

UNIVERSIDAD PANAMERICANA

FACULTAD DE DERECHO

CON RECONOCIMIENTO DE VALIDEZ OFICIAL DE ESTUDIOS ANTE LA S.E.P

CON NUMERO DE ACUERDO 944893 DE FECHA 24-III-94

“ACTIVOS VIRTUALES: PANORAMA REGULATORIO.”

**TESIS PROFESIONAL
QUE PARA OBTENER EL TÍTULO DE
LICENCIADO EN DERECHO**

P R E S E N T A

FERNANDO IRACHETA GARCÉS

DIRECTOR DE TESIS: DR. ALFREDO A. REYES KRAFFT

CIUDAD DE MÉXICO

2018

A mis padres, por darme la oportunidad de estudiar en una Facultad de excelencia. Por brindarme su apoyo incondicional y no dejarme desfallecer en los peores momentos. Por anteponer mi bienestar al suyo y hacer absolutamente todo lo que estaba en su poder para que yo pudiera superarme.

A Fernando por estar ahí siempre que lo necesité y a Lupita que siempre se desveló y madrugó conmigo, compartiendo alegrías y tristezas.

A mis abuelos por su amor y apoyo. A Jorge por sus enseñanzas, a Elizabeth, que por su cariño, honestidad e integridad se convirtió en un referente en mi vida

Al Doctor Alfredo Reyes Krafft por creer en mi trabajo y nutrir mi curiosidad. Por su asesoría y supervisión, a través de las cuales demostró su excelente calidad humana. Por ir más allá de lo estrictamente necesario y ayudarme siempre que tuvo la oportunidad de hacerlo.

A Arturo por su alegría, A Elías por su nobleza, A Luis por su candidez.

A Majo por su paciencia, comprensión y ayuda constante.

A todos los que me ayudaron a lo largo de mi viaje.

Gracias

Índice

I. Introducción	5
II. Bitcoin	8
II.1. Orígenes y Funcionamiento	10
II.2. Minería y Gobernanza en la Cadena	13
II.3. Bifurcaciones o <i>Forks</i>	20
II.4. Llaves Públicas, Privadas y Carteras	22
II.5. Valuación y Valor	26
II.6. Análisis	27
III. La Evolución de la Tecnología	28
III.1. Ethereum	31
III.1.1. <i>Ethereum Virtual Machine</i> (Funcionamiento de la Plataforma).....	32
III.1.2. <i>Proof-of-Work</i> y <i>Proof-of-Stake</i> en Ethereum (Minería).....	35
III.1.3. <i>Tokens</i>	39
III.1.4. <i>Initial Coin Offerings</i>	43
IV. Taxonomía de los Activos Virtuales.....	49
V. Panorama Internacional de los Activos Virtuales	57
V.1. Estados Unidos de América	58
V.1.1. <i>U.S. Securities and Exchange Commission</i>	61
V.1.2. <i>Commodity Futures Trading Commission</i>	69
V.1.3. <i>Financial Crimes Enforcement Network</i>	74
V.2. Suiza	78
VI. Panorama Nacional.....	86
VI.1 Disposiciones de Autoridades Diversas.....	87
VI.1.1. Servicio de Administración Tributaria.....	87

VI.1.2. Banco de México, Comisión Nacional Bancaria y de Valores y Secretaría de Hacienda y Crédito Público	92
VI.2. Antecedentes y Reformas al Marco Jurídico Existente	96
VI.3. Marco Jurídico Reformado	98
VI.4. Ley para Regular las Instituciones de Tecnología Financiera	110
VI.4.1. Instituciones de Financiamiento Colectivo	112
VI.4.2. Instituciones de Fondos de Pago Electrónico	120
VI.4.3. Capítulo Tercero, “De las Operaciones con Activos Virtuales” .	129
VII. Conclusiones.....	145
VIII. Bibliografía	155

I. Introducción

El objetivo del presente trabajo es comprobar que la Legislación Mexicana en lo relacionado con activos virtuales, particularmente la Ley para Regular las Instituciones de Tecnología Financiera (“LRITF”), no tiene un acercamiento óptimo al fenómeno regulatorio que estos representan, señalando las áreas de mejora. Sin embargo, cabe destacar que la legislación secundaria no se encuentra terminada; por lo que aún es posible que el marco regulatorio pueda ser alterado y con ello que las observaciones planteadas en la presente tesis pierdan validez o adquieran más vigencia.

Por consiguiente, el propósito de este documento es presentar posibles áreas de oportunidad en la legislación para así abonar en la construcción y evolución de tanto las leyes existentes. En otras palabras, la relevancia de esta investigación reside en la posibilidad de contribuir en la mejora del marco jurídico, a fin de que éste permita y promueva el desarrollo y el fortalecimiento de la industria de las tecnologías financieras en México, haciendo hincapié en el sector de activos virtuales.

Con la intención de hacer lo anterior posible, es necesario adentrarse en la naturaleza del objeto regulado, además de profundizar en los antecedentes regulatorios a nivel internacional en la materia. En esa misma línea, a continuación, se presentará la secuencia que llevará la presente tesis.

Primeramente, se abordará la historia y funcionamiento del primer activo virtual, bitcoin; con el objetivo de examinar una serie de circunstancias y tecnologías que surgieron a partir de este y que comparten ciertos de activos virtuales. De la misma manera, es necesario presentar su funcionamiento y características esenciales para poder establecer si la regulación que se desea imponer es compatible con los activos virtuales que se buscan regular.

Seguidamente, se analizará cómo evolucionó la tecnología que permitió la existencia de bitcoin y la generación de plataformas más complejas. Una de ellas siendo Ethereum, cuya investigación es de gran importancia para el estudio de los activos virtuales. Asimismo, se presentará cómo estos avances tuvieron un profundo

impacto en la industria de activos virtuales. También, se abordarán los eventos generadores de monedas o *ICOs*, y cómo es que éste modelo de fondeo o capitalización se convirtió en un punto clave en el espacio regulatorio.

En otro orden de ideas, el acelerado desarrollo de la industria de los activos virtuales no ha permitido el establecimiento de una terminología adecuada ni una clasificación definida, por lo que el capítulo subsecuente explorará las posibles maneras de categorizarlos, con el objetivo de aportar hacia la construcción de una terminología adecuada en la materia. Hasta el momento, la falta de una correcta categorización no ha tenido consecuencias importantes; sin embargo, al pretender regular a los activos virtuales, es de suma importancia que los términos utilizados sean lo más universales y precisos posibles para evitar problemáticas derivadas de ambigüedades.

Posteriormente, se explorará el panorama internacional. Se presentarán y analizarán los casos de los EE. UU. y Suiza, países seleccionados por su importancia en el escenario mundial de activos virtuales; lo anterior con el propósito de examinar la manera en la que fue abordado el problema regulatorio que presentan los activos virtuales en países y a la postre comparar las acciones tomadas en esos lugares con la experiencia mexicana en la materia.

En busca de una pauta que determine la evolución en la actitud de las autoridades respecto a los activos virtuales, en la sección denominada Panorama Nacional, se discutirán los acercamientos que tuvieron diversos entes regulatorios previo a la LRITF. Igualmente, se examinará de manera sucinta el proceso de conformación de la legislación en la materia; desde su elaboración hasta su votación en ambas cámaras legislativas, prestando especial atención a las leyes existentes que afectaron su aprobación. Por último, se estudiará la nueva LRITF analizando sus artículos relevantes con la finalidad de exhibir los posibles aspectos mejorables de la legislación.

A modo de conclusión, recordando que el objeto de este análisis es la búsqueda de un perfeccionamiento del marco jurídico nacional, se establecerá en qué puntos se considera que la legislación es mejorable. Es decir, se presentarán comentarios y

sugerencias con el objetivo de contribuir a la creación del mejor escenario posible para las industrias relacionadas y sus clientes.

II. Bitcoin

En esta primera parte se presenta Bitcoin, un concepto fundamental para el tema tratado en el presente trabajo y que debe de ser abordado antes de afrontar el problema principal de su regulación, así como la de otros activos de su clase. De acuerdo con Andreas Antonopoulos, uno de sus más populares apologistas, Bitcoin consiste en “una colección de conceptos y tecnologías que forman la base de un ecosistema digital de dinero. Unidades de valor llamadas bitcoin son usadas para almacenar y transmitir valor entre participantes de la red. Los usuarios de Bitcoin se comunican unos con otros a través del protocolo del mismo nombre, primordialmente vía internet, aunque otras redes pueden ser utilizadas con el mismo fin. El *stack* del protocolo bitcoin está disponible como un software abierto y puede ser ejecutado en múltiples dispositivos con capacidad computacional, incluyendo *laptops* y teléfonos inteligentes, haciendo la tecnología sumamente accesible”¹.

En su acepción de activo virtual, bitcoin² alcanzó una amplia aceptación entre el público y ha logrado ser el más reconocido entre los de su especie en el mercado. No obstante, su aportación al mundo no es sólo su altísimo valor, sino la tecnología sobre la cual descansa: el protocolo responsable de la revolución tecnológica creadora de los activos virtuales. De la misma manera, es necesario entender la naturaleza de estos activos y sus principios para encontrar la mejor manera de abordar el problema regulatorio que representan.

La red Bitcoin, sin la cual el activo virtual no podría existir, descansa en distintos elementos: una red descentralizada *peer-to-peer*, un registro público de transacciones (*blockchain* o *hash-linked data structures*), criptografía de llaves públicas, un conjunto de reglas de consenso usadas para verificar la validez de las transacciones y la emisión de nueva moneda, y un mecanismo de consenso global y descentralizado, también conocido como *Proof-of-Work*. Posteriormente, se

¹ (Antonopoulos, 2017, p. 18)

² En el presente trabajo se utilizará la notación utilizada por Antonopoulos. Es decir, cuando la palabra Bitcoin sea escrita con b mayúscula (“B”) se estará refiriendo a todo el conjunto de elementos que dan forma a la red; por otro lado, cuando la palabra bitcoin sea escrita, con b minúscula (“b”), se hará referencia al activo virtual.

profundizará en los conceptos anteriores, pero antes de hacerlo, es preciso que se conozca cómo se originó tanto el protocolo como el activo virtual para después adentrarse en su funcionamiento.

II.1. Orígenes y Funcionamiento

Bitcoin fue presentado al público por primera vez en un reporte técnico, conocido como “*White Paper*” o “Reporte”, publicado bajo el seudónimo de Satoshi Nakamoto³ y titulado: “*Bitcoin: A Peer-to-Peer Electronic Cash System*”⁴ (Bitcoin: Un Sistema de Dinero Electrónico Entre Pares).

En este documento, que fue inicialmente distribuido en el 2008 en correos de usuarios afectos a la criptografía, se plantearon diversos problemas relacionados con los sistemas de pagos electrónicos existentes, haciendo hincapié en las debilidades de un sistema de pagos centralizado basado en la confianza de un intermediario que procesa dichos pagos. Uno de los inconvenientes mencionados es la posibilidad de revertir los pagos⁵ frente a la prestación de servicios irreversibles, abriendo la puerta a la posibilidad de dejar a una de las partes expuesta al riesgo de no recibir su debida contraprestación. Esto sucede, según se teoriza en el documento, porque en caso de conflicto, la autoridad central no puede evitar intervenir para intentar resolver la reclamación, con el posible resultado de revertir el pago. Este peligro, dice Nakamoto, aumenta el costo transaccional de las operaciones que se llevan a cabo a través de cualquier tipo de sistema electrónico, además de obligar a los prestadores de bienes o servicios a recabar más información del cliente que la estrictamente necesaria, con el fin de evaluar el riesgo que existe de una reclamación que derive en un impago⁶. Ante esto, Nakamoto sugiere la eliminación del intermediario central que verifica los traslados de valor, proponiendo una solución novedosa que buscaba resolver los diversos problemas que traería el cambio.

Uno de estos problemas es el denominado “doble gasto”. La eliminación de un intermediario financiero centralizado que mantenga un registro de traslados de valor electrónico tiene como consecuencia la posibilidad de que el dinero se utilice dos o

³ Una persona o grupo de personas que aún hoy en día permanecen en el anonimato.

⁴ (Nakamoto, 2008)

⁵ *Ibidem*, p.1

⁶ Un ejemplo de esto es la práctica adoptada recientemente por los comercios de pedir una identificación en compras con tarjeta por montos superiores a cierta cantidad de dinero.

más veces a falta de un sistema capital que valide las transacciones, esta es una falla conocida como doble gasto o *double-spending*. Dicha complicación consiste “en un potencial fallo en una cripto-moneda o sistema de monedas virtuales, donde la misma unidad digital puede ser gastada más de una vez, ya que la unidad digital se compone un archivo digital que puede ser duplicado o falsificado”⁷. Esta circunstancia es similar a la de la falsificación del papel moneda, sin embargo, resulta ser más dañina en un ecosistema digital, ya que al ser relativamente sencillo replicar un activo virtual, se puede ocasionar una inflación desmedida que baje el valor del activo, además de afectar gravemente la confianza del usuario en el valor, así reduciendo su uso y retención. Lo anterior se relaciona estrechamente con el problema de la escasez virtual, lo que plantea la interrogante de cómo provocar y mantener una escasez artificial de un objeto virtual, considerando que va en contra de su naturaleza ser escaso.

Afortunadamente, Nakamoto planteó soluciones para resolver ambos problemas. Por medio de un sistema de trabajo computacional y comprobación criptográfica, propone la emisión controlada de lo que entonces clasificaba como una moneda virtual propia que logra ser escasa a pesar su naturaleza y no puede ser gastada más de una vez. Define a su creación como una serie de firmas digitales, en la cual “cada propietario del valor virtual lo transfiere firmando un hash de la transacción mediante la cual adquirió el valor en primer lugar con su llave pública y la llave del siguiente propietario, añadiendo esta información al final de la moneda virtual”⁸. A partir de este concepto desarrolla una red encargada de registrar, mantener y poner en circulación nuevas monedas, de acuerdo con lo establecido en las reglas de consenso, que permitan la operación de la red, mediante un sistema de incentivos. El mantenimiento de esta red permite asegurar a los usuarios que el valor no se gastó dos veces, registrando de modo inmodificable las transacciones, por lo que se tratan de operaciones irrevocables. Esto es logrado a través de una tecnología que después tomaría el nombre de cadena de bloques, mejor conocida por su

⁷ (Chohan, 2017, p. 2)

⁸ (Nakamoto, 2008, p. 2)

término en inglés; *blockchain*. El concepto, tal y como es planteado en el Reporte⁹ consiste en “un servidor distribuido mediante un sistema *peer-to-peer* capaz de imprimir una marca de tiempo que genere una prueba computacional del orden cronológico de las transacciones”¹⁰.

El registro en esta base de datos inicia con una pieza de información, en el caso de Bitcoin una transacción firmada, que se empaqueta y se traduce en una serie de números y letras que se denomina “*hash*”¹¹ utilizando la función matemática con el mismo nombre. Éste se convierte en la “huella digital” criptográfica de la transacción que representa una versión “comprimida” o “digerida” de la información introducida. Los datos que le dan forma al *hash* de un bloque son: la cantidad transferida, la dirección del emisor y la del receptor de la operación, representadas por la llave pública de ambos y la firma de ambos (conceptos sobre los cuales se profundizará más adelante), entre otros. La información de las transacciones se almacena en unidades llamadas bloques, que al unirse le dan nombre a la tecnología; *blockchain* o cadena de bloques. El vínculo que une a los bloques es el *hash*. Cada bloque contiene su *hash* y el del bloque inmediato anterior. El primero funge como el título del bloque, que es una representación criptográfica del contenido de este. El segundo es el eslabón que lo conecta con los bloques anteriores en la cadena, el título del bloque anterior. Una vez obtenidos estos datos, el bloque se debe de minar, una tarea que requiere de trabajo computacional y que permite al bloque ser añadido a la cadena.

⁹ En el Reporte nunca es mencionado explícitamente el término “*blockchain*”.

¹⁰ *Ibidem*, p.1, otras definiciones pertinentes son las dadas en (Van Valkenburgh, 2016, p. 3): “Registro compartido que lista una serie de transacciones (en el caso de Bitcoin) en la red y puede ser usado como un canal de transmisión irreversible y puede ser usado para el registro de datos o actividades relacionadas” y una serie de registros compartidos de forma descentralizada o distribuida que mediante algoritmos criptográficos que verifican la creación y transferencia de activos representados de forma digital en una red de pares, o (*peer-to-peer* en inglés)” (Maupin, 2017, p. 2)

¹¹ El *hash*, traducido libremente en español como picadillo, lío o digestión, es una serie de números y letras, siempre de la misma longitud, que son el resultado de revolver datos mediante una fórmula matemática, siendo muy poco probable que la función emita dos series de números y letras iguales de dos entradas de datos distintas. Si se tienen los datos originales es relativamente sencillo dar con el contenido del hash, pero especialmente complicado si los datos se desconocen (Wikimedia: The Free Encyclopedia, 2018). Esto se hace con fines de seguridad.

II.2. Minería y Gobernanza en la Cadena

La minería consiste principalmente, en registrar operaciones en la cadena de bloques, verificando si éstas son válidas o no de acuerdo con las reglas de consenso establecidas en el protocolo, acreditando que el usuario tenga los fondos suficientes para realizarla, empacándolas en bloques y añadiendo el encabezado del bloque anterior a la información del nuevo bloque, junto con un sello que marca la fecha y hora de la transacción¹². Esto es de suma importancia, dado que para evitar que un usuario envíe 50 bitcoins a dos sujetos al mismo tiempo, teniendo él únicamente 50, se registra sólo la primera operación basándose en la fecha y en el *Proof-of-Work* (“PoW”), solucionando el problema del doble gasto y de la escases. El PoW consiste en intentar resolver un problema matemático complejo, expuesto a mayor profundidad a continuación. Éste es un procedimiento que consume poder de procesamiento, energía y tiempo, con el objetivo de que sea complicada la creación de un nuevo bloque que posteriormente se propague en la red, buscando hacer más dificultoso el añadir información validada a la cadena. El concepto de PoW es fundamental para la red ya que permite a cientos o miles de nodos que no se conocen entre sí ponerse de acuerdo en el orden de las transacciones y permitir su registro en el orden adecuado. Además, evita que un atacante inunde la red de datos falsos o incorrectos al asignarle un costo a agregar cada pieza de información, haciendo económicamente inviable un envío masivo de transacciones falsas y ejecutar un *sybil attack*¹³.

Explicado de una manera más detallada, el proceso del PoW es el siguiente¹⁴: El minero propone la creación de un nuevo bloque con la información de las transacciones¹⁵ que es combinada con el *hash* del bloque anterior de más reciente

¹² Para validar la información de fecha y hora el minero verifica que esta sea mayor a la del bloque anterior y que sea de por lo menos de dos horas en el futuro, porque los bloques se crean en promedio cada diez minutos. (Buterin, 2013, p. 7)

¹³ Una parte fundamental del valor de una cadena de bloques es su resistencia a ser modificada por usuarios que controlan los nodos que pueden registrar transacciones falsas o inexactas, esto se logra asociando un costo a subir información a la cadena, como lo es PoW. Para más información ver (Newsome, et al., 2004)

¹⁴ (Hesiod Services LLC, 2013)

¹⁵ Las transacciones deben de ser colocadas en el orden en el cual sucedieron.

creación en la red y un *nonce*¹⁶, esto da como resultado un *hash* nuevo, que funge como título o encabezado del nuevo bloque. Como parte de este proceso se le dan diferentes dígitos al *nonce*, cuyo valor se debe establecer de modo que se logre que el *hash* del bloque en construcción contenga una serie de ceros al inicio¹⁷, tal como está establecido en las normas que rigen al sistema, las reglas de consenso.

