo, destacar que, de cara al IVA, la actividad de minería no reúne los requisitos de definición suficiente de servicios.

La disciplina americana tiene un punto de partida distinto y, a la postre, equivocado. Su experiencia en anteriores episodios relativos a la economía de trueque y, probablemente, monedas comunitarias que lo respaldan, le llevan a *concluir que Bitcoin no es sino el mero intercambio entre propiedades distintas,* sin moneda

de por medio; una operación o serie de operaciones de permuta, trueque o de *barter*.

El IRS califica a *Bitcoin* como propiedad, no como moneda, para los fines de impuestos federales. De ese modo los principios generales que se aplican a las transacciones de propiedad se aplican a las transacciones que usen moneda virtual convertible, cuya característica es de propiedad que servirá para el cambio por otros bienes o servicios, cambio, o inversión. Entre propiedad y moneda, elige la primera.

El cambio de moneda virtual por otra propiedad origina ganancias o pérdidas de capital. La transmisión de moneda virtual supone realizar ganancias o pérdidas de capital intangible, que no renta ordinaria; a menos que la actividad económica. Sea la de comercio en o con moneda virtual.

No es por otra razón que se dice que el tratamiento solo sirve para los inversores a largo plazo; pero, perjudica a los comerciantes o individuos que aceptan o usan la moneda virtual como pago de bienes y servicios, que quedan obligados a establecer valores razonables de mercado cambiantes sobre cada transacción diaria, que, inclusive, cambian en el decurso del mismo dia. El valor razonable supone aplicar un valor a la transacción que es variable, tornadizo, y, en micropagos, absolutamente irrelevante.

Tampoco es convincente asumir la actividad del minero como servicio, en lugar de estricta ganancia de capital, sea porque realiza la contraprestación, la recompensa de *Bitcoin* que recibe por la creación de moneda virtual y que, posteriormente, o invierte, cambia o compra bienes o servicios o, como pienso, porque su retribución es pura ganancia patrimonial sin transacción.

# BIBLIOGRAFÍA

## Artículos


**B.Akins, J.Chapman, J.Gordon, G.Gwinnett** College School of Business, A whole new world: income tax considerations of the bitcoin economy, Pittsburgh Tax review, 2015.

**R.Ali, Jh.Barrdear, R.Clews, J, Southgate,**

**—,** Innovations in payment technologies and the emergence of digital currencies, Quarterly Bulletin Bank of England, 2014.

**—,** The economics of digital currencies, Bank of England, Quarterly Bulletin, 2014.

**J.Allaire, Circle Internet Financial,** Testimony, november 18, 2013, Committe on Homeland Security and Governmental Affaires.

**Agencia Tributaria,** Consulta V1029-15 de la SG de Impuestos sobre el Consumo, 3-3-2015, compraventa de moneda electrónica Bitcoin.

**E.Androulaki, G.O.Karame, M.Roeschlin, T.Scherer, S.Capkun,** Evaluating user privacy in Bitcoin. ETH Zurich, 8092, 8 april 2013.

**N.Antonikova,** Real Taxes on Virtual Currencies: What does the IRS Say?, Virginia Tax Review, 34, 3, 2014.

**Bank of England,** One Bank Research Agenda, Discussion paper, february 2015.

**BaFin**,

**—,** Annual Report 2013.

—, Trading in Bitcoins, 17 june 2014.

**BaFin, J.Münzer, Bitcoins: Supervisory** assessment and risks to users, 17 february 2014.

**A.Bal,** Stateless virtual money in the tax system, European Taxation, july 2013.

**C.R.Baros,** Barter**,** Bearer and Bitcoin, The likely future of steless virtual money, University of Miami Business L.rev, 201,2014.

**N.A.Beckman,** Virtual Assets, real tax: The capital gains/ordinary income distinction in virtual worlds, The Columbia Science and Technology Law review, 11,2010.RMT (*real money trading).*

**J.A.Bergstra, P.Weijland,** Bitcoin: a money-like informational commodity, Informatics Institute, University of Amsterdam, february 20,2014.