Es imposible predecir qué serie de números (*nonce*) dará como resultado que el *hash* se considere correcto, por lo que el minero debe de empezar con un valor cero e intentar con cada número hasta dar con el indicado, mediante prueba y error. Esta es la parte más complicada del proceso, y la que consume más tiempo¹⁸. Esto tiene como resultado que la suma de todos los datos que contiene el bloque, incluido el *nonce* dé como resultado que los primeros dígitos del *hash* sean cero. Una vez alcanzado este valor el *hash* es considerado como “válido” por la red. A medida que el tiempo pasa y más mineros se añaden a la red, se ajusta la dificultad para hacer más complicado dar con el número del *nonce* que dé como resultado el *hash* deseado, haciendo más probable que éste sea más alto y sea necesario probar una mayor cantidad números para encontrar el correcto. Esta operación es difícil de realizar, pero una vez encontrado el resultado es fácilmente comprobable por otros miembros de la red, que lo verifican y en caso de considerarlo correcto lo añaden al registro, propagándolo. En la medida que se siguen creando y colocando bloques sobre uno creado con anterioridad, se considera que el primero es “sólido” y el riesgo respecto a ese bloque disminuye. Por esto es por lo que las operaciones denominadas en bitcoin no se consideran firmes hasta que un cierto número de bloques han sido creados después del que registró la operación¹⁹, conociéndose este concepto como confirmación de bloques.

¹⁶ Término que viene del inglés *non sense* y que es cambiado a voluntad para crear nuevos valores de comprobación.

¹⁷ (bitcoinwiki, 2011)

¹⁸ Como se mencionó con anterioridad, el *hash* se genera con base en la información que se introduce en la función *hash* y cuyo resultado es impredecible, por lo que se hace en el proceso es introducir información (combinación de transacciones, *hash* del bloque anterior y *nonce*, entre otros) una y otra vez hasta que arroje el resultado deseado.

¹⁹ (Akita, 2017)

Una vez que el bloque fue minado y diseminado, no es posible realizar un cambio inadvertido. En caso de que la información contenida en un bloque fuese modificada, el *hash* cambiaría, y el *nonce* que fue generado para el conjunto de datos anterior ya no daría como resultado que los primeros cuatro dígitos fueran cero²⁰, por lo que perdería la característica de ser un bloque válido en la cadena. Asimismo, si un bloque intenta ser modificado no sólo se evidenciaría en sí mismo sino en todos los subsecuentes, ya que la red detecta que el *hash* del bloque anterior que contiene el bloque siguiente ya no es el mismo, por lo que cambiaría la composición del *hash* del siguiente bloque, provocando una reacción en cadena.

Por ejemplo, si en una cadena de diez bloques se cambian los datos almacenados en el bloque uno, después de ser minado y lograr que los primeros cuatro dígitos del *hash* hayan tocado cero y por lo tanto se considere válido el bloque, el *hash* del primer bloque cambiaría, dado que se altera la información que representa, por lo que la red lo mostraría como una modificación no autorizada. El bloque número dos igualmente se vería afectado, ya que contiene el *hash* del bloque anterior como parte de la información que da forma a su propio *hash* que a su vez cambiaría, perdiendo su estampado de confianza, y así sucesivamente hasta el bloque diez afectando a toda la cadena, evidenciando un intento de alteración en la información registrada.

Sin embargo, existe el riesgo de que posterior a la modificación los bloques fueran minados de nuevo, buscando el *nonce* correspondiente, y se firmaran nuevamente, presentándose ante el usuario como no modificados. Gracias al protocolo *blockchain* esto no es viable, dado que se trata de una red descentralizada. Las operaciones no se guardan en un servidor central que se pueda hackear. En su lugar, la información se disemina en miles de equipos de cómputo que voluntariamente forman parte de la red (también conocidos como nodos), por lo que a pesar de que las transacciones pueden ser modificadas en una o más computadoras, la red detecta la disonancia y la rechaza, señalando la cadena más

²⁰ Al cambiar la información contenida en el bloque el hash previamente generado ya no es válido, ya que corresponde a la información previa.

larga como la correcta, entendiendo la más larga como en la que se ha realizado más trabajo computacional. Esto funciona para prevenir un ataque ya que mientras el agente hostil dedica sus recursos a la diseminación de datos falsos o inexactos, la cadena “correcta” se seguirá construyendo, por lo que al final de la operación del atacante los mineros ignorarán “su” cadena y continuarán montando bloques en la que no sufrió el ataque.

Empero, existe un riesgo. El creador del protocolo teoriza que un ataque exitoso sería posible si un agresor lograra controlar 51% o más del poder computacional de la red. No obstante, el embate únicamente sería posible con una transacción reciente, entre más nueva, mejor. Esto sucedería de la siguiente manera: El atacante enviaría una determinada cantidad de bitcoins a otro usuario y una vez confirmada la operación enviaría otra transacción de la misma cantidad a su cuenta, pero ésta sería rechazada, porque esos bitcoins ya no son suyos, ya los gastó. Para darle la vuelta a esto, el atacante minaría otra versión del bloque que contiene su transacción, pero modificando la información de esta, para hacer parecer como si nunca hubiera enviado los bitcoins al otro usuario en primer lugar. Para hacer esto no sólo tendría que minar el bloque que contiene la transacción modificada, sino todos los creados después de ese, teniendo que ir más rápido que todos los demás mineros juntos, cosa que solo podría hacer si tuviera más del 51% del poder computacional de toda la red, alcanzando la longitud de la cadena “original” y superándola. De esta manera tendría éxito, ya que crearía la cadena más larga y por lo tanto la que sería considerada como válida²¹.

Pero esta posibilidad es prontamente declarada como muy poco probable, ya que como se explica en el Reporte:

“Si un atacante codicioso logra reunir más poder de procesamiento que todos los nodos²² honestos, tendría que decidir entre usarlo para

²¹ Este ejemplo fue extraído de (Buterin, 2013, p. 8)

²² Existen varios tipos de nodos, el nodo completo es aquel que almacena toda la información registrada en la cadena de bloques, actualmente varios gigabytes que aumentan hora a hora. Del mismo modo, existen los nodos ligeros que no tienen la copia completa de la información de la cadena, sólo los encabezados de los bloques.

defraudar gente robando lo que les pagó, o usarlo para generar nuevas monedas. Él encontraría más redituable jugar respetando las reglas, ya que dichas reglas le favorecerían con más monedas, más que a todos los demás participantes de la red combinados, que quebrantar el sistema y la validez (o base) de su propia riqueza.”²³

Regresando al tema, además de registrar las operaciones, por lo cual los mineros reciben una retribución²⁴ pagada por el usuario y que aumenta en la medida que se desee que una operación se registre más rápidamente, la minería realiza otras dos funciones claves en la red de Bitcoin, la generación y colocación de nuevos bitcoins²⁵ y gobernanza. Los mineros cumplen la tarea de generar nuevos bloques que traen consigo la creación de nuevos bitcoins que obtiene el minero²⁶ como parte de su contraprestación. Esto fue establecido en el Reporte, como parte de las reglas de consenso, y fue así como surgieron los primeros bitcoins²⁷. No existe una autoridad central que emita moneda, sino que los mineros ponen más y más activos en circulación manteniendo la circulación de los ya existentes²⁸. Este proceso es casi aleatorio, dado que es muy poco probable predecir en qué momento se generará un nuevo bloque y se recompensará con nuevos bitcoins²⁹.

En otro orden de ideas, y antes de continuar con las funciones de la minería es pertinente abordar ciertos problemas relativos a la minería que afectan la velocidad de procesamiento de transacciones de la red. En teoría, cualquier aparato con poder

²³ (Nakamoto, 2008, p. 4)

²⁴ Esta comisión es decidida por lo mineros en una especie de decisión de libre mercado tomando en cuenta oferta y demanda. (Buterin, 2013, p. 27)

²⁵ (Antonopoulos, 2017, p. 287)

²⁶ (Nakamoto, 2008, p. 4)

²⁷ Es importante señalar que esto es una sobre simplificación de la manera en la cual la red maneja las transacciones e incluso el traslado de valor, incluyendo las transacciones llamadas *coinbase* la cual permite la introducción de nuevos bitcoins en circulación. En caso de que se desee profundizar en el tema leer (Antonopoulos, Mastering Bitcoin, 2017)

²⁸ *Ídem*

²⁹ Es importante distinguir entre las dos posibles fuentes de ingreso de un minero, el pago de comisiones por la inscripción y diseminación de operaciones y los que obtienen derivados de la creación de un nuevo bloque. Esto sucede a un ritmo fijo y que cuya frecuencia disminuye con el tiempo. (Antonopoulos, 2017, p. 287)

computacional puede minar³⁰, y en la práctica muchas computadoras de diversas capacidades lo hacen. Esto trae consecuencias buenas y malas, las principales ventajas son la seguridad y estabilidad que se le da a la red, ya que, al reducir las barreras de entrada a ser minero, la cantidad de estos aumenta constantemente, haciendo la red más estable y segura, dado que las operaciones se registran en más nodos. No obstante, también trae una desventaja imprevista, que ha resultado muy gravosa. Las operaciones de la red descentralizada se registran en todos los nodos³¹, por lo que la velocidad de la red se ve afectada negativamente cuando hay nodos lentos en la misma, limitando la cantidad de transacciones por segundo que pueden ser procesadas. Cabe destacar que esto no era un problema cuando surgió Bitcoin debido al bajo volumen de operaciones, pero hoy en día se ha convertido en una complicación grave, al ser cada vez más las transacciones en la red.

Existen diversas soluciones propuestas ante la problemática³², todas presentando ciertos inconvenientes. La primera, en términos generales, es dejar el sistema Bitcoin tal cual es y aceptar que los usuarios migrarán a otros sistemas basados en el mismo protocolo *blockchain* que permitan una mayor rapidez en el reflejo de las operaciones.

La segunda es incrementar el tamaño de los bloques. Esta solución parece ser adecuada al corto plazo, no obstante, existe el riesgo de que al aumentar el tamaño de los bloques estos únicamente puedan ser manejados por supercomputadoras y se caiga en una centralización *de facto*.

³⁰ No obstante, actualmente se ha creado un mercado de equipos computacionales especializados que permiten que el costo de la electricidad no sea más alto que los ingresos que se obtienen de la minería. Hoy en día es no rentable iniciar una operación de minería de bitcoin sin tener equipo especializado con altísimo poder computacional y extremadamente eficiente en términos energéticos.

³¹ El espacio ocupado por el registro de la multitud de operaciones es optimizado mediante un concepto conocido como *Merkle Trees*. Hay dos tipos de nodos, el completo, que tiene todas las operaciones registradas, y el ligero, que no tiene los suficientes recursos para hacerlo o simplemente no lo desea. En el nodo ligero se almacenan los hashes de los hashes de los hashes de las transacciones, o sea que toma los títulos de varios bloques y los convierte en hash. Se verifican que los hashes sean consistentes con los anteriores y así solo hay que registrar los hashes más recientes, que se entienden validados, y no así toda la información. (Buterin, 2013, p. 9)

³² (Zamyatin, 2017)

La tercera consiste en la minería de fusión o “*Merge Mining*” que consiste en minar en dos cadenas independientes, o más, de forma simultánea. Es decir, se buscan valores del *nonce* y se comprueban en múltiples cadenas al mismo tiempo para ver si es el número correcto. Al minar en diversas cadenas se aumenta la eficiencia del proceso al acrecentar las posibilidades de que se encuentre la solución en alguna de ellas. A un nivel teórico esta solución parece viable, pero existe el gran peligro de que al no estar unidas las cadenas si los mineros no encuentran suficientemente rentable mantener una de ellas pueden abandonarla teniendo como consecuencia final su desaparición.

Por lo tanto, parece que sólo es posible escoger dos características de tres posibles: descentralización, escalabilidad y seguridad³³. Este es un problema sobre el que actualmente la comunidad sigue trabajando y para el cual seguramente en poco tiempo se presentarán soluciones interesantes.

Retomando el tema anterior, además de cumplir con una función técnica, los nodos forman parte de la gobernanza de la cadena. Esto significa que, así como no hay una autoridad que tenga el control sobre la emisión de la moneda tampoco hay un ente individual que gobierne la cadena. Las decisiones se toman a través un consenso entre los nodos que votan conforme al poder de procesamiento que aportan al *blockchain*. En otras palabras, desarrolladores de la comunidad³⁴ proponen cambios a la red; si los nodos están de acuerdo con las propuestas transformaciones en la cadena seguirán construyéndola mediante la creación de nuevos bloques, pero si no encuentran los suficientes incentivos para continuar pueden abandonarla, efectivamente destruyéndola. Lo anterior es relevante para entender el concepto de bifurcación o “*fork*”³⁵.

³³ *Ídem*

³⁴ Para más información de los desarrolladores voluntarios que influyen en el desarrollo del protocolo actualmente visitar: <https://github.com/bitcoin/bitcoin/graphs/contributors> y para más información acerca de la historia y desarrollo de la comunidad ver: (Wang, 2017)

³⁵ El termino proviene del léxico de los desarrolladores, principalmente, de Linux, en el cual significa “el acto de tomar una pieza de código de un proyecto de software gratuito y bifurcarlo” mediante una “decisión de algunos desarrolladores dentro de un proyecto abierto de duplicar el código de un

II.3. Bifurcaciones o *Forks*

El sistema Bitcoin, antes que ser una red de pares que mantiene un registro, es un *software*³⁶ que corre en los nodos y les permite conectarse y crear una red. Este *software* es libre y puede ser visto y modificado por cualquier usuario³⁷. Asimismo, los cambios que se le realizan pueden tener diferentes consecuencias:

“Las modificaciones pueden resultar en que el software permanezca compatible con la red de Bitcoin o lo deje de ser. Cambios que no rompen la compatibilidad son referidos como cambios en la política de reglas del software (*software’s policy rules*)³⁸. Cambios que rompen esta compatibilidad son conocidos como cambios en las reglas de consenso del software (*software’s consensus rules*) que se refieren a las reglas sobre las cuales la red completa debe de estar de acuerdo”³⁹

“Crear cualquier modificación personalizada del núcleo del software es llamada una “bifurcación” (*forking*) del código. Este término tiene dos acepciones, la primera se refiere a una bifurcación en el software y la segunda a una en la cadena de bloques.”⁴⁰

“Correr un software bifurcado que no altere las reglas del consenso no causa una bifurcación de la cadena, los nodos que corren el software estarán de acuerdo con la red existente de Bitcoin respecto al estado de las transacciones en el registro. En contraste, correr software bifurcado que altere las reglas de consenso resultará ya sea en una completamente nueva cadena de bloques o en una nueva cadena de bloques de Bitcoin. Los nodos que corran el nuevo software reconocerán una serie de transacciones confirmadas alternativas en su propia red como correctas.”⁴¹

proyecto y mantenerlo de manera separada para crear una invención derivada” (Hill, 2005) en (Van Valkenburgh, 2016, p. 5)

³⁶ (Bonneau, et al., 2015) en (Van Valkenburgh, 2016, p. 5)

³⁷ El código puede ser consultado en la siguiente liga: <https://github.com/bitcoin/bitcoin/blob/master/COPYING> consultado el 27 de febrero de 2018

³⁸ Un ejemplo podría ser una actualización.

³⁹ (Van Valkenburgh, 2016, p. 5)

⁴⁰ *Ídem*

⁴¹ *Ibídem*, p.6

La acepción más relevante y que puede tener un impacto más profundo en la regulación, es la que implica que una bifurcación en la cadena de bloques provoca que existan dos versiones alternativas del historial de transacciones⁴². Dependerá de los nodos escoger cual es la correcta, mediante la continuación de trabajo en la que consideren como tal. Por lo tanto, son los mineros los que deciden si aceptan o no un cambio en la cadena, votando con su poder de procesamiento en la cadena.

⁴² *Ibidem*, p.5

II.4. Llaves Públicas, Privadas y Carteras

Pasando al siguiente tema, en el Reporte, el autor también hizo hincapié en otro aspecto que resulta de suma importancia: la privacidad. Nakamoto rompe con el modelo tradicional en el cual las partes no conocen todos los datos de su contraparte, pero la autoridad central, generalmente un banco, conoce los datos de ambos. En su modelo, todas las transacciones se anuncian de manera pública a través de la red *blockchain*⁴³ por lo que todos pueden ver las operaciones y las “direcciones” de los participantes, pero no hay información que vincule dichas direcciones con los usuarios⁴⁴. Esto se logra a través de las llaves públicas y privadas.

Cada usuario de la red que realice una transacción posee dos cadenas de caracteres⁴⁵, una de ellas se conoce como llave pública y otra como llave privada, que está bajo el exclusivo control de su titular. La primera es análoga a un número de cuenta bancaria común y corriente y se utiliza para poder mandar valor al usuario y puede ser dado a conocer al público. Idealmente no está relacionada de ninguna manera con los datos del usuario, como nombre o domicilio, sin embargo, si se conoce la identidad del tenedor de la llave pública es posible conectar las operaciones que tuvieron como origen o destino la dirección⁴⁶ con su emisor o destinatario. A su vez, la llave privada es similar a una contraseña a través de la cual el usuario accede a sus fondos. Se genera en relación con la llave pública, sin que la privada pueda ser derivada de la pública⁴⁷. Dependiendo del tipo de cartera

⁴³ (Nakamoto, 2008, p. 6)

⁴⁴ De acuerdo con el autor esto es similar a las operaciones realizadas en la bolsa de valores en la cual se conocen las operaciones, pero no quien las realiza.

⁴⁵ “Una llave privada es un conjunto de caracteres alfanuméricos utilizados para gastar o mandar cantidades de Bitcoin. Tiene una longitud de 256-bits y es escogido de manera aleatoria en el momento que la cartera es creada. Una llave pública es un número o dirección a través de esta se reciben fondos que se deriva de la llave privada mediante funciones matemáticas criptográficas. Es imposible encontrar la llave pública utilizando la llave privada. (Khatwani, 2018)

⁴⁶ Esto puede ser evadido con un *mixer*, que consolida diversas operaciones y las manda desde una sola cuenta ajena al usuario, que hace que sea muy complicado saber de qué usuario provienen los valores. Para más información ver (Financial Action Task Force, 2014, p. 6)

⁴⁷ (Brownworth, 2017)

que se utilice, es posible utilizar una dirección para cada operación y maximizar la privacidad del usuario.

Además de servir como contraseña, la llave privada es utilizada para “firmar” transacciones. Al ser rubricadas las transacciones se genera una “firma” única que acompaña la operación⁴⁸. El que recibe el pago, y el propio sistema, al conocer la llave pública, la transacción y la firma, entendida como aquella que fue generada a partir de la llave privada, puede saber si la transacción efectivamente fue emitida por el que dice ser el expedidor ya que las tres se relacionan matemáticamente. La llave privada jamás debe de ser dada a conocer a nadie, ya que si alguien obtuviera ambas secuencias de caracteres podría vaciar los fondos asociados con ellas sin que el usuario propietario pueda hacer algo al respecto⁴⁹.

Para poder operar en la red, el usuario debe de tener una “cartera”, que le permita acceder a la cadena de bloques y registrar traslados de valor. De acuerdo con A. Antonopoulos, las carteras “se tratan de aplicaciones que sirven como la interfaz de usuario primaria, controlando el acceso a los activos de un usuario, manejando las llaves y dirección de este, verificando el “balance” y creando y firmando transacciones utilizando las respectivas llaves privadas”⁵⁰. Existen diferentes tipos de las también llamadas “*wallets*”⁵¹. Las carteras de Hardware, como su nombre lo indica consisten en un pedazo de hardware tal como un USB, disco duro o aparato especializado, que al no estar conectados a internet permanentemente poseen un

⁴⁸ (Khatwani, 2018)

⁴⁹ El riesgo de esto disminuye mediante la implementación de la tecnología multi firma (*multisig*) que divide la responsabilidad de la posesión de cripto-activos. Mediante este sistema se requiere que dos o más sujetos firmen una transacción para que esta sea autorizada. La idea es que se le imponga al cripto-activo un gravamen especial que requiera la participación de diversas personas para disponer de ellos. (bitcoinwiki, 2017). Las direcciones de carteras de Bitcoin que están reforzadas con este avance se reconocen por que empiezan con el número 3. Esta tecnología ha sido prontamente adoptada por las casas de cambio que operan con activos virtuales. Dado que por las grandes cantidades de valor que manejan son un blanco atractivo para hackers que buscan robar los valores criptográficos de sus clientes. Mediante esta tecnología se establece una regla que restringe el movimiento de valores a la utilización de dos de tres llaves. Dichas llaves se resguardan en lugares diferentes, por lo que aún si los servidores de la empresa se ven comprometidos se necesitaría otra llave para mover los fondos.

⁵⁰ (Antonopoulos, 2017, p. 145)

⁵¹ (Khatwani, 2017)

grado de seguridad más alto. Las carteras móviles son aplicaciones de sistemas operativos móviles que presentan una gran facilidad en su uso, pero tienen el inconveniente de que en caso de robo o pérdida del equipo celular existe la posibilidad de no recuperar la cartera⁵² si no se tomaron las medidas de previsión adecuadas o ver robados los fondos. Asimismo, hay aquellas que se ejecutan en una computadora de escritorio que corra cualquiera de los tres sistemas operativos principales, *macOS*, *Windows* y *Linux*. Igualmente, hay la posibilidad de utilizar carteras en línea, que básicamente son servicios web accesibles mediante internet. Las llaves privadas de este tipo de cartera se almacenan en línea, por lo que a pesar de ser convenientes son las más inseguras, siendo vulnerables a un acceso no autorizado por un tercero. Por último, están las de papel, que son un pedazo de papel con una llave pública y privada impresas en ellas, que son seguras a robo digital, pero vulnerables ya que el papel puede dañarse o perderse lo que llevaría al propietario a perder el monto almacenado en la misma.

Del mismo modo, es necesario mencionar que existen carteras determinísticas y no determinísticas. En las primeras “todas las llaves son derivadas de una sola llave maestra, conocida como la semilla o “*seed*”. Todas las llaves en este tipo de cartera están relacionadas unas con otras y pueden ser generadas otra vez si se tiene la semilla”⁵³, por lo que si se pierden las llaves privadas pueden ser recuperadas. Asimismo, otorga un mayor grado de privacidad al usuario, dado que este tipo de *wallet* es propicia para no reutilizar direcciones, generando una nueva para cada operación. En el segundo tipo de cartera “cada llave es generada de manera independiente de un número aleatorio. Las llaves no están relacionadas unas con otras, también es conocida como “Sólo un Montón de Llaves” o por sus siglas en inglés JBOK”⁵⁴.

Paralelamente, conforme a su conectividad, existen dos clasificaciones de carteras. El primer rubro se comprende de aquellas que están constantemente en línea, conocidas como carteras calientes o *hot wallets*. A través de éstas es más fácil

⁵² Siempre y cuando se trate de una cartera determinística.

⁵³ (Antonopoulos, 2017, p. 146)

⁵⁴ *Ídem*

mover valor, pero son más vulnerables al robo de fondos. Por otro lado, están las carteras no conectadas, llamadas frías o *cold wallets*, las cuales ofrecen mayor seguridad, pero menor disponibilidad de los activos guardados en ellas.

De igual manera, es posible agrupar las carteras conforme a quien mantiene la custodia de las llaves que dan acceso a los fondos, pudiendo tener o no el usuario custodia de ellas. Las últimas son aquellos servicios en los cuales el usuario confía en un tercero para que mantenga sus llaves, como una cartera de un intercambio. Este sistema es más conveniente de usar, pero vulnerable a un ataque al servidor que las aloja. En esta modalidad, el tercero que ofrece el servicio posee las llaves y tiene custodia de los activos del usuario. En caso contrario, cuando los usuarios mantienen la custodia de las llaves, los fondos de la cartera están exclusivamente bajo su control. Si el propietario no pierde sus llaves, nadie puede tener acceso a su cartera sin su autorización, proveyéndolo así de mayor seguridad, pero disminuyendo facilidad de uso⁵⁵.

Retomando el funcionamiento del protocolo, y relacionándolo con las carteras, tenemos que éste funciona como un sistema de transición de estado⁵⁶ en cuanto a envío de valor se refiere, ya que registra el estado antes y después de una transacción. Es decir, una operación es autorizada verificando las transacciones hechas con anterioridad por el usuario, con las de ingreso sumando a su “balance” y las de egreso restándole. En el caso de un “depósito” el sistema considera válida una transacción si existen operaciones de ingresos que permitan realizar la operación⁵⁷. Conectándolo con el párrafo anterior, una cartera no almacena valor, sino que “contiene” las llaves para acceder al mismo, registrado en el *blockchain*, pareciéndose, en este sentido, más a un llavero que a una cartera.

⁵⁵ (Khatwani, 2017)

⁵⁶ (Buterin, 2013, p. 1)

⁵⁷ (Buterin, 2013, p. 6)

II.5. Valuación y Valor

En otro orden de ideas, una característica muy controversial de bitcoin es el hecho que, a diferencia de las monedas fiduciarias, su valor no está respaldado por las reservas de un país o la productividad del mismo, sino que tiene el valor que la comunidad está dispuesta a darle. Es decir, su precio se basa en la oferta y la demanda⁵⁸. El qué determina el valor del bitcoin es motivo de amplia discusión, y ameritaría por sí mismo un trabajo dedicado a responder a la pregunta. No obstante, para efectos de la presente tesis, se concluirá que vale lo que el público esté dispuesto a pagar por él.

⁵⁸ Esto no evita que haya ciertas voces que defiendan que el valor de cada bitcoin está relacionado con el que costo de minarlo u otros factores, para más información, consultar (Hayes, 2017). De igual modo, es posible sostener que su precio es dado por la utilidad que representa la red Bitcoin para otros proyectos, fungiendo bitcoin como una especie de materia prima que permite el mantenimiento de la red.

II.6. Análisis

A modo de conclusión, es debido asentar que hoy en día Bitcoin permite el traslado de valor a nivel mundial sin ninguna limitación y en la mayoría de los casos, con comisiones más bajas y en tiempos mucho menores de lo que tardaría una transferencia internacional de dinero a través de métodos convencionales. Pero lo más valioso de Bitcoin no es eso, lo más importante es la tecnología que introdujo al mundo, *blockchain*. Satoshi Nakamoto presentó al público más que un activo, estableció un medio de pago revolucionario y una manera en la cual computadoras conectadas a la misma red que no guardan ninguna relación pueden alcanzar un consenso acerca de datos compartidos⁵⁹. Esto permitió crear una red abierta que contiene una base de datos descentralizada, transparente, abierta, auditable, neutral, en la cual intentos de modificación son evidenciados y es resistente a ataques *sybil*. Asimismo, este registro tiene la cualidad de inscribir las operaciones en el orden adecuado, sin más interacción de los nodos más que la que mantienen a través de la red, logrando un consenso descentralizado. El protocolo tiene el potencial para cambiar la manera en la cual se entiende el manejo de datos hasta ahora y es la base para entender el valor y el funcionamiento de los activos virtuales. Además, cabe señalar que Bitcoin no fue el último de su clase, sino que pavimentó el camino de muchos otros que abrían de seguirle, siendo el más importante de ellos Ethereum.

⁵⁹ (Van Valkenburgh, 2017)

III. La Evolución de la Tecnología

En este capítulo se pretende analizar como evolucionó la tecnología *blockchain* a través del tiempo, y cómo eventualmente esto desembocó en el desarrollo de una nueva plataforma basada en la misma tecnología llamada Ethereum. Esta nueva plataforma se ha convertido en un proyecto de referencia en materia de infraestructura de *blockchain* y ha cambiado completamente el cuadro de los activos virtuales en los últimos años. Actualmente, el ether, su medio de pago es el segundo activo más importante en términos de capitalización de mercado⁶⁰, además de permitir la emisión de miles de *tokens* o sub-monedas por parte de cientos de emprendimientos que junto con la plataforma han moldeado el panorama actual de activos virtuales.

Después de la llegada de bitcoin y de su protocolo, no fueron pocos los que vieron el potencial que la tecnología representaba. Muchos se dieron cuenta que el sistema sobre el cual descansaba Bitcoin no servía solamente para registrar transacciones. La comunidad reconoció las posibilidades de un registro descentralizado, transparente y resistente a modificaciones no autorizadas. Así nació la idea de los activos criptográficos 2.0, construidos sobre el mismo protocolo, con la intención de llevar a la siguiente etapa la tecnología.

En este contexto, surgieron múltiples proyectos que intentaron utilizar la infraestructura existente de Bitcoin (siendo esta su cadena) como base para una red propia en la cual se transmitirían no solo bitcoins, sino todo tipo de información. Entre lo que se podía registrar estaba el cambio de propiedad de cualquier cosa⁶¹, el registro de nombres de dominio mediante meta monedas llamadas *Namecoins*⁶²

⁶⁰ Para información en tiempo real de varios indicadores de activos virtuales, entre ellos la capitalización de mercado, visitar: <https://coinmarketcap.com/>

⁶¹ (Mizrahi, s.f.)

⁶² Para más información acerca del proyecto visitar: <https://namecoin.org/>

o cualquier otro dato. Para poder introducir la información en la cadena se idearon múltiples métodos, uno de ellos es conocido como “colorear monedas”⁶³.

El coloreado consiste en marcar fracciones de bitcoins, acción de la cual proviene el término, mediante la emisión de una cuenta común y relacionarlos a una llave privada que representa al propietario. Usando este procedimiento, se pueden enlazar activos físicos, como un inmueble, acciones de una empresa o cualquier otra cosa, con un bitcoin coloreado, haciendo posible el registro en la cadena de Bitcoin de la transmisión de su propiedad. Un ejemplo podría ser un automóvil cuya tenencia se vincula mediante la anterior técnica a una fracción de bitcoin utilizando su número de motor. Así, cada vez que el auto cambie de propietario la fracción de la moneda criptográfica también lo haría al respectivo comprador. De esta manera se registraría la transacción como un envío de bitcoins con un especial significado para las partes y los terceros interesados, que saben que lo que representa dicha transacción. El registro en ocasiones es complementado con un servidor que establece el vínculo de la particular moneda, o fracción de ella, con un activo del mundo real. Otro método consiste en la introducción de una pequeña cantidad de información en la moneda, de modo que sea esta la que indique a que activo real corresponde. De manera similar, Bitcoin también permite una versión limitada de lo que ahora se conoce como “Contratos Inteligentes”⁶⁴ concepto que será explorado en las páginas siguientes.

Además de las anteriores aplicaciones, muchas otras surgieron del intento aprovechar el potencial de la tecnología. Al hacerlo sobre infraestructura existente de un proyecto anterior, se genera la ventaja de no tener que crear una nueva cadena para registrar operaciones, siendo posible “montarse” en la robusta *blockchain* de Bitcoin, que cuenta con cientos de nodos trabajando. Por otro lado, el intento de crear una cadena nueva representa un despliegue de recursos considerable ya que es necesario crear incentivos para la atracción y retención de

⁶³ (Rosenfeld, 2012, p. 1)

⁶⁴ (Buterin, 2013, p. 12)

nodos. No obstante, el intento de utilizar Bitcoin para otros fines estaba terriblemente limitado, ya que la unidad de valor no fue diseñada para ser una base para otros proyectos, fue diseñado para ser un método de pago.

Junto con las limitantes señaladas con anterioridad, muchas otras fueron evidenciadas por Vitalik Buterin, el creador del ecosistema Ethereum. Él sostiene que la manera de operar de Bitcoin no estaba, ni está, preparada para verificar la validez de las transacciones de los protocolos montados en ella, ya que el sistema únicamente analiza una transacción y determina su validez con base en el balance del usuario que envía la transacción. Por lo tanto, lo que los mineros podrían registrar como una operación válida en el contexto de un traslado de valor de bitcoin podría no serlo de acuerdo con las reglas específicas del proyecto. Por otra parte, en ciertos casos, se requiere de un servidor central que almacene el significado de cada transacción. A modo de ejemplo, el registro almacenado en la cadena únicamente mostraría un cambio en la propiedad de cierta moneda, pero no le sería posible interpretar que representa la operación, como puede ser la compraventa de un auto o una casa. Por último, resulta evidente que la utilización de un servicio centralizado, para el registro de cierta información que permita el funcionamiento del esquema, es un contrasentido a los principios fundamentales de un sistema descentralizado⁶⁵, por lo que una nueva plataforma debía que ser creada si se querían superar estas limitaciones.

⁶⁵ (Buterin, 2013, p. 11)

III.1. Ethereum

El ecosistema estaba inmerso en el anterior panorama cuando Ethereum fue creado en el año 2013. La presentación del proyecto que da su creador Vitalik Buterin ha ido cambiando con el tiempo en la medida que la tecnología ha ido evolucionando. En un principio, la plataforma se comparaba con otros proyectos de tecnología *blockchain* que existían en ese momento y se definía con base en esa comparación. Sin embargo, la documentación del proyecto se ha actualizado con el tiempo, por lo que, en la revisión más reciente de la misma, que data del 2017, la definición se ha hecho más precisa, además de profundizar en ciertos aspectos. No obstante, la definición original, tal cual se plasmó en el “*Ethereum White Paper*” con título “*A Next Generation Smart Contract & Decentralized Application Platform*” (Una plataforma de nueva generación de contratos inteligentes y aplicaciones descentralizadas), es la siguiente:

“El propósito de Ethereum es el combinar y mejorar los conceptos de scripting, *alt-coins* y meta protocolos montados en la cadena (de Bitcoin), permitiendo a los desarrolladores crear aplicaciones con las características de arbitrariedad, base en el conceso, escalabilidad, estandarización, funcionalidad completa, facilidad de desarrollo e interoperabilidad ofrecidas por cada uno de los paradigmas anteriormente mencionados al mismo tiempo. Ethereum hace esto construyendo lo que es básicamente la mejor base fundacional: una cadena de bloques con un lenguaje de programación completo Turing⁶⁶, que permite a quien sea escribir un Contrato Inteligente y aplicaciones descentralizadas a través de los cuales pueden crear sus propias reglas de propiedad, formatos de transacción y funciones de transición de estado.”⁶⁷

⁶⁶ Un lenguaje de programación que puede correr más de un tipo de programa.

⁶⁷ (Buterin, 2013, p. 13)

III.1.1. *Ethereum Virtual Machine* (Funcionamiento de la Plataforma)

Ethereum es mucho más que un sistema de pagos, que si bien comparte con Bitcoin el estar basado en *blockchain*, tiene funcionalidades mucho más amplias. Se trata de una plataforma que permite a los desarrolladores crear “Contratos Inteligentes”⁶⁸ (“Contratos”) que ejecuten diversas funciones, como lo hace un programa en un ordenador. En otras palabras, es una especie de computadora (conocida como *Ethereum Virtual Machine*⁶⁹) no centralizada, que se aloja en *blockchain*⁷⁰, y que por lo tanto no existe físicamente en ningún lugar en su totalidad. En ella se puede programar prácticamente lo que sea, como un servicio de transmisión de la propiedad o cualquier otro que se pudiera ver beneficiado por el uso de *blockchain*. Por lo tanto, permite el desarrollo de diferentes tipos de aplicaciones descentralizadas alojadas en *blockchain*, incluido, pero no limitado, a registros de activos virtuales. De igual manera es importante recalcar que, a diferencia de Bitcoin, Ethereum cuenta con un líder visible. El proyecto es avanzado de manera abierta por diversos desarrolladores⁷¹ con el fundador del proyecto, Vitalik Buterin, a la cabeza, todos ellos forman parte de una organización sin fines de lucro llamada “Fundación Ethereum”.

Por lo tanto, Ethereum opera utilizando la misma tecnología que Bitcoin, pero llevándola mucho más allá. En el protocolo original, por diseño, únicamente se pueden registrar operaciones de intercambio de valor, o lo que es lo mismo, transacciones. La comunidad llevó esto al límite intentando transmitir y registrar otro tipo de información por medio del protocolo, pero de una manera muy limitada. El

⁶⁸ Definido como una serie de enunciados condicionantes que al momento de ser cumplidos detonarían una consecuencia, diferente al concepto jurídico.

⁶⁹ Se entiende como una computadora ya que, a diferencia de Bitcoin, que se registran estados de cuenta, se registran estado de una computadora. (Ethereum Foundation, 2016)

⁷⁰ Uno de sus cofundadores, el Dr. Gavin Wood, lo define como una computadora situado en la cadena de bloques capaz de ejecutar aplicaciones, algo similar a un script esparcido en el Blockchain. (Wood, 2015)

⁷¹ Para más información acerca de los desarrolladores presentes y pasados del proyecto, visitar: <https://www.ethereum.org/foundation> página oficial de la fundación Ethereum. Esta organización controla en cierta medida la dirección de la plataforma.

proyecto nace con estas limitaciones en mente, y constituye una plataforma que permite la libre creación de programas basados en la cadena de bloques. Estas aplicaciones son conocidas como *decentralized applications* o *dApps*⁷², y son un conjunto de Contratos, los cuales son creados mediante el envío de una transacción de datos transformado en código, que se aloja en el *blockchain* de Ethereum. Al respecto, Vitalik Buterin propone la existencia de tres categorías de aplicaciones programadas en la plataforma: las meramente financieras⁷³, las parcialmente financieras y las no financieras en absoluto⁷⁴.

El código se ejecuta en la computadora que es *Ethereum Virtual Machine*, la cual corre lo programado por los usuarios a través nodos, muy similares a los que mantienen la red de Bitcoin con un software que se actualiza constantemente. La primera versión fue llamada *Frontier* y fue una beta, después de esta, llegó la versión actual, *Homestead*⁷⁵ y en el futuro se liberará *Metropolis*.

Retomando la explicación del funcionamiento de la plataforma, en el protocolo Ethereum existen dos tipos de cuentas, las controladas de manera externa (“EOAs”, por sus siglas en inglés) con una llave privada, es decir por personas y las de contratos que son controladas por su código; el cual, una vez propagado en la red es inmodificable. De la misma manera, las cuentas de contratos son “activadas” por un EOA⁷⁶ mediante una transacción enviada a su dirección. Asimismo, las “transacciones” en Ethereum son parecidas a las que se encuentran en Bitcoin con ciertas divergencias. Por ejemplo, ambos tienen un *nonce*, el destinatario, la cantidad de valor a enviar y la firma, sin embargo, difieren en el concepto de Gas.

⁷² Para explorar una lista de aplicaciones descentralizadas, consultar el sitio web: <https://www.stateofthedapps.com/> Consultado el 20 de febrero de 2018

⁷³ Un ejemplo de estas sería un contrato de Ethereum de cobertura, en el cual dos individuos depositan en ether lo equivalente a mil dólares. Y al paso de un mes un individuo obtiene mil dólares de vuelta y el otro obtiene el valor restante. Uno de ellos se cubre contra la volatilidad y el otro especula a favor del ether.

⁷⁴ Para mayor información de los posibles usos no financieros (Catalini, 2017) de la tecnología *blockchain* consultar: <https://hbr.org/2017/03/how-blockchain-applications-will-move-beyond-finance>

⁷⁵ Si se desea profundizar en el tema se recomienda leer *Ethereum Homestead Documentation*.

⁷⁶ (Anon., 2017, p. 4)

En Ethereum existe una noción llamada “Gas”, que representa el precio que debe de ser pagado para activar el poder computacional de la plataforma. Éste es una especie de comisión que se debe de solventar ya sea para realizar un traslado de valor o por cada tarea computacional que ejecuta un nodo de la red y se abona en la moneda de la plataforma, ether.