**D.G.W.Birch,** What does cryptocurrency mean for the new economy, en D.LEE Kuo Chuen, Handbook of Digital Currency.

**R.Bohme, N.Christin, B.Edelman, T.Moore,**

—, Bitcoin, working paper 15-015 july 15, 2014, Harvard Business School.

**J.Brito,** Global Markets Advisory Committee, 9-10-2014, CFTC.

**J.Brito, A.Castillo,** Bitcoin: a primer for policymakers.

**J.Brito, Eli Dourado**, Comments to the New York Department of Financial Services on the Proposed Virtual Currency Regulatory Framework, August 14,2014, Mercatus Center George Mason University.

**Jerry Brito, Houman Shadab, Andrea Castillo,** Bitcoin Financial Regulation: Securities, Derivatives, Prediction Markets, and Gambling, The Columbia Science & Technology Law Review, Vol. XVI, 2014.

**A. Blundell- Wignall,** 2014, The Bitcoin Question: currency versus trust-less transfer technology, OECD Working papers on finance, insurance and private pensions, 37.

**California Assembly** Bill no.129 Chapter 74, june 28 2014.

**B.T.Camp,** The Play`s the Thing: A theory of taxing virtual worlds, 59 Hastings L.J., 4,2007.

**Cartographie 2014** des risques et tendances sur les marchés financiers et pour l' épargne, Risques et tendances n.15, juillet 2014, Autorité des Marches Financieres.

**E.Castronova,**

**—,** Virtual worlds: a first-hand account of market and society on the cyberian frontier, december, 2001, Center for Economic Studies & Ifo Institute for Economic Research, working paper no. 618.

**—,** The right to play, 8, december, 2004, ssrn.com 733486.

**CFPB,** Risks to consumers posed by virtual currencies, August, 2014.

**A.Chodorow,** Tracing Bias through Virtual Spaces, Cornell Law review, Vol.95, 2, january 2010.

**D S.Cohen,** Adressing the illicit finance risks of virtual currency, 3-18-2014.

**Commission des Finances**. **Consumer Financial Protection Bureau,** Les Conclusions et Recommandations, Risks to consumer.

**CSBS** Policy on State Virtual Currency Regulation, december 14,2014.

**D.Chaum**, Blind signatures for untraceable payments, Department of Computer Science University of California, Santa Barbara, 1983.

**S.Chung,** Real taxation of virtual commerce Virginia Tax review, Vol 28, 2008.

**Wei Dai,** B-Money, 1998.

**J.J.Doguet,** The nature of the form: legal and regulatory issues surrounding the bitcoin digital currency system, 73 Louisiana.L.Review, 2013.

**E. Dourado, J. Brito,** Cryptocurrency, The New Palgrave Dictionary of Economics, Online Edition, 2014, edited by S.N. Durlauf y L. E. Blume.

**C.K.Elwell, M.Maureen Murphy, M.V.Seitzinger,** Bitcoin: Questions, Answers, and Analysis of legal Issues, Congressional Research Service, july 15, 2014,7-5700

**European Banking Authority,** EBA Opinion on "virtual currencies", 4, july 2014.

**Josh Fairfield,**

—**,** Virtual Property, Boston University Law review, Vol 85,2005.

—**,** The Magic Circle, 14 Vand.J.Ent. &Tech L 545,2012.

—**,** "Bitproperty", Washington & Lee Public Legal Studies Research Paper Series.n.2014-17, october 2, 2014, p.18.

—**,** "Bitproperty", Washington and Lee University School of Law, paper No 2014-17, October 2, 2014, 88 S.**Cal.L.Rev** (2015).

**European Central Bank,** Virtual Currency Schemes, october 2012; Virtual currency schemes- a further analysis, february 2015.

**M.Farouk** Analysis, California Assembly Third Reading, january 23,2014.

**FATF** Report, Virtual currencies. Key definitions and Potencial AML (antimoney laundering)/CFT (countering the financing of terrorism, june 2014, FATF/OECD, Paris.