Para poder realizar el pago al que se refiere el párrafo anterior, se define la variable *Gas*. De manera similar, es determinado por el usuario el precio que se le da a este (precio del *Gas* o *gasPrice*) así como lo máximo que se está dispuesto a pagar por él (*gasLimit*). El darle un “presupuesto” a la transacción cumple con dos funciones. La primera es que, al igual que con Bitcoin, un usuario que desea que su operación se propague por la red más rápidamente pagará más. La segunda consiste en que, al cobrar por cada operación procesada, se protege a la red contra un agente hostil que intente un ataque a los nodos a través de un programa que exija que se le corra de manera infinita. Se debe de mencionar que con el objetivo que el costo de las transacciones permanezca estable⁷⁷, se intenta que el valor del *Gas* permanezca igual ajustándolo a las variaciones de precio del ether. Por lo demás, también son parte de la transacción los datos o *data*, (los cuales son relevantes únicamente cuando se envía un mensaje a un contrato, que los puede leer y actuar de acuerdo con esta entrada y a lo que le indique su código) e *init*, que importa para transacciones que tengan por objeto la creación de un contrato ya que es el cuerpo del código que le da forma a un contrato de nueva creación y una vez que es ejecutado por primera vez queda fijado en el *blockchain*⁷⁸.

⁷⁷ (Anon., 2017, p. 49)

⁷⁸ (Kasireddy, 2017)

III.1.2. *Proof-of-Work* y *Proof-of-Stake* en Ethereum (Minería)

La minería utilizada para mantener la cadena de Ethereum es similar a la que se lleva a cabo en la cadena de Bitcoin. Las actualizaciones de estado de una cuenta son propagadas en la red a través de nodos mineros mediante una PoW de una manera muy parecida a como funciona en Bitcoin. Empero, para cuando Ethereum surgió ya se había tomado nota de las dificultades que había encontrado la minería en Bitcoin, siendo una de las principales la utilización de hardware especializado. En búsqueda de mayores utilidades, los mineros pasaron de minar con el *CPU*⁷⁹, que consume muchos recursos y hace lenta a la computadora huésped, a minar con el *GPU*⁸⁰ que es mucho más rápido y eficiente. Posteriormente, saltaron a un hardware especializado en la minería llamado “Circuitos Integrados para una Aplicación Específica” o “*ASIC*” por sus siglas en inglés.

Los *ASICs* hacen que los mineros sean mucho más eficientes en el registro de operaciones en la cadena, pero traen la desventaja de que son pocos los que pueden hacer una inversión lo suficientemente grande como para adquirir uno, ya no se diga varios, de estos equipos especializados. Lo anterior causó que múltiples mineros abandonaran la minería de Bitcoin, dado que minar con cualquier otro aparato que no fuera un *ASIC* dejó de ser rentable. No obstante, los que tuvieron el capital migraron a los equipos especializados, ocasionando una centralización *de facto*. Los niveles actuales de concentración son preocupantes, con los cuatro grupos (o como se les conoce: “*Miner’s Pools*”) de mineros más grandes generando, en el último año, cerca de 48% de los bloques nuevos. Esto trae graves riesgos de centralización y representa peligros adicionales si se consideran la cantidad de mineros que hay en China, y que por lo tanto están sujetos a su jurisdicción, dejando el destino de la red Bitcoin en las manos de muy pocas personas.

⁷⁹ Unidad Central de Procesamiento o en inglés: *Central Processing Unit*.

⁸⁰ Unidad de Procesamiento Gráfico o *Graphics Processing Unit* en inglés, comúnmente conocido como tarjeta gráfica.

Esta situación causó que desde su origen en Ethereum se desincentivara el uso de hardware especializado, optándose por la minería usando *GPU*, evitándose la minería con *CPU* por los problemas previamente mencionados⁸¹. La idea era evitar la centralización y procurar que el minero promedio fuera un usuario con una computadora común y corriente, incentivando la descentralización. No obstante, a pesar de las innovaciones de la plataforma, el problema de la lentitud de procesamiento de las operaciones no ha sido resuelto en su totalidad. Es importante mencionar que con el objeto de derribar este obstáculo existe la posibilidad de pasar de un esquema de PoW⁸² a uno de “*Proof-of-Stake*” (“PoS”⁸³) por problemas de manejo de volumen de operaciones en la red.

Por lo tanto, es importante mencionar que el esquema PoS es una manera de mantener la integridad de la red, “confiando” en aquellos usuarios que tienen mucho en juego respecto al activo virtual en cuestión. Para lograr esto, se bloquea una cantidad de cripto-activos del usuario por una cantidad predeterminada de tiempo, por lo que el participante tiene algo que perder si el proyecto llegara a fracasar. La idea detrás de esto es mover el costo de oportunidad desde fuera del sistema a dentro del sistema, ya en un esquema de prueba de trabajo o PoW se crea un incentivo de probar la mayor cantidad de trabajo posible⁸⁴, este crecimiento de trabajo tiene límites físicos, que en el caso de Bitcoin ya alcanza niveles preocupantes⁸⁵. Respecto al tema, Poelstra da una definición más detallada de cómo opera un esquema PoS:

“En un nivel básico y conceptual, la manera en la que trabaja el “PoS” es que los tenedores pueden bloquear sus valores por un periodo determinado de tiempo, rentando⁸⁶ la apuesta que se hace por dicha

⁸¹ (Buterin, 2013, p. 32)

⁸² A manera de recordatorio, PoW significa *Proof-of-Work*.

⁸³ Para más información acerca de este cambio consultar: <https://blog.ethereum.org/2015/08/01/introducing-casper-friendly-ghost/>

⁸⁴ (Poelstra, 2016)

⁸⁵ (Popper, 2018)

⁸⁶ El usuario al bloquear una cierta cantidad de fondos obtiene un beneficio después de cada determinado tiempo o renta.

moneda, siendo dicho depósito demostrable criptográficamente. Posteriormente, para extender la historia del consenso, en lugar de hacerlo mediante una “PoW”, cada depositario de una “apuesta” firma digitalmente la extensión del historial. Por razones de practicidad, típicamente se escogen de manera aleatoria una pequeña cantidad de partes interesadas para la firma de cada extensión y sólo se requiere la firma de una mayoría de los seleccionados para darle validez a la extensión firmada. Los escogidos se hacen acreedores de una recompensa y después de un tiempo podrán desbloquear los fondos bloqueados parte de su “apuesta”.

“La idea es que más allá de depender en la inviabilidad económica de tomar el control de un historial de transacciones, las partes interesadas están incentivadas para ponerse de acuerdo unos con otros en cada extensión porque: (a) son seleccionados de manera aleatoria y por lo tanto es poco probables que estén en colusión, y (b) aún si están en colusión, no querrían erosionar el sistema (por ejemplo, firmando historiales en conflicto) por que quieren recuperar su valor depositado cuando este se desbloquee, y (c) de todos modos tienen capacidad limitada para causar daño, ya que por las razones anteriormente mencionadas, el siguiente grupo de partes interesadas probablemente escogería de manera razonable el historial para ser extendido.”⁸⁷

A pesar de los anteriores beneficios, este sistema presenta ciertos inconvenientes para generar un consenso distribuido, además de presentar problemas en la generación de nuevos bloques⁸⁸.

Por otro lado, gracias a las mejoras previamente mencionadas contenidas en la plataforma, ésta ha florecido y con ello vino una innovación tecnológica que ha

⁸⁷ (Poelstra, 2016)

⁸⁸ Para profundizar sobre el tema se recomienda (Poelstra, 2016)

cambiado el panorama no sólo del mundo virtual, sino también al mundo financiero tradicional: la emisión de *tokens*.

III.1.3. Tokens

Una de las características más interesantes de la plataforma Ethereum, y la más relevante para el presente trabajo, es la posibilidad de crear Contratos que permiten la emisión de sub-monedas montadas en el *blockchain* de Ethereum. Dichos Contratos son programados a través de una cartera y son activados mediante un envío de ether a su respectiva dirección⁸⁹. Los activos emitidos utilizando este método son conocidos con distintos nombres tales como: *Meta Coins*, *App Coins*, fichas o de manera más popular, *tokens*.

El origen del término es explicado en una entrevista de Chris Dixon, un emprendedor del internet e inversionista, por la *New York Times Magazine* en la cual expone por medio de una metáfora el origen del uso de la palabra:

“No estamos intentando reemplazar al gobierno de los Estados Unidos. No intenta ser una moneda real, sino una pseudo moneda que sirva dentro de este mundo (virtual)”⁹⁰

Por lo tanto, es evidente que el término *token* fue formulado para hacer hincapié en que no se trata de un conjunto de activos “que intentan competir con las monedas emitidas por un país”. No se deseaba que se encasillaran a los tokens como un medio de pago, sino que se consideraran similares a fichas o tokens de un *arcade*, que sirven dentro del ecosistema de Ethereum, pero fuera de él son inútiles, tal como las fichas (o *tokens*) de un *arcade*.

No obstante lo anterior, los *tokens* son cripto-activos similares al ether, bitcoin o cualquier otro, emitidos por un Contrato en el caso particular de Ethereum. Estos pueden ser utilizados para representar una gran variedad de cosas: desde una moneda fiduciaria, alguna mercancía, acciones o bonos, o servir para activar una

⁸⁹ Para conocer el procedimiento detallado para la programación de un contrato emisor de *tokens* consultar <https://www.ethereum.org/token>

⁹⁰ (Johnson, 2018)

determinada función en la red. Pueden ser fungibles, como lo son la gran mayoría, o no. Su valor puede ser dado por el mercado de la libre oferta y demanda, o por su vinculación con algún activo material. En síntesis, son sumamente versátiles. Hoy por hoy, a pesar de que existen otros sistemas que lo permiten, Ethereum es la plataforma líder⁹¹ para emisión de *tokens*, posteriormente colocados mediante un *ICO*⁹². La mayoría de ellos son compatibles con ERC20, una estandarización que permite la interoperabilidad entre los *tokens* y el sistema Ethereum y es explicada a continuación, dada su relevancia para explicar la proliferación de este tipo de activos.

⁹¹ Existen otras plataformas como “NEO” que cada día cobran más relevancia en el panorama de los activos virtuales. Para más información acerca del proyecto visitar: <https://neo.org/>

⁹² (Darko, 2017)

III.1.3.1 ERC20

Como fue mencionado con anterioridad, Ethereum no es una plataforma estática, necesita ser mejorada constantemente y actualizarse, optimizando su estabilidad y seguridad. Una forma de hacer esto es mediante comentarios de agentes especializados, como desarrolladores. La manera en la cual se incorporan estas mejoras o actualizaciones es mediante un mecanismo de comentarios llamado *Ethereum Request for Comments* (“ERC”). El nombre del proceso proviene de uno similar llamado *Request for Comments* (“RFC”) que actualiza y mejora ciertos protocolos⁹³ sobre los cuales descansa el Internet, publicado por el “*Internet Engineering Task Force*” y la “*Internet Society*”⁹⁴. Con el RFC en mente, en el portal GitHub⁹⁵, desarrolladores propusieron una manera de actualizar el protocolo Ethereum⁹⁶, llamándolo “*Ethereum Request for Comments*” (“ERC”) en honor a los RFC⁹⁷.

En el caso en concreto de la vigésima edición, las reglas permiten a los *tokens* concurrentes con ellas operar de manera completamente compatible con la plataforma Ethereum. Para cumplir con el estándar deben de ser emitidos a través de un Contrato y cumplir con ciertas especificaciones técnicas. Si los *tokens* se apegan a los requisitos anteriores, pueden ser manejados con las mismas *wallets* a través de las cuales se interactúa con el ecosistema Ethereum. Por consiguiente, pueden ser enviados a las mismas direcciones y que sus transacciones sean verificadas utilizando los mismos mecanismos, con la diferencia de que un

⁹³ Se entiende el protocolo como “la versión en software de una lengua franca”, una manera en la cual múltiples computadoras se ponen de acuerdo para comunicarse entre ellas. Hay protocolos que gobiernan el flujo de la información sin procesar de internet y protocolos para mandar mensajes de correo electrónico y protocolos que definen las direcciones de páginas web” (Johnson, 2018)

⁹⁴ (IETF, 2018)

⁹⁵ Plataforma social para desarrolladores en la cual es posible compartir código y administrar proyectos, entre otros.

⁹⁶ (ethers, 2017)

⁹⁷ Para más información acerca de la corta historia del desarrollo del método ver: <https://ethereum.stackexchange.com/questions/33956/are-there-any-other-smart-contract-standards-like-erc20>

explorador de bloques⁹⁸ en lugar de mostrar una transferencia de ether expondrá una transferencia de un *token* en específico⁹⁹. Paralelamente, estas *App Coins* hacen la plataforma de Ethereum más robusta, ya que para emitir y adquirir fichas se requiere que los usuarios adquieran ether, lo que hace que aumente su demanda y su precio. Aunado a esto, existen mayores incentivos económicos para que los mineros dediquen su poder computacional al mantenimiento de la cadena de Ethereum por que el uso de *tokens* provoca que aumente el tráfico en la red y por lo tanto el pago de comisiones. Es por lo anterior que los *tokens* que cumplen con el comentario número 20 de las ERC son conocidos como tokens ERC20¹⁰⁰.

Gracias a los *tokens*, y a la estandarización, el mercado de los cripto-activos explotó. Anteriormente, si se quería emitir un valor virtual, se tenía que crear una *blockchain* que sostuviera ese valor en específico, y sólo ese valor, ya sea creando una cadena desde cero o bifurcando una existente. Para proyectos de gran calado esto es posible, sin embargo, para proyectos pequeños era sumamente complicado por la cantidad de recursos que debían de ser desplegados. Con la llegada de Ethereum cualquiera puede programar un Contrato para emitir *tokens* que pueden tener múltiples funciones. Asimismo, las sub-monedas pueden servir para lo que sea, hay cientos de ejemplos de proyectos que les dan un uso novedoso a sus *App Coins*. Por ejemplo, algunos sirven para pagar comisiones de plataformas de intercambio de *tokens*¹⁰¹, algunos otros como un medio de pago y otros más permiten acceder a un ecosistema que conecta el mundo del *blockchain*¹⁰². Así, los *Meta Coins* pueden ser programados para cumplir con cualquier objetivo, y ser usados prácticamente para lo que sea en el mundo virtual, ya sea representado el valor de cualquier activo (sea real o virtual) o teniendo o no una funcionalidad dentro del proyecto que los emite.

⁹⁸ Programa que permite explorar las transacciones guardadas en la cadena, ya sea de Ethereum o cualquier otro. Un ejemplo de estos es <https://etherscan.io/>

⁹⁹ (Darko, 2017)

¹⁰⁰ (Vogelsteller, 2015)

¹⁰¹ Binance Coin, con un precio de \$10.23 USD y una capitalización de mercado de \$73,287,800 USD, al 14 de feb. de 18

¹⁰² ICX, con un precio de \$4.35 USD y una capitalización de mercado de \$1,662,881,595 USD, al 14 de feb. de 18

III.1.4. *Initial Coin Offerings*

El objetivo final de crear un *token*, independientemente de su función en particular, es ser colocado entre el público. La forma más popular hacerlo y así obtener financiamiento para el proyecto, es mediante una oferta inicial pública de monedas, o como se conoce en inglés *Initial Coin Offering* (“*ICO*”).

El término *ICO* es un “eco deliberado” a las *Initial Public Offerings* (“*IPO*”)¹⁰³ que fueron tan características de la burbuja *dot com* de los años noventa¹⁰⁴. El concepto se refiere a “una manera no regulada, por lo menos en la jurisdicción mexicana, de obtener fondos mediante un esquema de financiamiento colectivo usando cripto-activos¹⁰⁵. Un *ICO* representa una alternativa al riguroso y profundamente regulado proceso de levantamiento de capital convencional requerido por capitalistas de riesgo, bancos o la bolsa. En un *ICO*, un porcentaje de la nueva moneda emitida es vendida a los inversionistas a cambio de moneda de curso legal u otros cripto-activos tales como bitcoin”¹⁰⁶.

Desgraciadamente, los *ICOs* llegaron al foco público a partir de un suceso lamentable, el incidente del “*Decentralized Autonomous Organization*” (“*DAO*”) en el año 2016. Este proyecto estaba diseñado para operar como un fondo de inversión sin intervención humana, gracias a un complejo entramado de Contratos. Para fondearse emitió *tokens* que además permitían a sus “clientes” poder votar acerca del destino de los fondos y que la organización de manera autónoma ejecutara dichas decisiones¹⁰⁷. Se lograron recaudar cerca de 150 millones de USD de capital, por parte de más de 11,000 inversionistas¹⁰⁸. Sin embargo, éste sufrió un ataque que tuvo como consecuencia un robo de ether equivalente a cerca de 60 millones

¹⁰³ En español se denomina, Oferta Pública de Venta (“*OPV*”).

¹⁰⁴ (Johnson, 2018)

¹⁰⁵ Estas pueden ser *tokens* ERC20, como lo son la mayoría actualmente, pero no necesariamente.

¹⁰⁶ (Schueffel, 2017, p. 15)

¹⁰⁷ (del Castillo, 2016)

¹⁰⁸ (Vigna, 2016)

de USD¹⁰⁹. El desfalco tuvo consecuencias que trascendieron el hecho, ya que, en un intento de regresar las monedas virtuales a sus legítimos propietarios, la comunidad llevó a cabo una bifurcación profunda o *hard fork*, que en términos prácticos tuvo como consecuencia borrar la transacción derivada del robo del registro. Para simplificar, es como si la sustracción nunca hubiera pasado, los fondos regresaron al DAO¹¹⁰.

Sin embargo, hubo una minoría que se opuso terminantemente a la bifurcación. El grupo opositor presentó un proyecto llamado Ethereum Classic, que replicaba la plataforma de Ethereum, con la diferencia que en su historial de transacciones el hurto nunca fue revertido. Nació de la bifurcación y emitió su propio activo virtual, el Classic Ether (“ETC”)¹¹¹. Los que estuvieron detrás del nuevo Ethereum fundamentaron su actuar en la naturaleza de la tecnología de cadena de bloques que aspira a ser completa y totalmente inmutable, e incluso apelaron al rompimiento del principio básico de la neutralidad por parte de la Fundación Ethereum, que tomó partido por los inversionistas. Acusaron, por medio de su portavoz Arvicco (un seudónimo para un desarrollador ruso), a la fundación de lo siguiente:

“La estructura y gobernanza de ethereum creó inestabilidad y las condiciones necesarias [que permitieron] la violación de sus características de Blockchain. Crear la Fundación Ethereum y todo el entramado corporativo alrededor de ethereum fue un grave error”

Además del anterior, defendieron su postura cripto-descentralista radical¹¹², con el argumento del gran riesgo que representaba el asentar un precedente tan peligroso. Al permitir que algo en este registro inmutable y resistente a la censura, que debería de ser *blockchain*, se modifique, nada impide que el día de mañana solicite lo mismo

¹⁰⁹ (Popper, 2017)

¹¹⁰ (Buterin, 2016)

¹¹¹ (Rizzo, 2016)

¹¹² Para más información acerca de esta corriente de pensamiento especialmente extremista, leer (Novosti, 2016)

un gobierno o cualquier otro poder fáctico¹¹³. Este evento suscitó un debate muy acalorado tanto entre los miembros de la plataforma como en la industria en general dadas las profundas implicaciones que esto podría tener para todo el ecosistema en general¹¹⁴.

Por otro lado, a pesar del muy desafortunado incidente, los *ICOs* como forma de obtener financiamiento explotaron. Los datos de 2014 muestran que en ese año únicamente se realizó un *ICO*, que recaudó \$461,802.00 USD¹¹⁵. En 2015 esa cifra creció a \$6,084,000.00 USD¹¹⁶ con la realización de 3 *ICOs* en el año. Posteriormente, en 2016, hubo un incremento impresionante a 30 *ICOs* con un levantamiento de capital por \$94,009,144 USD¹¹⁷. En 2017 esta cifra creció aún más, con 883 *ICOs* recaudando en total \$6,073,707,934 USD¹¹⁸. En lo que va de 2018, enero y febrero, se han realizado 275 *ICOs* con un levantamiento de capital de \$2,241,268,462 USD¹¹⁹. Este crecimiento explosivo es explicado fácilmente por los retornos de inversión estratosféricos que en tan poco tiempo obtienen los que compran estos productos. Las utilidades son brutales, por ejemplo, desde el momento de su lanzamiento el ether ha crecido de valor en alrededor de 26,000%¹²⁰ y en el caso de NEO, se trata de un 35,000%¹²¹.

De la misma manera es importante recalcar que las monedas o *tokens* objeto de un *ICO* tienen como característica en común el ser creados o sustentados con base en tecnología *blockchain*, a pesar de que los diversos activos virtuales pueden ser completamente diferentes uno de otro. De la misma forma, todos los *ICOs* se

¹¹³ (ghostyeti, 2016)

¹¹⁴ Está discusión aún sigue vigente en el espacio y las implicaciones que un *blockchain* pueda o no ser modificado por causas extraordinarias sigue siendo motivo de gran debate.

¹¹⁵ Datos obtenidos de <https://www.icodata.io/stats/2014>, consultado el 26 de febrero de 2018

¹¹⁶ Datos obtenidos de <https://www.icodata.io/stats/2015>, consultado el 26 de febrero de 2018

¹¹⁷ Datos obtenidos de <https://www.icodata.io/stats/2016>, consultado el 26 de febrero de 2018

¹¹⁸ Datos obtenidos de <https://www.icodata.io/stats/2017>, consultado el 26 de febrero de 2018

¹¹⁹ Datos obtenidos de <https://www.icodata.io/stats/2018>, consultado el 26 de febrero de 2018

¹²⁰ A menos que se especifique de otra manera, los valores son a febrero de 2018

¹²¹ Para ver el retorno de inversión de algún Token desde el *ICO*, visitar <https://icostats.com/roi-since-ico>, consultado el 27 de febrero de 2018

parecen en cuanto a que sirven como una forma de capitalización para un proyecto que puede o no, estar relacionado con la tecnología *blockchain*. A cambio de estos *tokens* se le puede prometer al inversionista una participación en las ganancias del proyecto¹²² o una parte de la propiedad de este, o incluso ninguna de las anteriores dando un beneficio diferente. Virtualmente cualquiera con conexión a Internet puede participar en una *ICO*¹²³, sin embargo, esto se ha vuelto más y más difícil conforme al paso del tiempo, debido a la naciente regulación.

Los *ICOs* pueden presentar una oportunidad interesante y digna de un estudio más profundo ya que podrían posibilitar un acceso más democrático a la bolsa, tanto desde el punto de vista de los emprendedores como de los inversionistas. A los primeros, permitiéndoles acceso a más y mejor financiamiento en comparación con lo que les ofrecería una institución de crédito, similar al que podrían obtener en la bolsa, sin requerir todo el andamiaje institucional necesario para poder cotizar en ella. A los segundos les permite apostar por proyectos en los que creen, de manera temprana y obteniendo beneficios económicos, sin tener que satisfacer múltiples requisitos, poseer grandes sumas de dinero ni ser un inversionista calificado.

Por otro lado, es importante recalcar que infortunadamente en el espacio de los *ICOs* hay cientos, sino no es que miles, de proyectos que presentan características de un esquema *Pump-and-Dump*¹²⁴. En este tipo de modelos se promociona el proyecto de una manera muy profusa, al tiempo que se abren preventas a un selecto grupo de personas, generalmente relacionado con los creadores, que permiten la compra de los *tokens* a un precio menor. Cuando la venta de *tokens* se abre al público en, por toda la expectativa generada el precio sube espectacularmente. En ese momento, quien adquirió los *tokens* a un precio de descuento vende su

¹²² Se le llama proyecto al emisor de los *tokens* ya que no necesariamente tiene que ser una persona moral debidamente constituida de acuerdo con leyes nacionales o extranjeras para emitirlos.

¹²³ (European Securities and Markets Authority, 2017)

¹²⁴ Esquema que consiste en un esfuerzo en manipular el precio de una acción o volumen de intercambio de esta mediante el uso de información supuestamente confidencial que resulta ser falsa o inexacta, es común verlo en proyectos con una capitalización de mercado muy pequeña. (SEC's Office of Investor Education and Advocacy, 2016)

participación obteniendo grandes ganancias, dejando a los inversionistas que llegaron después con *tokens* de un proyecto inservible¹²⁵. Esto ha llevado a la *Securities Exchange Commission* a advertir al público acerca de proyectos en los cuales se cuente con un portavoz de fama¹²⁶, ya que esta situación se presta a que el proyecto tome valor únicamente del reconocimiento del representante y no de su viabilidad.

Aún peores son aquellos proyectos que prometen un precio mínimo garantizado, ofreciendo un precio inferior en una preventa, “sugiriendo que el activo virtual en cuestión está relacionado de alguna manera con algún activo real con un precio fijo, o mencionando que se logró algún acuerdo con algún conglomerado empresarial de importancia”¹²⁷. Los proyectos de esta naturaleza, hasta ahora, han demostrado, en casi en todos los casos, tratarse de un fraude¹²⁸. Asimismo, el tiempo ha demostrado que la gran mayoría de proyectos fondeados a través de *ICOs* resultan poco viables y por fracasan a los pocos meses.

Sin embargo, no todo es negativo, los *ICOs* podrían ser una manera diferente de fundear proyectos, especialmente cuando los *tokens* emitidos sean de utilidad. La verdadera ventaja de una *App Coin* se revela cuando los *tokens* no sirven para extraer valor del proyecto, sino que se lo añaden. Lejos del esquema tradicional en el cual los inversionistas inyectan capital al proyecto con la expectativa de extraer valor de este, la utilización de fichas podría ser muy útiles para incentivar la adopción de nuevas tecnologías. Esto es especialmente útil en mercados sumamente competidos o incluso, saturados¹²⁹.

¹²⁵ Se calcula que alrededor de 80% de los lanzamientos de *alt-coins* encuadran dentro de un esquema *pump-and-dump* (Morris, 2013) en (Van Valkenburgh, 2016, p. 22)

¹²⁶ (SEC Division of Enforcement and SEC Office of Compliance Inspections and Examinations, 2017)

¹²⁷ (Van Valkenburgh, 2016, p. 23)

¹²⁸ (Van Valkenburgh, 2016, p. 23)

¹²⁹ (Dixon, 2017)

En el cripto-espacio hay miles de proyectos que llegan a los inversores a través de los *ICOs*. Algunos pueden resultar positivos, aunque desafortunadamente son la minoría, así que depende de los inversionistas y de las autoridades reguladoras fomentar que el espacio madure y pueda salir algo positiva de la experiencia. Este es un esquema que promete tener un potencial enorme, pero si se permite que proliferen los proyectos dañinos se le puede condenar al fracaso.

IV. Taxonomía de los Activos Virtuales

Hasta este punto del trabajo, han sido utilizados los términos moneda digital, activo virtual o cripto-moneda sin que se haya presentado una explicación acertada de lo que significan en el contexto de este trabajo y de la materia. Al ser una rama del conocimiento naciente, sobre todo en lo que concierne al ámbito legal, la doctrina no se ha desarrollado a profundidad. Los especialistas se han ocupado más de los aspectos prácticos de la tecnología, o técnicos desde un punto de vista computacional, que en la formación de conceptos. Esto es entendible, ya que en este punto del desarrollo de la tecnología parecería ocioso hacerlo. No obstante, al estar cada vez más regulado el sector, es importante establecer definiciones claras para delimitar conceptos que a su vez permitan una discusión adecuada sobre el tema.

Un punto de partida razonable es el reporte escrito por el Grupo de Acción Financiera Internacional¹³⁰, (“GAFI”) o “FATF” por sus siglas en inglés, titulado “Dinero Virtual, Definiciones Clave y Riesgos Potenciales en Materia de Lavado de Dinero y Financiamiento al Terrorismo”. En este documento se define a las monedas virtuales como:

“Una representación digital de valor que puede ser intercambiada de manera digital y que funciona como (1) un medio de intercambio; y/o (2) una unidad de cuenta; y/o (3) un depósito de valor, pero que no tiene curso legal en ninguna jurisdicción. No es emitida por ninguna jurisdicción y cumple con las funciones mencionadas con anterioridad únicamente por acuerdo de la comunidad de usuarios de la moneda virtual en cuestión¹³¹.”

¹³⁰ Grupo independiente e intergubernamental que desarrolla y promueve políticas que protegen el sistema financiero global contra lavado de dinero, financiamiento del terrorismo y proliferación de armas de destrucción masiva (Financial Action Task Force, 2014)

¹³¹ (Financial Action Task Force, 2014, p. 4)

De manera adicional GAFI hace una aclaración de suma importancia: el dinero virtual es distinto al *e-money* o dinero electrónico, el cual es una representación electrónica de moneda fiduciaria, usado para transferir valor de forma electrónica denominado en moneda fiduciaria. Es decir, el *e-money* o dinero electrónico, de acuerdo con el multicitado escrito, es una manera de transmitir de manera digital dinero de curso legal¹³². Por último, afirma que la moneda digital puede significar una representación ya sea de una moneda virtual (no fiduciaria) o dinero respaldado por un banco central¹³³. Con esto, establece diferencias entre lo virtual, electrónico y lo digital.

En seguida, el reporte profundiza en las diferentes clasificaciones del dinero virtual. Establece que éste puede ser dividido en dos categorías. La primera comprende al dinero virtual de tipo convertible o abierto, y es aquella que “tiene un equivalente en dinero real y puede ser intercambiado hacia y desde él”¹³⁴, es decir que se puede convertir fácilmente en dinero fiduciario. Por otro lado, presenta el dinero virtual no convertible o cerrado, creado para un dominio virtual específico, como un juego o una tienda virtual y cuyas reglas no permiten que pueda ser convertible a moneda fiduciaria¹³⁵. Empero, el reporte especifica que, si bien de manera oficial dicho dinero no puede ser convertido en dinero real, esto no impide que existan canales no oficiales por medio de los cuales esta moneda pueda ser convertida en dinero real. El desarrollo de un mercado negro secundario puede efectivamente convertir una moneda virtual cerrada en una abierta, por lo que su característica de no convertibilidad no es estática¹³⁶.

En contraste, el Compendio Conciso de Fintech de P. Schueffel¹³⁷, define al dinero digital como: “un tipo de dinero que no existe en el plano físico (por lo tanto, no

¹³²(Financial Action Task Force, 2014, p. 4)

¹³³ *Ídem*

¹³⁴ *Ídem*

¹³⁵ *Ídem*

¹³⁶ *Ibidem*, p. 5

¹³⁷ (Schueffel, 2017)

existen monedas o billetes) y que sólo puede ser transmitido por medios electrónicos, típicamente permitiendo transacciones instantáneas y transferencias de propiedad sin fronteras”¹³⁸, por lo que, en otras palabras, iguala lo digital con lo virtual.

A continuación, se presenta un análisis del contraste de definiciones de las anteriores fuentes, exponiendo las razones por las cuales se considera que la aproximación hecha por el FATF es más adecuada. En primer lugar, el grupo intergubernamental considera al dinero electrónico como una mera representación de valores ya sean fiduciarios o de cualquier otro tipo, difiriendo así con la definición de P. Schueffel, que conceptualiza al dinero digital como aquel valor que no tiene una contrapartida física. La primera definición parece ser la correcta dado el propio significado de la palabra digital. Como contexto, la Real Academia Española¹³⁹ define “digital”, en el ámbito concerniente, como aquello que “se realiza o trasmite por medios digitales” y/o “aquel sistema que presenta información mediante el uso de señales en forma de números o letras”. De esta definición se desprende un sustento al concepto presentado por la FATF, al considerar que el dinero digital no es un valor en sí mismo, sino que es meramente la representación computacional de otro.

Es por eso que, se sostiene la validez del término virtual para definir los activos a los que se refiere el presente trabajo en conformidad con el concepto dado por la FATF. Además de sustentar dicha aseveración en la definición dada por el documento, es preciso remitirse al significado de la palabra virtual. De acuerdo con el diccionario de la Real Academia Española¹⁴⁰ se trata de aquello que: “tiene virtud para producir un efecto, aunque no lo produce de presente, frecuentemente en oposición a efectivo o real”; de la misma manera refiere a aquello que “tiene existencia aparente y no real”. En el contexto de este trabajo es muy claro que se trata de la forma adecuada de referirse a un valor que no tiene un sustento “real” y

¹³⁸ (Schueffel, 2017, p. 9)

¹³⁹ (Real Academia Española, 2014)

¹⁴⁰ *Ídem*

cuya existencia se circunscribe únicamente al ámbito virtual, sin una representación física.

Una vez establecido el término virtual como el indicado para referirnos al objeto del trabajo, es transcendental especificar que las cripto-monedas, que se entienden como “una moneda virtual descentralizada y basada en matemáticas que es protegida mediante métodos criptográficos”¹⁴¹, son un subconjunto de la categoría llamada activos virtuales. Y es que a pesar de que no todos los activos virtuales son activos criptográficos, la enorme mayoría de ellos sí lo son, dejando a los demás en un papel secundario de tal magnitud que son prácticamente despreciables en términos del mercado y la regulación materia del trabajo. Añadido al tema económico, los activos virtuales criptográficos también tienen su fundamento en una tecnología, la cadena de bloques, que tiene la capacidad de ser revolucionaria a un nivel aún inimaginable.

Aclarado este punto, resta especificar por qué se hace referencia a ellos como activo o valor y no como moneda. Esto puede parecer confuso o contra intuitivo ya que, incluso en su nombre, bitcoin lleva la intencionalidad de ser considerado como dinero. Sin embargo, hay características de los multicitados activos que parecen indicar que se tratan de una nueva clase de activos dentro de la clasificación de súper clases de activos¹⁴² de Robert Greer, que van más allá del concepto del dinero. Asimismo, se considera que a pesar de que los cripto-activos comparten características con otros activos, estos no pueden ser clasificados de una manera tradicional y requieren de una nueva clasificación. Lo anterior es sustentado por Adam White y Chris Burniske, inversionistas y financieros con interés en el cripto-espacio, quienes, en su reporte de investigación “*Bitcoin Ringing the Bell for a New*

¹⁴¹ (Financial Action Task Force, 2014, p. 5)

¹⁴² Se entiende una clase de activos como un conjunto de activos que tienen entre ellos alguna similitud económica fundamental y que a su vez tienen características que los hacen distintos a otros activos que no son parte de su clase. Las tres súper clases de activos son: Activos de Capital, Activos Consumibles o Transformables (“C/T”), Activos de Guarda de Valor (“SOV”), de estas se derivan múltiples clases y grupos. Como bonos, acciones, deuda, etc. (Greer, 1997, p. 1)

*Asset Class*¹⁴³, presentan esta idea. En dicho reporte, ellos toman factores como la liquidez, el perfil político-económico, la independencia de su precio respecto a factores exógenos, su volatilidad y su retorno de inversión para clasificar al bitcoin, desde un punto de vista financiero, dentro de un nuevo grupo de activos distinto y único hasta el momento.

Adicionalmente, la propuesta de clasificar al bitcoin como activo¹⁴⁴ también es apoyada por Ed Howden¹⁴⁵, quien considera que la clasificación más lógica para un objeto tan *sui generis* como lo es el bitcoin es la de un activo. Aunque también acepta que al final del día podría parecer una clasificación que no ayuda a avanzar en cómo se debería de regular. Dado a que, al mismo tiempo este activo podría ser utilizado como dinero, inversión o una mercancía, dejando el tema en el punto en el que inició al no tomar una postura definitoria. Además, considera que la clasificación de “Activo Digital¹⁴⁶” es demasiado amplia, pero lo justifica con el hecho de que, en efecto, bitcoin y otros “cryptos”¹⁴⁷ cruzan un amplio espectro de posibles etiquetas¹⁴⁸ y advierte de los peligros que traería el poner una etiqueta demasiado amplia o estrecha al fenómeno de los activos virtuales.

Paralelamente, el autor insiste en que es importante el término que se les asigne, ya que muy posiblemente, esta denominación impactará de manera directa el tipo de regulación impuesta en la industria; situación que se ve reflejada en México al poner dentro de las atribuciones de Banco de México la regulación de activos virtuales. En contraste, el autor concluye con la propuesta de no insistir con el

¹⁴³ (Burniske & White, 2017)

¹⁴⁴ Se entiende activo cómo: un recurso con valor económico que un individuo, corporación o país tiene o controla con la expectativa de que le provea de un beneficio futuro. (Investopedia, 2016)

¹⁴⁵ (Howden, 2015, p. 766)

¹⁴⁶ El uso de la palabra digital se antoja desafortunado por los motivos expuestos con anterioridad, sin embargo, este el término que utiliza el autor en su trabajo.

¹⁴⁷ En el momento de la escritura de este artículo, 2015, el cripto-espacio se encontraba en un estado menos desarrollado que lo que se encuentra actualmente, por lo que muchos de los “cryptos” (término utilizado por el autor) a los que se refiere el autor han desaparecido o han sido modificados radicalmente.

¹⁴⁸ (Howden, 2015, p. 769)

intento de asignarle un término específico al conjunto de “cryptos” y aboga por una clasificación en la cual simplemente se les catalogue como “buenos”, permitiendo así su desarrollo¹⁴⁹ al no forzar sobre ellos una clasificación que puede no ser óptima de acuerdo con su naturaleza.

Por otro lado, la taxonomía de los activos fue retomada en una obra posterior¹⁵⁰ de C. Burniske y J. Tatar en la cual se reitera que es poco afortunado denominar monedas a una serie de activos de muy diversas características, que no necesariamente corresponden con las que tiene o debería de tener el dinero¹⁵¹. Es por eso que los autores que proponen tres grupos dentro de la categoría de cripto-activos: las cripto-mercancías o cripto-materias primas (*cryptocommodities*), los *criptotokens* (*cryptotokens*) y las cripto-monedas (*cryptocurrencies*) en *sensu stricto*.

Las cripto-mercancías son aquellos activos virtuales que permiten la utilización de recursos para la transformación o producción de un bien o producto final¹⁵², un ejemplo de esta categoría es el ether o ETH¹⁵³ que permite la ejecución de tareas computacionales de la plataforma Ethereum, ya sea para programas *dApps* o emitir *tokens*. El segundo grupo es aquel de los cripto-tokens, estos permiten el uso de bienes o servicios finales y requieren de la infraestructura proveída tanto por los *cryptocommodities* como por las cripto-monedas para su debido funcionamiento¹⁵⁴. Un ejemplo de cripto-tokens es Binance Coin o BNB que facilita el pago de comisiones en un intercambio de activos. No obstante, es relevante mencionar que también existe el argumento que ciertos *tokens* pueden ser clasificados como monedas, ya que dentro del ecosistema de la aplicación que los emitió sirven como medio de pago. Por último, pero no menos importante, tenemos a las cripto-monedas en sentido estricto. Estos activos tienen la función de desempeñarse como

¹⁴⁹ (Howden, 2015, p. 769)

¹⁵⁰ (Burniske & Tatar, 2018)

¹⁵¹ “El dinero debería cumplir con funciones bien definidas, servir como medio de pago, unidad de cuenta y depósito de valor”. (Burniske & Tatar, 2018, p. 84)

¹⁵² *Ibidem*, p. 79

¹⁵³ *Ibidem*, p. 113

¹⁵⁴ *Ibidem*, p. 80

dinero. Ejemplo muy claro de éstas es el tether (“USDT”) un activo atado al valor del dólar evitando la volatilidad generalmente asociada con activos virtuales, creado y utilizado para pagar.