**FinCEN,**

**Financial Crimes** Enforcement Network, Networking Bulletin, march 2013, Cryptocurrencies.

—**,** Application of FinCEN`s regulations to persons administering, exchanging or using virtual currencies, FIN-2013-G001, march 18 2013.

—**,** Application of FinCEN`s Regulations to Persons Administering, Exchanging or Using Virtual Currencies, cit; D.S.Cohen, Adressing the illicit finance risks of virtual currency, Secretary of Terrorism and Financial Intelligence, Treasury, 3/18/2014.

**Focus,** 10- 5 décembre 2013, Banque de France.

**Fondo Monetario Internacional**, Bitcoin versus Electronic Money, Brief, january 2014.

**Gibson Dunn,** BitLicense 2.0: New York moves closer to comprehensive virtual currency regulation, february 15,2015.

**C.Gomez Jimenez.** El bitcoin y su tributación, Contabilidad y Tributación, 380, noviembre 2014.

**Government Accountability Office, GAO,**

**—,** 13-156, Virtual Economies and Currencies: Additional IRS Guidance could reduce tax compliance risks, 2013.

**—,** 14-496, Virtual Currencies. Emerging regulatory, Law Enforcement, and Consumer Protection Challenges, may 2014.

**EBA** European Banking Authority, Opinion on "virtual currencies",4 july 2014.

**Financial Industry Regulatory Authority**, Bitcoin: more than a bit risky, may 7,2014.

**GOV. UK,** Annual Report to Congress-V.One. Revenue and Customs Brief 9(2014, Bitcoin and other cryptocurrencies.

**S.Gorjon,** Divisas o Monedas virtuales. El caso Bitcoin, Dirección General De Operaciones, Mercados y Sistemas de Pago, Banco de España, enero 2014.

**R.Grinberg,** Bitcoin: An Innovative Alternative Digital Currency, Hastings Science & Technology Law Journal, Vol. 4:1, Winter, 2012.

**Internal Revenue Service,**

**—,** Internal Revenue Bulletin 2014-16, april 14 2014, Notice 2014-21, IRS Virtual Currency Guidance.

**—,** Bartering Tax Center, 2-10-2014.

**J. Isom,** As certain as Death and Taxes: Consumer Considerations of Bitcoin Transactions for when the IRS Comes Knocking, December 9,2013, l IRS, ssrn.com.2365493.

**M.A.Jansen,** Bitcoin: the polític "virtual" of an intangible material currency, International Journal of Community Currency Research, Vol 17(A) 8-18, 2013.

**N.M.Kaplanov.** Nerdy Money: Bitcoin, the private digital currency, and the case against its regulation, ssrn.com 2115203.

**Gary C.Kessler,** An overview of cryptografphy, 21, january, 2015.

**J.A.Kroll, I.C.Davey, E.W.Felten,** The economics of Bitcoin mining, or Bitcoin in the presence of adversaries, The Twelfth Workshop on the Economics of Information Security (WEIS 2013, Washington DC, june 11-12- 2013.

**L. Laubisch,** Debate about alternative monetary systems- Silvio Gesell, John Maynard Keynes, Irving Fischer, Thesis Master of Science in International Finance, Berlin School of Economics and Law, École Supérieure de Commerce Extérieur Paris, 15, july 2013.

**L.Lederman,** Stranger tan fiction: Taxing virtual worlds, New York University Law review, 2007,82.

**J.Lee, A.Long, M.McRae, J.Steiner, Sth. Gosnell Handler,** Primer on Virtual Currencies, Business Law International, Vol.16, nro. 1, january 2015

**W.Lewis,** Why the IRS is wrong on the taxation of bitcoin mining, march 27, 2014, The Global law & Business perspective.

**Superintendent Lawsky** remarks on revised BitLicense framework for virtual currency regulation and trends in payments technology, December 18,2014.

**Ph.Marini-F.Marc,** Rapport d´information, Commission des finances sur les enjeux liés au developpement du Bitcoin et des autres monnaies virtuelles, Sénat, n. 767 rectifié, 23 juillet 2014.

**Ministere des Finances et des Comptes Publiques**, L`encadrement des monnaies virtuelles.Recommandatations visant a prévenir leurs usages á des fins frauduleuses ou de blanchiment, junio 2014.

**P.McLeod,** Taxing and regulating Bitcoin: the governments game of catch up, CommLaw Conspectus, Vol 22,2014.

**I.Mas, D.LEE Kuo Chuen**, Bitcoin-Like Protocols and Innovations, en Handbook of Digital Currency.

**Timothy C.May**, Cifernomicon. Manifiesto criptoanarquista.1992.

**N.Mirjanich,** Digital Money: Bitcoin`s Financial and Tax Future Despite Regulatory Uncertainty, De Paul Law Review, Vol.64, 201., 2014.OJO

**P.Murck,** Testimonio de Bitcoin Foundation ante The Homeland Security and Governmental Affairs Committee, November 18, 2013.

**S.Nakamoto**, Bitcoin: a peer-to-peer electronic cash system, www.bitcoin.org., 2008.

**NASSA,** North American Securities Administrators Association, What`s in your e-Wallet?, april 2014

**—,** North American Securities Administrators Association, New Products in classic schemes identified as top investors threats, november 12, 2014.

**A.Nellen,** Sales Tax and Bitcoin (or other virtual currency), December, 19,2014.

**New York State. Department of Financial,**

**—,** Services proposed New York codes, rules, regulations.Title 23.Department of Financial Services. Chapter I.Regulations of the Superintendent of Financial Services. Part 200 Virtual Currencies. Proposal, july, 23, 2014.

**—,** Technical Memorandum TSB-M-14(5) C, (7) I, (17) S, December 5 ,2014.

**L.Pak Nian, D.LEE Kuo Chuen,** Introduction to Bitcoin en Handbook of Digital Currency.

**S.Pareja,** It Taxes a Village: the problema with routinely taxing barter transactions, Catholic University Law review, vol.59, 2010.

PosNote, 475 August 2014, Houses of Parliament, **Parliamentary Office of Science & Technology**, Alternative Currencies.

**S.Patterson,** How Bitcoin Works, october 2014, hillsdale.edu.

**M.Raman,** Assistant Attorney General Criminal Division, US Department of Justice, Testimony, november 18,2013, Committee on Homeland Security and Governmental Affairs US Senate, cit.

**M.T.Schaefer,** Bastard Culture: How Users Participation Transforms Cultural Production., p.64, 2009.

**SEC,**

**—,** v. WJ Howey Co 328 US 293(1946).

**—,** Investor Alert.Ponzi Schemes Using Virtual Currencies, Investor Alert, (SEC Pub no 153(7/13), 23 july 2013.

**—,** v Shavers 2013 US Dist LEXIS 11018(E.D. Texas, august 6 2013.

**—,** Bitcoin and other virtual currenciy-Related investments, Investor Alert, 7, may, 2014.

**Securities and Exchange Commission v. Shavers,** Nº 4:13-CV-416(E. D. Tex. 6 2013).

**B.Segendorf,** What is bitcoin?. Sveriges Riksbank Economic review, 2,2014.

**H.B.Shadab,** Regulating Bitcoin and Block Chain Derivatives, Commodity Futures Trading Commission Global Markets Advisory Committee Digital Currency Introduction-Bitcoin, October, 9, 2014.

**Jennifer Shasky Calvery, Testimony, FinCEN US Senate Committee on Homeland** Security and Governmental Affairs, november 18,2013,"Beyond Silk Road: Potential risks, threats, and promises of virtual currencies,".

**M.Shubik,** Simecs, Ithaca Hours, Berkshares, Bitcoins and Walmarts, Discussion Paper nº. 1947, Cowles Foundation for research in economics, Yale University, may 2014.

**Yen-Shyang Tseng,** Governing Virtual Worlds: Interration 2.0, Washington University Journal of Law & Policy, 2011, Vol 35.