Cabe mencionar que esta clasificación no es rígida dado el estado de desarrollo tan primigenio de la tecnología y nada impide que, por ejemplo, un activo que con anterioridad se consideraba una moneda pase a ser materia prima o viceversa. Además, no se puede descartar que una vez que se asiente el polvo del impacto inicial del protocolo, nuevos conceptos más concretos y delimitados surjan en torno a los cripto-activos. De hecho, desde que la obra fue publicada a inicios del 2018, pocos meses después, C. Burniske declaró en una entrevista¹⁵⁵ que es posible que una nueva categoría ya haya surgido, la de los cripto-coleccionables. Un ejemplo de este último grupo son los *CryptoKitties*¹⁵⁶. Son aplicaciones descentralizadas que emiten activos que cumplen el estándar técnico ERC-721 a través del cual se emiten *tokens* no fungibles¹⁵⁷ y no divisibles¹⁵⁸. Finalmente, es de suma importancia mencionar que las fronteras entre todas las categorías no son muy claras y que estas sirven únicamente como las bases para un posterior desarrollo más profundo de la taxonomía de los cripto-activos.

Recapitulando, es importante seguir construyendo en el tema de definición de conceptos para evitar que se genere un punto de vista regulatorio demasiado estrecho que asfixie el desarrollo de la tecnología *blockchain* o demasiado amplio que simplemente sea inútil para establecer la naturaleza del objeto a regular. Igualmente, la definición de conceptos toma una importancia particular por el rápido avance de la tecnología, ya que de tomar una decisión apresurada que imponga un

¹⁵⁵ (Burniske & Tatar, 2018), episodio 218 del programa *Epicenter* titulado *Cryptoassets – The Rise of a New Asset Class*, con los invitados Chris Burniske & Jack Tatar, publicado el 17 de enero de 2018, ver en línea: <https://epicenter.tv/episode/218/>

¹⁵⁶ Para saber más del proyecto, consultar: <https://www.cryptokitties.co/>

¹⁵⁷ Bien fungible: Bien que está determinado solo por su género y puede por tanto ser sustituido por otro, siempre que el género sea el mismo. En contraposición, el bien no fungible no es sustituible, se haya determinado por su especie o individualidad y no puede por tanto ser sustituido por otro ni aun dentro del mismo género. (Real Academia Española; Consejo General del Poder Judicial, 2016)

¹⁵⁸ Para más información respecto el tema, consultar el artículo en línea: <https://www.coindesk.com/crypto-collectables-ethereums-next-killer-app-is-on-its-way/>

marco regulatorio no óptimo se corre el riesgo que, al surgir nuevos activos virtuales, estos caigan fuera de las disposiciones existentes con el efecto de dejarlas sin efecto en su caso particular, algo que puede ser peligroso para el orden legal y tener consecuencias no previstas.

V. Panorama Internacional de los Activos Virtuales

Los mercados de activos virtuales, aunque son de reciente creación, han aumentado su tamaño a una velocidad apabullante, a un nivel no visto antes en la historia moderna. Esto ha llamado la atención de múltiples gobiernos que han volteado a ver con renovado interés lo que antes era una economía subterránea y no regulada, solicitando a sus reguladores que actúen para aplicar la ley o emitiendo nuevas normas. Dado el objetivo del presente trabajo, es pertinente analizar lo hecho en otros países para, en la medida de lo posible, adoptar las mejores practicas y aprender de los errores y aciertos cometidos en otras jurisdicciones. En particular, se examinará lo sucedido en los Estados Unidos de América y Suiza.

Es importante mencionar que la selección de estos países fue hecha con base en la importancia que presentan en la economía de activos virtuales. Tal como es señalado en la Figura 1, en términos porcentuales, el origen de los proyectos que más capital han levantado a través de un ICO son los de EE. UU. y Suiza. De igual manera, también son países que han hecho un esfuerzo considerable para encontrar el marco regulatorio que se ajuste a estos nuevos activos y esta economía.

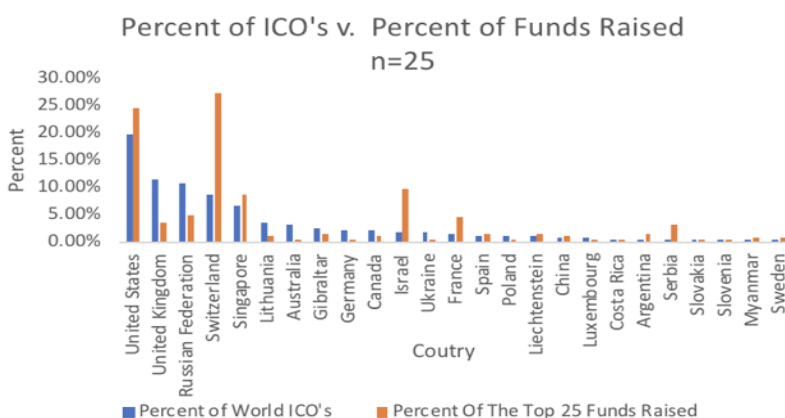


Figura 1. Porcentaje de ICOs por país respecto al total (en color azul) y porcentaje de capital levantado por los 25 principales ICOs del país (naranja) en el periodo de 2017¹⁵⁹.

¹⁵⁹ (Kaal, 2018)

V.1. Estados Unidos de América

Hoy por hoy, en el vecino país del norte existe una gran incertidumbre regulatoria referente a los activos virtuales. El desarrollo del sector ha sido mucho más rápido que el de su reglamentación correspondiente y esto ha resultado en la falta de un regulador o marco jurídico adecuado¹⁶⁰. No obstante, esto no ha impedido que se hayan dado esfuerzos por regularlos de diferentes maneras.

Se comenzará por analizar la pregunta clave que han intentado contestar las agencias reguladoras en los EE. UU. ¿Cómo se utilizan los activos virtuales y que es lo que se busca lograr a través de ellos¹⁶¹. Es decir, hasta ahora no ha existido un especial interés en contestar qué es un activo virtual a un nivel conceptual; sino que el interés reside en la necesidad de regular a aquellos actores que comercian con estos activos y por lo tanto son el punto de encuentro entre el sistema financiero tradicional y el cripto-espacio, como lo son los intercambios o *exchanges*. Esta actitud va de acuerdo a la tendencia pragmática hacia la que se inclina todo el fenómeno. Empero, esta actitud trae consigo la desventaja de la producción de múltiples definiciones del objeto a regular que en ocasiones pueden resultar contradictorias¹⁶². La anterior situación se da en parte porque los reguladores buscan que los activos virtuales, que originalmente no están dentro de sus facultades regulatorias, entren dentro de su ámbito de competencia, determinando su naturaleza de tal modo que así sea. Por lo tanto, un activo virtual, de manera inicial, ha sido definido por diferentes agencias regulatorias de maneras muy diferentes.

El primer ejemplo de un acercamiento realizado por una agencia regulatoria es el perpetrado por la *U.S. Securities and Exchange Commission* (“SEC”), que equipara, en el ámbito de su competencia, a los *tokens* colocados a través de un *ICO* con

¹⁶⁰ (Van Valkenburgh, 2016, p. 1)

¹⁶¹ *Ibidem*, p. 2

¹⁶² *Ídem*

valores colocados a través de una emisión; lo cual, tendría un gran impacto no sólo en los *ICOs* sino en las plataformas en las cuales se comercian con los activos distribuidos mediante un *ICO*.

Por otro lado, la *Commodity Futures Trading Commission* (“CTFC”) tomó un enfoque diferente. A partir de la resolución del caso *Coinflip, Inc., d/b/a Derivabit*, y Francisco Riordan compareciendo ante la CFTC¹⁶³, haciendo referencia a la definición de lo que considera una mercancía, la agencia tomó la siguiente decisión:

“Bitcoin y otras monedas virtuales están comprendidas en la definición (de mercancía) y son propiamente definidas como tales.”

No obstante, se debe de remarcar que, de la resolución se desprende que el encuadramiento a la definición de mercancía apela más a la naturaleza de los contratos de futuros que de bitcoin. Es decir, en dicho fallo se establece que al ser objeto de un contrato de futuros el subyacente debe de ser una mercancía, y clasifica a bitcoin como mercancía ya que es un subyacente, sin mayor consideración al respecto. Por lo anterior, es necesario tomar con reserva la definición planteada por la CFTC, sin ignorar la importancia que haya clasificado el bitcoin como materia prima o mercancía¹⁶⁴.

Paralelamente, añadiendo a la confusión, el Departamento del Tesoro, a través de la *Financial Crimes Enforcement Network* (“FinCEN”), considera a los activos virtuales, en específico bitcoin, como “dinero utilizado para transmisión de moneda”¹⁶⁵.

Por último, los activos virtuales, particularmente bitcoin, fueron clasificados como propiedad o activos físicos por el *Internal Revenue Service* (“IRS”) para fines fiscales

¹⁶³ (CFTC Orders Bitcoin Options Trading Platform Operator and its CEO to Cease Illegally Offering Bitcoin Options and to Cease Operating a Facility for Trading or Processing of Swaps without Registering, 2015) ver en línea en: <https://www.cftc.gov/PressRoom/PressReleases/pr7231-15>

¹⁶⁴ CFTC Orders Bitcoin Options Trading Platform Operator and its CEO to Cease Illegally Offering Bitcoin Options and to Cease Operating a Facility for Trading or Processing of Swaps without Registering, ver en línea: "http://www.cftc.gov/idc/groups/public/@lrenforcementactions/documents/legalpleading/enfcoinfliporder09172015.pdf, visitado el 27 de febrero de 2018.

¹⁶⁵ (FinCEN, 2013) en (Van Valkenburgh, 2016, p. 3)

en el aviso 2014-21¹⁶⁶. La institución reconoció que el activo puede ser usado como un método de inversión o pago de productos o servicios¹⁶⁷, no obstante, también estableció que nunca se deberá entender como moneda. Conjuntamente, se señala que es computable como un ingreso cuando es recibido como pago, registrándose al precio que tenía en la fecha de aceptación, de una manera razonable que se aplique de manera consistente. De igual manera, se computa como un ingreso cuando a cambio de una unidad, a través de un intercambio, se obtiene una cosa que supere el valor de la primera y se registra como una pérdida si sucede lo opuesto¹⁶⁸. Estas, entre otras cuestiones, resuelve el IRS para el tratamiento fiscal de activos virtuales.

Gracias lo expuesto con anterioridad, resulta evidente que no existe un criterio unificado de cómo se deben de regular los activos virtuales o de qué autoridad debe hacerlo. Aun más, en la comparecencia ante el comité de Banca, Vivienda y Asuntos Urbanos del Senado, los titulares de la *U.S. Securities and Exchange Commission* (“SEC”), Jay Clayton, y de la *Commodity Futures Trading Commission* (“CFTC”), J. Christopher Giancarlo, dos de los organismos más relevantes en la materia, nuevamente se hizo evidente la incertidumbre que existe en materia jurisdiccional respecto a las agencias previamente mencionadas, junto con el Departamento del Tesoro¹⁶⁹. A continuación, se analizará de manera detallada los esfuerzos de aplicación de la ley y las consideraciones hechas al respecto por parte de los organismos federales más relevantes en la materia: la SEC, la CFTC y FinCEN. Cabe mencionar que se dejará a un lado la legislación estatal, ya que está fuera del enfoque del presente trabajo.

¹⁶⁶ (Internal Revenue Service, 2014)

¹⁶⁷ Actualmente existe una discusión en cuanto a cómo gravar los llamados *airdrops* y monedas resultantes de una bifurcación (Roberts, 2017)

¹⁶⁸ (Internal Revenue Service, 2014)

¹⁶⁹ (Comité de Banca, Vivienda y Asuntos Urbanos, 2018)

V.1.1. U.S. Securities and Exchange Commission

Para comenzar, es pertinente aclarar que la regulación de los EE. UU. no está encaminada a limitar activos virtuales *per se*. En cambio, fue considerado que el ámbito lógico para aplicar la fuerza del Estado eran los puntos de contacto entre el cripto-espacio y el mundo financiero tradicional, siendo estos las casas de intercambio de moneda fiduciaria por activos virtuales.

En consecuencia, hay ciertas áreas regulatorias que son cada vez son más claras y definidas. Un ejemplo son las reglas que se aplican a las casas de intercambio de activos virtuales. La mayoría de éstas han decidido atenerse al régimen de un servicio de transmisión de dinero, haciendo de esta figura, reglamentada a nivel estatal, una solución provisional al acertijo regulatorio que son las casas de cambio de cripto-activos. Sin embargo, constituirse como un transmisor de dinero presenta diversos inconvenientes, entre los que se encuentran el problema de la custodia de los fondos y tener que solicitar un permiso en cada estado en el que los *exchanges* desean operar¹⁷⁰. Además, la figura de un transmisor de dinero no fue diseñada para amparar el intercambio de activos con características similares a las de un valor, como lo considera J. Clayton, titular de la SEC¹⁷¹. Es decir, la operación de un intercambio, bajo la denominación de un trasmisor de dinero, presenta problemas regulatorios y operativos aún no resueltos.

Para añadir a la confusión en la materia, la SEC emitió un comunicado posterior¹⁷² en el que declara a las plataformas virtuales de intercambio de activos criptográficos como no reguladas y recomienda al público no pensar en ellas en los mismos términos que una plataforma de intercambio de valores convencionales que cumple con el marco legal vigente. Uno de los temores del organismo es que al existir ciertas similitudes entre las plataformas reguladas y las no reguladas, los inversionistas

¹⁷⁰ (Van Valkenburgh, 2018), episodio 227 del programa Epicenter titulado Towards Sound Bitcoin Policy, con el invitado Peter Van Valkenburgh, publicado el 9 de mayo de 2017, ver en línea en: <https://epicenter.tv/episode/227/>

¹⁷¹ (Clayton, 2018, p. 5)

¹⁷² Statement on Potentially Unlawful Online Platforms for Trading Digital Assets ver en línea en "https://www.sec.gov/news/public-statement/enforcement-tm-statement-potentially-unlawful-online-platforms-trading"

tengan la impresión de que, al igual que en una plataforma reglamentada, tendrán cierta protección por parte del gobierno federal. En el reporte, la agencia hace hincapié en diversos inconvenientes que pueden traer dichos sitios, cómo la nula supervisión de los activos que se comercian a través de ellos, aparte del desconocimiento de cómo operan los protocolos para la ejecución de órdenes. Esto trae el problema que dichos sistemas no están revisados por la autoridad competente, por lo que es incierta la manera en la cual interactúan y se liquidan las órdenes de compra y venta. Por último, el documento concluye solicitando a dichas plataformas que se sometan a la regulación pertinente ya sea bajo la figura de un intercambio de valores nacional, un sistema alternativo de intercambio (“ATS”), un intermediario bursátil (“*broker-dealer*”) o presenten alguna excepción que los releve de sujetarse a alguna de esas figuras, informando que, en caso de no hacerlo, se atienen a la acción regulatoria de la agencia. Es decir, el intercambio de *tokens*, emitidos a través de un *ICO*, se debería de hacer en intercambios similares en naturaleza a la *New York Stock Exchange*¹⁷³.

En este punto, es conveniente recalcar que la SEC iguala un *ICO* a una oferta privada inicial y los *tokens* emitidos a través de ella son, de acuerdo con su marco normativo, títulos de valor (“*securities*”). Parte del razonamiento que sostiene este argumento es el resultado de una prueba de carácter jurídico llamada *Howey Test* (o la prueba de Howey), basada en un caso analizado por la Suprema Corte de los Estados Unidos en 1946¹⁷⁴ que destiló en el siguiente precepto a través del cual se decide si un instrumento clasifica o no como un contrato de inversión, defendiéndolo de la siguiente manera:

“Un contrato, transacción o esquema por medio del cual una persona invierte su dinero en una iniciativa común y es dirigida a esperar utilidades derivadas únicamente de los esfuerzos del promotor o una tercera persona”

¹⁷³ (del Castillo, 2017)

¹⁷⁴ (Securities and Exchange Commission v. W. J. Howey Co., 1946)

A consideración de la SEC, la enorme mayoría de los *tokens* colocados a través de un *ICO* cumplen con dichas características¹⁷⁵. Lo anterior no significa que todos los activos criptográficos sean valores a ojos del regulador, dado que la decisión del regulador se hará ateniéndose a las características particulares que presente cada caso. Sin embargo, si resulta que un activo es efectivamente clasificado como valor será sujeto a múltiples normas.

A esta dificultad regulatoria, se añade que, posterior a un análisis casuístico, los productos financieros que están ligados a activos virtuales puedan ser clasificados como valores¹⁷⁶. Es por esta facultad que la SEC, a la fecha, aún no ha autorizado un *Exchange-traded fund* (“ETF”) o fondo de inversión cotizado en vista que los crypto-activos presentan ciertos problemas de liquidez, valuación y custodia de los fondos, además de otros inconvenientes¹⁷⁷ que no se han podido resolver de manera satisfactoria. Por otro lado, retomando el caso de los *ICOs*, es significativo mencionar que a pesar de que la clasificación de *tokens* como valores se establece caso por caso, existen precedentes que señalan que la tendencia regulatoria tiende a clasificarlos como tales. Un ejemplo de esto es el antecedente marcado por el caso DAO.

Como fue abordado con anterioridad, en el capítulo titulado *Initial Coin Offerings*, la DAO fue un proyecto que emitió *tokens* para capitalizarse. Respecto al caso, la SEC determinó que las sub-monedas emitidas por la DAO debían ser considerados como *securities* o valores; así llegando a la conclusión que los compradores de los respectivos *tokens* realizaron efectivamente una inversión con una expectativa razonable de obtener utilidades, derivados de los esfuerzos administrativos de otros. El anterior comportamiento encuadra en la prueba de Howey y por lo tanto los *tokens* fueron considerados como valores. Al respecto, en la resolución del caso

¹⁷⁵ El titular de la SEC J. Clayton ha declarado, que todos los *ICOs* que ha visto constituyen una oferta de valores. (Comité de Banca, Vivienda y Asuntos Urbanos, 2018)

¹⁷⁶ (Clayton, 2018, p. 6)

¹⁷⁷ *Idem*

se establece de una manera un poco más clara el razonamiento que utilizará la agencia para establecer que un activo efectivamente es un valor:

“Lo que determinará que una transacción en particular involucra o no la oferta y venta de un valor, sin importar la terminología usada, dependerá de los hechos y circunstancias, incluyendo la realidad económica de la transacción. [...]”¹⁷⁸

El fallo hace hincapié en que al momento del análisis del *token* en particular, se debe de tener especial atención en la substancia de la transacción que le dio origen a éste y no en la forma, por lo que proveer de una utilidad al *token* no lo exime necesariamente de ser un valor regulado¹⁷⁹. De igual manera, considera que es una característica clave para clasificar a los *tokens* como valores es su mercado secundario tan prolífico, que permite especular con la compra y venta de estos activos¹⁸⁰. El documento también plantea la preocupación de la agencia de que al ser un mercado con tan poco volumen es relativamente fácil realizar una manipulación de precios¹⁸¹.

Por otro lado y a pesar de lo anterior, el regulador sí distingue entre *ICOs* llevados a cabo antes y después de la terminación del producto. En consecuencia, establece que aumentan las posibilidades que un activo sea clasificado como valor si es emitido antes de que exista un producto funcional. Por consiguiente, si la colocación es realizada después, disminuye la posibilidad de que los *tokens* distribuidos sean considerados como tales. De ahí, nace el *Simple Agreements for Future Tokens* (“SAFT”) o los Acuerdos Simples para *Tokens* Futuros, a través del cual una compañía que está en una fase pre-producto realiza una oferta amparada bajo la *Regulation D* a inversionistas calificados y posteriormente un *ICO* no registrado al público en general¹⁸².