**D.J.Solove,**

**—,** Digital Person.Technology and privacy in the Information Age.New York University Press, 2004.

**—,** "I´ve Got nothing to hide" and other misunderstandings of privacy, 2-7-2008, ssrn: 998565.

**J. Spoenle,** Cloud computing and cybercrime investigations: territoriality vs. The power of disposal?, 31 August 2010, Project on Cybercrime, Council of Europe.

Conference of **State Bank Supervisors,** North American Securities Administrators Association, Model State Consumer and Investor Guidance on Virtual Currency, april 23,2014.

**California State Board** of Equalisation, Accepting Virtual Currency as Payment Method, 2 june 2014.

**Superintendent Lawsky`s** remarks at the Bipartisan Policy Center on Regulating Virtual Currencies and Payments Technology, Washington DC, December 18,2014.

**Sustainable Economies Law Center**, 2015, Community Currencies Program, California.

**Chairman Timothy G.Massad** before the US House Committee on Agriculture, Washington DC, february 12, 2015. CFTC.

**UK HM Treasury,** Digital currencies: response to the call for information, march 2015.

**UE.**

Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por el que se establece el marco comunitario para la firma electrónica; Ley 59/2003, de 19 de diciembre, de firma electrónica.

Directiva 2009/110/ce del Parlamento europeo y del Consejo de 16 de septiembre de 2009, art.2, 2).

**UNCITRAL,**

**—,** Model Law on Electronic Signatures with Guide to Enactment, 2001.OJO

**UNODC,** Basic Manual on the detection and Investigation of the Laundering of Crime Proceeds using virtual currencies, june 2014.

**P.Van Valkenburgh, H.Geiger, B.Szoka, Comments** to the New York Department of Financial Services on the Proposed Virtual Currency Framework, October 21,2014.

**C.Viegas, J.Giglio Santamaría, S.Perciavalle, M.Urquiza,** Bitcoin: un desafio para la ejecución de políticas de la Banca Central. Banco Central de República Argentina, agosto 2014.

**Virtual Currency Tax Reform** Act de may 7, 2014, HR 4602.

**S.Lo, J.Ch. Wang,** Bitcoin as money, Current Policy Perspectives, Federal Reserve Bank of Boston, no.14-4, september 4,2014.

**C.G.Warley,** Federal Tax Policy Committee, Texas Society of Certified Public Accountants, en carta dirigida al John A.Koskinen, Comisionado del Internal Revenue Service, sobre Notice 2014-21 Virtual Currency Guidance, september 22, 2014.

**M.Wetgen, T**he Global Markets Advisory Committee Open Meeting, 9.10.2014.CFTC.OJO

**H.Wiener, J.Zelnik, I.Tarshish, M.Rodgers, Chomping** at the Bit:US Federal Income Taxation of Bitcoin Transactions,Tax Notes International, january 27, 2014, Vol 73-4.

**M.J.White,** Chair SEC, 30, August, 2013, carta al Committee on Homeland Security and Governmental Affairs.

**G.Wood, A.Buchanan,** Advancing Egalitarianism, en D.LEE Kuo Chuen, Handbook of Digital Currency.

**A.Yee,** Internet architecture and the layers principle: conceptual framework for regulating Bitcoin, 2014, Internet Policy Review,3(3)DOI:10.14763/2014.2.289.

## Libros

**E.Castronova,** Wildcat Currency.How the virtual money revolution is transforming the economy. Yale University Press, 2014.

**De Cossio,** Instituciones de Derecho Civil.To I. Parte General, Madrid 1988.

**V.Lehdonvirta, Edward Castronova,** Virtual Economies. Design and Analysis.2014, Massachussets Technological Institute.

**D.LEE Kuo Chuen**, Handbook of Digital Currency. Bitcoin, innovations, financial instruments and big data, Elsevier, 2015,San Diego.

**B.Lietaer,** The future of money: Creating new wealth, work and a wiser world, London, january, 2001.

**T. Rosembuj,**

**—,** Intercambio internacional de información tributaria, Barcelona, 2004.

**—,** El impuesto digital, Barcelona, 2015.

**P.Vigna, M.J.Casey,** The Age of Cryptocurrency.How Bitcoin and Digital Money are challenging the Global Economic Order, New York, 2015.