¹⁷⁸ (Securities and Exchanges Commission, 2017) consultar en línea en: "<https://www.sec.gov/litigation/investreport/34-81207.pdf>"

¹⁷⁹ (Clayton, 2018, p. 7)

¹⁸⁰ *Ibidem*, p. 8

¹⁸¹ *Ídem*

¹⁸² (Bully, 2018)

Por otro lado, el director de la SEC J. Clayton considera que en el caso que se emita un *token* calificado como valor y se accione el supuesto regulatorio correspondiente, parte de las reglas que deben de cumplir los proyectos que llevan a cabo un *ICO* es registrarse como una emisora de valores, a excepción de que caigan en algún supuesto legal que los excuse de dicho requisito, considerando que todos los *ICO* que ha visto deben de llevar a cabo el registro¹⁸³. De igual manera, las plataformas que intercambien estos valores virtuales también deben registrarse como plataformas nacionales de intercambio de valores a no ser que la ley los exima de este requisito¹⁸⁴.

A consecuencia de estas consideraciones, la SEC ha actuado en múltiples ocasiones contra operaciones fraudulentas o no reguladas de emisión de valores. En primer lugar, se han emprendido acciones legales contra *ICOs* de proyectos que presentan a su *token* como supuestamente respaldado con activos reales¹⁸⁵, compañías que prometen un servicio de comida basado en *blockchain*¹⁸⁶ o incluso contra una organización que hizo la promesa de echar andar un banco descentralizado¹⁸⁷. Posteriormente, la agencia “ha emitido docenas de citatorios a personas y compañías detrás de *ICOs*”, con estimados de hasta 80 envíos de citaciones, uno de los esfuerzos regulatorios más grandes emprendidos por la agencia¹⁸⁸. Esto muestra una clara intención de tomar la iniciativa regulatoria en el área, con mucha más actividad del organismo en el tema, teniendo en mente combatir la posibilidad de modificar el precio con un par de ventas coordinadas y manipular el mercado.

Es importante mencionar que dichos citatorios se generan meses después de la recopilación de información de los proyectos financiados mediante *ICOs*. Destaca la recopilación de datos proveídos a los compradores de los *tokens* relativos a su

¹⁸³ (Comité de Banca, Vivienda y Asuntos Urbanos, 2018)

¹⁸⁴ (Clayton, 2018, p. 7)

¹⁸⁵ (Securities and Exchange Commission, 2017) en (Clayton, 2018, p. 9)

¹⁸⁶ *Ídem*

¹⁸⁷ *Ídem*

¹⁸⁸ (Popper, 2018)

inversión y los informes de quien adquirió estos activos¹⁸⁹, además de la estructura de las ventas y preventas¹⁹⁰. Es significativo que, al parecer, la agencia se enfocó particularmente en proyectos que hicieron uso de un SAFT¹⁹¹, instrumento explicado a continuación.

¹⁸⁹ *Ídem*

¹⁹⁰ (Eaglesham & Paul, 2018)

¹⁹¹ *Ídem*

V.1.1.1 Simple Agreement for Future Tokens (“SAFT”)

Los *Simple Agreement for Future Tokens* o SAFT son contratos de inversión que permiten:

“[...] a los grandes inversionistas e inversionistas con sumas relativamente grandes de capital, comprar los derechos sobre los *tokens* antes de su venta al público. Estos derechos pueden ser intercambiados por utilidades, incluso antes de que la venta comience”¹⁹²

En esencia, son contratos de inversión que contemplan la venta de uno de estos instrumentos por parte de los desarrolladores de un proyecto a un grupo de inversionistas calificados¹⁹³ y en virtud del cual los segundos se obligan a proveer de fondos a los desarrolladores. Quedando en cambio, comprometidos los desarrolladores a usar los fondos para crear una red genuinamente funcional, con *tokens* verdaderamente utilizables, comprometiéndose a entregar dichos activos a los inversionistas una vez que sean funcionales. Con posterioridad y una vez que se tenga un producto eficaz, los inversionistas, así como los desarrolladores, pueden revender las *App Coins* al público, a cambio de una utilidad¹⁹⁴. A través de este tipo de pactos se busca evitar caer en los supuestos regulatorios contenidos en la legislación de valores.

De acuerdo con la opinión de sus creadores, Juan Batiz-Benet, Marco Santori y Jesse Clayburgh, y en concordancia con la normatividad vigente, aunque el SAFT es un valor (*security*), por lo que debe de cumplir con los requisitos regulatorios señalados, los *tokens* emitidos una vez que el proyecto sea funcional, no deberían

¹⁹² (Eaglesham & Paul, 2018)

¹⁹³ (Batiz-Benet, et al., 2017)

¹⁹⁴ *Ibidem*, p. 1

de ser considerado como tales¹⁹⁵. Ya que se tratan de un producto de consumo, cayendo en la clasificación de *tokens* post producto¹⁹⁶, siendo estos aquellos que:

“Están diseñados para ofrecer una utilidad intrínseca que habilita el uso de una red descentralizada y distribuida que da [acceso] a los usuarios de la red a un bien o servicio [...]”¹⁹⁷

A través de este contrato se pensaba, analizando la decisión que tomó la SEC respecto a la DAO¹⁹⁸, que los *tokens* emitidos por medio de un *ICO* serían menos propensos a ser clasificados como valores. Derivado de lo anterior, se lanzaron los SAFT con un enfoque completamente orientado hacia los *tokens* post producto. No obstante, parece que los argumentos detrás del instrumento no fueron lo suficientemente fuertes como para convencer al regulador. La SEC no cambió su criterio de aplicar la *SEC Act* a los *tokens* post producto que utilicen un SAFT para colocarse entre el público, dejando serias dudas respecto al futuro regulatorio del ecosistema en los Estados Unidos de América. Añadido a esto, existen voces¹⁹⁹ que llaman el acercamiento del SAFT a los eventos generadores de monedas no sólo restrictivo, en cuanto al público al que se dirige, sino potencialmente peligroso. Al limitar la venta de *tokens* a capitalistas de riesgo e inversionistas calificados, el proyecto le está vendiendo los derechos sobre lo que se entiende, o lo que quieren que se entienda, bienes de consumo a sujetos que es muy posible no sean consumidores de estos, por lo que se está condenado a los *tokens* de la plataforma a un uso meramente especulativo.

¹⁹⁵ Esta estrategia parece no haber convencido a el regulador, la SEC de darles tal tratamiento, a la luz de sucesos recientes y la propia opinión del titular, Jay Clayton, que considera que todos los *ICOs* que ha visto se tratan de una oferta de valores. Para más información ver (Eaglesham & Paul, 2018) y (Comité de Banca, Vivienda y Asuntos Urbanos, 2018)

¹⁹⁶ (Batiz-Benet, et al., 2017, p. 1)

¹⁹⁷ *Ibidem*, p. 3

¹⁹⁸ (Securities and Exchanges Commission, 2017) consultar en línea en: <https://www.sec.gov/litigation/investreport/34-81207.pdf>.

¹⁹⁹ (Dolan, 2017)

V.1.2. Commodity Futures Trading Commission

La CFTC es la agencia regulatoria estadounidense con autoridad sobre los mercados de materias primas y contratos a futuro tanto de mercancías como de productos financieros. Además, después de la crisis financiera del 2008, es la encargada de supervisar la mayoría de los mercados en los cuales se negocian contratos *swaps*. Para poder cumplir con sus obligaciones tiene una serie de facultades que se derivan de la *Commodity Exchange Act* (“CEA”) de 1974²⁰⁰.

Esta institución ha tenido un papel activo en el nacimiento de la incipiente regulación de bitcoin y de las plataformas a través de las cuales se intercambia en su modalidad de activo subyacente, tratándose de futuros. La posibilidad de hacer esto se derivada de que, desde su creación y para poder cumplir con su mandato de supervisión de mercancías (*commodities*), se definió en el CEA sección 1ª (9) de una manera amplia lo que entiende como una para fines legales:

(9) Commodity

El término *commodity* (mercancía) significa trigo, algodón, arroz, maíz, avena, cebada, centeno, semilla de lino, grano de sorgo, alimento de molino, mantequilla, huevos, papás, lana, lana peinada, grasas y aceites [...], y todos los servicios, derechos, e intereses [...] sobre los cuales se pacten y se negocien contratos de futuros de manera presente o futura²⁰¹.

Conforme a esta definición, la CFTC ha emprendido diversas acciones relativas a activos virtuales, ya que existen plataformas que comercian con contratos de futuros utilizando el bitcoin como subyacente. Consecuentemente, desde el 2014 la CFTC ha discutido acerca de su posible papel en la regulación de los activos virtuales²⁰². De manera posterior, en el 2015, la institución determinó que bitcoin caía dentro del

²⁰⁰ (SEC, 2017) en (Giancarlo, 2018)

²⁰¹ Commodity Exchange Act, con enmiendas, y regulaciones subsecuentes (7 U.S.C. § 1a (9)) énfasis añadido.

²⁰² (Massad, 2014)

supuesto de mercancía contenido en la CEA, dada la relación que guardaba con contratos de futuros. La decisión se tomó con base en el caso de Coinflip, Inc., d/b/a Derivabit, y Francisco Riordan compareciendo ante la CFTC²⁰³. Más recientemente, en el 2016, la CFTC emprendió acciones contra una plataforma de intercambio de futuros de bitcoin que no se registró ante la misma²⁰⁴, estableciendo de manera tácita su jurisdicción sobre este tipo de plataformas, reafirmando la obligación de registrarse ante la agencia. A la postre, en septiembre del 2017, la CFTC emprendió tres demandas por la vía civil contra diversas organizaciones por fraude, manipulación de mercados e intercambio de activos virtuales. Entre los demandados destacan: *My Big Coin Pay, Inc*, que emitió un activo fraudulento y cometió malversación de fondos, *The Entrepreneurs Headquarters Limited* por malversación de fondos y *Coin Drop Markets* por fraude y malversación de fondos²⁰⁵.

Estas actuaciones se han destilado en una serie de facultades que se han reconocido como propias del órgano gubernamental que, en palabras de su titular, Christopher Giancarlo son:

“Hacer cumplir la ley investigando mediante citatorios y sus otras facultades de investigación y, si lo cree apropiado, emprender acciones por la vía civil contra fraudes y manipulación de mercados derivados de monedas virtuales y en los mercados *spot* subyacentes”²⁰⁶

Por consiguiente, a las plataformas a través de las cuales se operan con contratos de futuros utilizando como subyacente algún activo virtual, se les impuso la misma obligación de autorregulación a las que están sujetas otras plataformas en las que se comercian otros derivados con subyacentes tradicionales²⁰⁷.

²⁰³ (CFTC Orders Bitcoin Options Trading Platform Operator and its CEO to Cease Illegally Offering Bitcoin Options and to Cease Operating a Facility for Trading or Processing of Swaps without Registering, 2015) ver en línea en: "<http://www.cftc.gov/PressRoom/PressReleases/pr7231-15>"

²⁰⁴ (CFTC, 2016)

²⁰⁵ (Giancarlo, 2018, p. 6)

²⁰⁶ *Ibidem*, p. 4

²⁰⁷ *Ibidem*, p. 7

En conformidad con lo anterior, las plataformas de intercambio de futuros de bitcoin han estado en constante comunicación con la agencia para afinar los detalles de su operación. A lo largo de este proceso, los funcionarios del CFTC buscaron priorizar la visibilidad, datos, y monitoreo de los mercados de derivados de bitcoin y las tasas de referencia de liquidación subyacentes²⁰⁸. Esta información permite a la agencia tener una visión mucho más clara de los precios de los activos con el objeto de evitar fraudes y manipulación en los mercados. Lo anterior ha permitido, de acuerdo con Giancarlo, tener en los EE. UU. el primer mercado de derivados de bitcoin regulado a nivel federal en el mundo²⁰⁹.

No obstante, lo hecho por la CFTC no sólo comprende acciones apuntadas hacia la regulación de operadores clave de la industria, sino que ha emprendido otras labores para proteger a la población. Una de ellas fue la formación de diversos grupos de trabajo que han asistido a la comisión en buscar el cumplimiento novedoso en materia regulatoria. El primero de ellos es un grupo interno de trabajo especializado en materia de activos virtuales²¹⁰, otro es el *LabCFTC*²¹¹ que busca “promover innovación responsable y competencia justa en beneficio del público estadounidense, [...] sirviendo como una plataforma para mantener informado al regulador de nuevas tecnologías y desarrollar políticas públicas adecuadas”. A la par, se nombró un *Chief Innovation Officer* (“CINO”) para promover la innovación dentro de la organización²¹². Conjuntamente, la agencia ha hecho grandes esfuerzos por educar a la población acerca de los riesgos que puede suponer invertir grandes cantidades de dinero en cripto-activos sumamente volátiles²¹³. Este esfuerzo pedagógico ha sido el más grande en la historia del organismo²¹⁴. Entre los materiales que se han hecho del conocimiento del público se encuentran: “información básica de activos virtuales, consejos de mercado al invertir en activos

²⁰⁸ *Ibidem*, p. 8

²⁰⁹ *Ídem*

²¹⁰ *Ibidem*, p. 5

²¹¹ Ver en línea en: <http://www.cftc.gov/bitcoin/index.htm>

²¹² (Comité de Banca, Vivienda y Asuntos Urbanos, 2018)

²¹³ *Ídem*

²¹⁴ *Ídem*

virtuales, una página web dedicada al bitcoin²¹⁵ con “podcasts relevantes en materia de activos virtuales y la tecnología subyacente y una publicación semanal de datos relevantes al intercambio de bitcoin”²¹⁶. Este esfuerzo se ha hecho junto a múltiples instituciones que pugnan por la protección del público.

Sin embargo, la agencia considera no tener jurisdicción sobre los mercados *spot*²¹⁷ en los cuales se comercian con activos virtuales²¹⁸. Más aún, a consideración de este órgano regulador, ninguna agencia gubernamental federal posee tales facultades, de acuerdo con el estado actual del ordenamiento jurídico²¹⁹. Por lo que existe una laguna legal en materia de competencia, que aún es disputada entre agencias y que seguramente pronto requerirá intervención legislativa.

En consecuencia, el titular de la CFTC, Christopher Giancarlo sugirió la creación de una reglamentación alternativa para los mercados *spot*, dejando a un lado la figura de transmisor de dinero regulada a nivel estatal que en su opinión no otorga una protección completa a consumidores e inversionistas²²⁰. Defendió su idea expresando lo siguiente:

“Se debe de caminar hacia una regulación federal muy pulida, centrándose en los riesgos que presentan las actividades de intercambio actual, manteniendo los esfuerzos de perseguir fraudes e intentos de manipulación. La adecuada supervisión federal debe de incluir la obligación de reportar información, requerimientos de capital, requisitos de ciberseguridad, medidas para prevenir fraude y manipulación de precio y antilavado de dinero y protecciones en materia de “*know your*

²¹⁵ Los recursos pueden ser consultados en la siguiente dirección web: <http://www.cftc.gov/bitcoin/index.htm>

²¹⁶ (Giancarlo, 2018, p. 9)

²¹⁷ El *Model State Commodity Code* contiene a una excepción a un contrato de mercancías cuando el acuerdo ocurre dentro de un plazo de 28 días, para más información ver: *Model State Commodity Code* sección 1.01(e). En parte por lo anterior, la CFTC no tiene jurisdicción sobre los mercados *spot* modernos de activos virtuales, en los cuales las operaciones típicamente se cierran en mucho tiempo menor que 28 días, privando a los inversionistas de la protección del CEA. (Commodity Futures Trading Commission, 2017, p. 60339)

²¹⁸ (Giancarlo, 2018, p. 4)

²¹⁹ *Ídem*

²²⁰ (Giancarlo, 2018, p. 13)

customer”. Sobre todo, un posible marco jurídico federal debe de propugnar por ser eficiente y efectivo en asegurar la integridad del mercado subyacente²²¹.”

En síntesis, la CFTC ha emprendido un acercamiento basado en los siguientes puntos²²²: Educación del consumidor, establecimiento de su autoridad legal sobre instrumentos derivados de activos virtuales, redoblar sus esfuerzos en materia antifraude y manipulación, implementar labores de inteligencia en el mercado, fortalecer sus capacidades de monitoreo de mercados de activos virtuales, robustecer la aplicación de la ley y mantener una coordinación junto con las demás agencias que pudieran ser competentes, incluyendo a los órganos de impartición de justicia, la rama legislativa, la ejecutiva y otros actores relevantes.

Los esfuerzos realizados en materia regulatoria y de protección del público inversionista y la estabilidad de los mercados han sido significativos, pero sólo el tiempo dirá si las decisiones tomadas al respecto fueron las correctas.

²²¹ (Giancarlo, 2018, p. 14)

²²² (CFTC Backgrounder on Oversight of and Approach to Virtual Currency Futures Markets, CFTC, 2018)

V.1.3. *Financial Crimes Enforcement Network*

FinCEN es una agencia que forma parte del Departamento del Tesoro de los EE. UU. y tiene el mandato de recopilar y analizar cúmulos de información financiera con el objeto de prevenir, investigar y castigar delitos financieros, fraude, lavado de dinero y financiamiento a grupos terroristas, protegiendo al sistema financiero estadounidense en el proceso. Entre sus facultades se encuentra la posibilidad de supervisar las instituciones financieras, como los servicios transmisores de dinero. Esta figura resulta particularmente relevante para el presente trabajo ya que, a falta de una legislación adecuada, es la denominación bajo la cual se han constituido múltiples plataformas de intercambio de activos virtuales. Esto a pesar de que la naturaleza de las plataformas de intercambio no es completamente compatible con la de la figura, en parte por las razones expuestas en el capítulo anterior.

No obstante, FinCEN emitió una guía interpretativa en marzo de 2013, en la cual se establecieron ciertos conceptos relevantes con consecuencias jurídicas concretas para los *exchanges*. En primer lugar, se definieron las nociones de lo que se considera es un administrador o intercambiador, categoría en la cual entran las plataformas de intercambio de activos virtuales:

“Intercambiador: es una persona involucrada como empresa con el intercambio de monedas virtuales por monedas reales, fondos u otras monedas virtuales.”²²³

“Administrador: es una persona involucrada como negocio en emitir (poner en circulación) una moneda virtual, y tiene la autoridad para redimir (a sacar de la circulación) dicha moneda virtual.”²²⁴

²²³ (FinCEN, 2013, p. 2)

²²⁴ *Idem*

A continuación, precisó lo que entiende la agencia por un servicio de transmisión de dinero, o como se les conoce en inglés *money services businesses* (“MSB”), estableciendo que los administradores o intercambiadores que:

- (i) acepten o transmitan una moneda virtual convertible o
- (ii) compren o vendan monedas virtuales convertibles por cualquier razón²²⁵

Serán considerados a los ojos de la agencia un MSB, debiéndose registrar como tal²²⁶. Lo anterior se confirma por la definición de un MSB, dada por propia agencia:

“Aquel servicio consistente en la aceptación de dinero, fondos, o cualquier otro valor que sustituya al dinero de una persona y la transmisión de dinero, fondos, u otro tipo de valor que sustituya a el dinero a otra ubicación o persona por cualquier medio.”²²⁷

El encuadre de una plataforma de intercambio en la figura de un MSB es desafortunado ya que a pesar de que hay elementos en común entre ambas figuras, el espíritu de los intercambios no es la transmisión de valor, como si lo es en un MSB, además que la necesidad de una licencia estatal entorpece innecesariamente la operación de los *exchanges*. Asimismo, la reglamentación de un MSB no está totalmente adaptada a las particularidades de un intercambio, muestra de ello es que la definición de un servicio de dinero no establece diferencia entre transmisión de dinero real y virtual²²⁸.

No obstante, a través del mismo comunicado, la agencia declara que un usuario que utilice las monedas para comprar bienes y servicios no será clasificado como un MSB²²⁹. En la misma línea, en un documento posterior se precisó que los

²²⁵ *Ibidem*, p. 3

²²⁶ (FinCEN, 2013, p. 2)

²²⁷ 31 CFR § 1010.100(ff)(5)(i)(A)

²²⁸ (FinCEN, 2013, p. 3)

²²⁹ *Ibidem*, p. 2

usuarios que mediante un equipo computacional “minen” un activo²³⁰, tampoco serán considerados como MSB, en el entendido que el usuario mine el activo con fines personales y no para el beneficio de otro.

La evolución del criterio de la agencia continuó en fechas más recientes, específicamente el 13 de febrero del 2018²³¹, cuando FinCEN envió una carta²³² al Senador Wyden en la cual hablaba acerca de sus facultades regulatorias en materia de activos virtuales. Especificaba que, un vendedor de *tokens* caía en la misma categoría que una plataforma de intercambio y por lo tanto se debía de considerar como un MSB, estando obligado a cumplir con los requerimientos en materia de antilavado y evitar el fondeo al terrorismo. Esto implica que cualquier persona que:

(A) Haya vendido *tokens* a compradores que sean residentes de los Estados Unidos de América (por ejemplo, a través de un *ICO*) y

(B) No se hayan registrado con FinCEN como un servicio de transmisión de dinero y cumplido con los requisitos en materia de antilavado de dinero y de KYC,

Puede ser perseguida por cometer un delito federal²³³. Empero, esta carta no es clara en cuanto a cómo FinCEN determinará que se viola esta normativa y a las decisiones que tomará la agencia en el futuro al respecto, agregando a la incertidumbre legal de la industria.

Es notable que no existe un consenso entre las distintas agencias en cuanto a qué es un activo virtual, clasificándolo cada agencia a modo que encuadre en sus facultades regulatorias. Esta situación deriva en una completa confusión para los usuarios y prestadores de servicios, que se encuentran en diferentes marcos regulatorios dependiendo de la agencia a la que se le pregunte, con diferentes requisitos cada uno. Asimismo, es muy preocupante que se esté legislando sobre

²³⁰ (FinCEN, 2014)

²³¹ La carta fue liberada al público el día 6 de marzo de 2018.

²³² (Van Valkenburgh, 2018), carta de Drew Maloney, secretario asistente para asuntos legislativos FinCEN dirigida al senador Ron Wyden fechada 13 de febrero de 2018, ver en línea en: <https://coincenter.org/files/2018-03/fincen-ico-letter-march-2018-coin-center.pdf>

²³³ (Van Valkenburgh, 2018)

una materia que es tan nueva e innovadora, a través de actos administrativos que ni si quiera son claros o vienen acompañados de una debida explicación que ayude a entender el por qué un órgano gubernamental actuó de determinada manera. La situación debe cambiar, debiendo dejar atrás la situación de nula certeza que se vive hoy en día y crear reglas claras que incentiven la inversión y le den seguridad a los inversionistas y a la industria en general.

V.2. Suiza

Suiza es considerado como un centro financiero de importancia global que no se ha quedado atrás en el tema de activos virtuales, incentivando cada vez más la inversión en el sector de las tecnologías financieras. La estrategia ha rendido frutos ya que son cientos de proyectos que se han financiado, y continúan haciéndolo, a través de un *ICO* y que tienen como base el territorio suizo, obteniendo grandes cantidades de capital. Al mismo tiempo, se han impulsado clústeres de innovación en materia de *blockchain*, siendo el más famoso de ellos la zona conocida por el nombre de “*Crypto Valley*”, una región conocida por el gran número de compañías que desarrollan proyectos basados en la tecnología de cadena de bloques.

Adicionalmente, el Concilio Federal Suizo propuso en 2017²³⁴ un esquema de regulación tipo “*sandbox*”²³⁵ para empresas que utilicen nuevas tecnologías abonando a un panorama regulatorio amigable para la innovación. Todo esto rodeado de declaraciones de oficiales del gobierno que ven en la tecnología *blockchain* una gran oportunidad de desarrollo, propugnando por una regulación “liberal” que “abra oportunidades para mejorar la posición suiza, al tiempo que se reducen riesgos”²³⁶. En este contexto han aumentado los esfuerzos regulatorios que tienen como objetivo promover el desarrollo de la industria y proteger al público. Uno de estos ha sido la creación en 2018 de un grupo de trabajo concentrado en la supervisión de la tecnología *blockchain* y *ICOs* que incluye miembros de distintas dependencias gubernamentales con el objetivo de brindar mayor certidumbre regulatoria en la materia²³⁷, que se añade a la labor de los órganos ya existentes.

Actualmente, la autoridad encargada de regular los mercados financieros en suiza es la Autoridad Financiera Suiza de Supervisión de Mercados Financieros (“FINMA”)

²³⁴ (Higgins, 2017)

²³⁵ Término que se refiere a un espacio regulatorio en el cual las compañías pueden experimentar con diferentes modelos de negocio no convencionales o apropiadamente regulados, sin llegar a ser ilegales, que permite una innovación acelerada que no espera a una adecuada respuesta regulatoria.

²³⁶ (De, 2018)

²³⁷ (Reuters, 2018)

la cual ha emitido diversos comunicados para aclarar al público la postura que tomará en materia de regulación de activos virtuales. Las recomendaciones, si bien tocan otros puntos, toman como eje central los *ICO* o eventos generados de *tokens*.

El primer documento que se publicó sobre el tema son las directrices 04/2017 en materia de tratamiento regulatorio de *Initial Coin Offerings*²³⁸, en las cuales se recuerda que la regulación financiera suiza está basada en ciertos principios. De la misma manera, plantea que, dependiendo de la manera en la que se estructure un *ICO* puede estar sujeto a diversas obligaciones de la ley financiera suiza existente. En caso de que el *token* emitido sea utilizado como medio de pago se deben de desplegar medidas para evitar de lavado de dinero y financiamiento al terrorismo, ya que aplicarán las medias regulatorias correspondientes. Asimismo, se establece que, si los *tokens* generan una obligación hacia los vendedores de estos, la reglamentación que aplicaría, de acuerdo con FINMA²³⁹, sería en materia bancaria, y el *ICO* necesitaría una licencia bancaria para su realización. En la misma línea, se necesitaría un permiso para operar con *tokens* que sean clasificados como valores por la autoridad competente. Finalmente, advierte sobre las posibles consecuencias que podría traer el que un tercero maneje el capital levantado a través de un *ICO*. No obstante, el comunicado aclara que toda decisión se tomará atendiendo al caso concreto y que las dudas al respecto deben de hacerse llegar a la agencia para ser respondidas adecuadamente y evitar sanciones.

Posteriormente, en febrero de 2018, se emitieron nuevas directrices²⁴⁰ en las cuales se establecía de manera más precisa el marco regulatorio de un *ICO*, reiterando que el análisis se hará caso por caso y previo análisis de las circunstancias particulares del proyecto y se pide que se hagan llegar las dudas a la agencia para ser aclaradas. La novedad en este escrito es que presenta una serie de principios aplicables a las solicitudes y reconoce que más allá de que tienen similitudes con figuras existentes, los *ICOs* presentan una serie de problemas legales que no son

²³⁸ (FINMA, 2017)

²³⁹ *Ibidem*, p. 3

²⁴⁰ *Ídem*

solucionados de manera satisfactoria por ningún ordenamiento o doctrina existente²⁴¹.

En consecuencia, establece una categorización provisional de los *tokens* de acuerdo con su función económica subyacente, que si bien ya había sido presentada de manera indirecta con anterioridad, se presenta a mayor profundidad y explicando ciertos conceptos con mayor claridad. Primeramente, se mencionan los *tokens* de pago, aquellos también conocidos como cripto-monedas, los cuales son utilizados como medio de pago de bienes o servicios, dinero o transferencia de valor, estos no generan ninguna responsabilidad para el emisor. Posteriormente, presenta los llamados *tokens* de utilidad, los cuales cumplen la función de proveer acceso digital a una aplicación o servicio basado en infraestructura de cadena de bloques. Consecutivamente, introduce a los *tokens* tipo activo que representan deuda o una participación en el capital social de quien los emite, prometiendo un beneficio económico al tenedor, ya sea mediante una participación en las utilidades, rendimientos o cualquier otro, siendo análogos, en materia económica a acciones, deuda o derivados de acuerdo con el caso concreto. De igual manera, pertenecen a esta categoría aquellos *tokens* que están relacionados de alguna manera con activos reales. Por último, se hace mención de las preventas, que FINMA considera como una manera de los inversionistas de comprar *tokens* cuya única finalidad es ser posteriormente permutados por otros diferentes y que ultimadamente son los que desea el inversor.

Es transcendental mencionar que esta clasificación, al igual que las demás que existen hasta ahora, no es rígida o excluyente, por lo que un token puede circular libremente por cualquiera de las categorizaciones o incluso ser considerado como un token híbrido²⁴².

²⁴¹ *Ídem*

²⁴² *Ídem*

Con posterioridad en el escrito, la agencia discute si se deben o no considerar ciertos *tokens* como valores y bajo qué circunstancias. Para abordar la discusión, en primer lugar, presenta la definición de un valor en su legislación:

“Certificados estándar o valores no certificados, derivados y valores intermedios²⁴³, que son adecuados para una alta bursatilización, suponiendo que no hayan sido creados para contrapartes individuales.”

244

Después, ahonda en la definición determinado a se refiere con valores no certificados:

“Se establecen los valores no certificados como derechos que basados en una base legal común son emitidos o establecidos en largas cantidades y son genéricamente iguales, teniendo el emisor como obligación mantener un registro en el cual se detalle el número y denominación de los valores no certificados emitidos y los tenedores estén registrados.”²⁴⁵

Se desprende de la definición anterior que los *tokens* tipo activos, de acuerdo con la clasificación de FINMA, podrían ser considerados como valores, específicamente no certificados, dada la naturaleza del activo y la definición. No obstante, la agencia hace hincapié en que no tomará decisiones respecto a la naturaleza de las *AppCoins* sin antes revisar el caso particular.

Los tokens valores sólo podrán ser considerados como valores si representan un valor no certificado, además de estar estandarizados y ser adecuados para el intercambio masivo. También serán considerados como valores aquellos que representen un derivado y cumplan con las características de estandarización y liquidez. Igualmente, tendrán la misma naturaleza las preventas en las que se comprometan *tokens* futuros. En caso de que la autoridad efectivamente los

²⁴³ Art. 2 let. B FMIA en (FINMA, 2018, p. 4)

²⁴⁴ Art. 2 párrafo primero de FMIA en (FINMA, 2018, p. 4)

²⁴⁵ Artículo 973c párrafo tercero Código de Obligaciones Suizo en (FINMA, 2018, p. 4)

considere valores se registrarán por lo establecido en el artículo 2 let. B de la *Financial Market Infrastructure Act* (“FMIA”).

En cuanto a los *tokens* de pago, o cripto-monedas, FINMA anuncia que, dado que estos están diseñados para ser utilizados como medio de pago y no son análogos en naturaleza a valores tradicionales, no les dará el tratamiento de valores, advirtiendo que esto puede cambiar a través de la resolución de un nuevo caso o con el surgimiento de nueva legislación²⁴⁶. El mismo tratamiento se les dará a los *tokens* que cumplan con una función de utilidad, sólo si su único propósito es dar acceso a un producto o servicio de naturaleza digital, siendo importante en estos casos no la denominación del *token* sino su naturaleza.

Las consecuencias jurídicas de que un *token* sea considerado como un valor bajo la legislación suiza se encuentran previstas en la *Stock Exchange Act* (“SESTA”). Los valores no certificados están básicamente no regulados²⁴⁷ al igual que las ofertas públicas de valores a terceros. En contraste, la creación de un producto derivado está sujeta a lo establecido en el Artículo 3° párrafo tercero del *Stock Exchange Ordinance* (“SESTO”). A la par, garantizar y ofrecer *tokens* que constituyan valores de terceros de manera pública en el mercado primario es, si se conduce de manera profesional, una actividad que requiere licencia en términos del Artículo 3° párrafo 2 de SESTO. De igual manera, la agencia considera, que la emisión de *tokens* con la misma naturaleza de un bono de deuda o una participación social puede, atendiendo al caso concreto, obligar al emisor a presentar un prospecto de inversión, de acuerdo con el Código Suizo de Obligaciones²⁴⁸.

No obstante, FINMA no sólo aborda el tema desde el punto de vista si ciertos *tokens* son o no valores, también toma un acercamiento con relación a la posible naturaleza de depósitos de activos virtuales, estableciendo que se constituirá depósito cuando existe una promesa de retorno de capital garantizado. En este caso, se considera

²⁴⁶ (FINMA, 2018, p. 4)

²⁴⁷ (FINMA, 2018, p. 4)

²⁴⁸ *Ibidem*, p. 6

que el capital es un depósito y se requiere una licencia de banca para operar con ellos, en concordancia con el *Banking Act*²⁴⁹. Asimismo, advierte a la industria de la posibilidad de verse sujetos a la *Collective Investment Schemes Act* en caso de que los fondos levantados a través de un *ICO* sean manejados por un tercero, como si de un fondo de inversión se tratara.

La última categoría de obligaciones que tocan las directrices son las relacionadas con la prevención de lavado de dinero y financiamiento a grupos terroristas. Estas aplicarán en el caso que se emitan *tokens* que tengan por finalidad servir como medio de pago, estando el emisor sujeto a dichas obligaciones, tal como se establece en la *Anti-Money Laundering Act* (“*AML*”). No obstante, esta regulación no es aplicable en el caso de *tokens* de utilidad²⁵⁰. Las obligaciones que establece *AML* para los proyectos que caigan en el supuesto incluyen el registro de la identidad del dueño beneficiario y afiliarse a una organización auto regulatoria o sujetarse directamente a la supervisión de *FINMA*.

Posteriormente, la parte final del reporte es especialmente relevante dado que las actividades realizadas por los intercambios en los cuales se cambian activos virtuales por moneda fiduciaria, o viceversa, caen en lo establecido en Artículo 2 párrafo 3 de *AML*, teniendo que cumplir con las obligaciones pertinentes. Aplicando lo mismo para cualquier servicio de transferencia de *tokens* en los cuales el proveedor del servicio mantenga la custodia de la llave privada²⁵¹.

²⁴⁹ *Ídem*

²⁵⁰ *Ídem*

²⁵¹ *Ibidem*, p. 6

La anterior clasificación de obligaciones respecto a la categorización de *tokens* es convenientemente resumida en una tabla, contenida en la misma circular, que se presenta a continuación:

	Pre-financing and pre-sale / The token does not yet exist but the claims are tradeable	The token exists
ICO of payment tokens	= Securities ≠ subject to AMLA	≠ Securities = means of payment under AMLA
ICO of utility tokens		≠ Securities, if exclusively a functioning utility token = Securities, if also or only investment function ≠ means of payment under AMLA
ICO of asset tokens		= Securities ≠ means of payment under AMLA

Figura 2. Tabla que, de manera resumida, presenta la posición del regulador suizo en materia de activos virtuales²⁵².

Por último, el documento informa de los requerimientos mínimos en materia de información que deben contemplar los que deseen llevar a cabo un *ICO*²⁵³ y menciona que FINMA se reserva la posibilidad de cambiar lo establecido en la presente circular en la medida las condiciones del mercado se modifiquen.

²⁵² *Ibidem*, p. 8

²⁵³ Para más información ver: (FINMA, 2018)

Por lo escrito en las anteriores directrices, es evidente la postura más flexible que presenta FINMA respecto a los activos virtuales con relación a su contraparte estadounidense, la SEC. La autoridad suiza tiene una mayor apertura a no considerar ciertos *ICOs* y *tokens* como valores, además de que en caso de que sean considerados como tales, la carga regulatoria es, en términos generales, mucho menor. Sin embargo, parece una constante la imposición de obligaciones en materia de prevención de lavado de dinero y financiamiento a organizaciones criminales. Asimismo, como parece ocurrir en este momento en múltiples jurisdicciones, la autoridad se muestra recelosa en tomar una postura determinante, esperando la consolidación del fenómeno para discurrir la mejor manera de regularlo.

VI. Panorama Nacional

A continuación, será abordado el estado que guarda el país en materia de tecnologías financieras. Concretamente en lo que se refiere a activos virtuales y a la operación con los mismos.

El objetivo del presente capítulo es hacer un análisis pormenorizado del marco jurídico mexicano en materia de activos virtuales, haciendo hincapié en la LRITF. Asimismo, se expondrán diversos comunicados emitidos por las autoridades que contienen disposiciones relevantes. Esto en un intento de comprender la actitud de estas hacia los activos virtuales.

El propósito es mostrar de manera puntual que disposiciones se consideran como un acierto y cuales se piensan inadecuadas, junto con las razones para calificarlas como tales. Dicho análisis se hará a la luz de las características de los activos virtuales y la experiencia internacional.

En primer lugar, serán presentadas las múltiples disposiciones que preceden a la ley específica en la materia, la Ley para Regular las Instituciones de Tecnología Financiera (“Ley Fintech” o “LRITF”) emitidas por diversas autoridades, como el Servicio de Administración Tributaria, el Banco de México, la Secretaría de Hacienda y Crédito Público y la Comisión Nacional Bancaria y de Valores.

Posteriormente, se esbozará el desarrollo de la legislación actual, incluyendo las leyes que fueron reformadas con la entrada en vigor de ésta, sirviendo esto como un puente para explorar otras disposiciones relevantes.

Por último, será presentado un análisis artículo por artículo, o incluso fracción por fracción si es necesario, de los apartados que sean relevantes para el tema de la presente tesis. Esto no quiere decir que serán completamente dejadas a un lado otras disposiciones de la ley, las cuales, se presentarán a manera de contextualizar el tema central, únicamente deteniéndose en aquellas que sean particularmente relevantes.

VI.1 Disposiciones de Autoridades Diversas

VI.1.1. Servicio de Administración Tributaria

En enero de 2016 el Servicio de Administración Tributaria (“SAT”) dio a conocer un comunicado con título “Respecto a la utilización de Activos Virtuales en los actos u operaciones establecidos en el artículo 32 de la Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita (LFPIORPI)”²⁵⁴. A través de dicho documento, el SAT determinaba, basándose en los reportes de la FATF, limitar el uso de activos virtuales como medio de pago en los supuestos señalados en el artículo 32 de la LFPIORPI ²⁵⁵, prohibiendo o limitando el uso de

²⁵⁴ (Servicio de Administración Tributaria, 2015), consultar en línea en: <https://sppld.sat.gob.mx/pld/interiores/noticias.html>

²⁵⁵ Entre estos supuestos se encuentran:

I. Constitución o transmisión de derechos reales sobre bienes inmuebles por un valor igual o superior al equivalente a ocho mil veinticinco veces el salario mínimo vigente en el Distrito Federal, al día en que se realice el pago o se cumpla la obligación.

II. Transmisiones de propiedad o constitución de derechos reales sobre vehículos, nuevos o usados, ya sean aéreos, marítimos o terrestres por un valor igual o superior al equivalente a tres mil doscientas diez veces el salario mínimo vigente en el Distrito Federal, al día en que se realice el pago o se cumpla la obligación;

III. Transmisiones de propiedad de relojes, joyería, Metales Preciosos y Piedras Preciosas, ya sea por pieza o por lote, y de obras de arte, por un valor igual o superior al equivalente a tres mil doscientas diez veces el salario mínimo vigente en el Distrito Federal, al día en que se realice el pago o se cumpla la obligación;

IV. Adquisición de boletos que permita participar en juegos con apuesta, concursos o sorteos, así como la entrega o pago de premios por haber participado en dichos juegos con apuesta, concursos o sorteos por un valor igual o superior al equivalente a tres mil doscientos diez veces el salario mínimo vigente en el Distrito Federal, al día en que se realice el pago o se cumpla la obligación;

V. Prestación de servicios de blindaje para cualquier vehículo de los referidos en la fracción II de este artículo o bien, para bienes inmuebles por un valor igual o superior al equivalente a tres mil doscientas diez veces el salario mínimo vigente en el Distrito Federal, al día en que se realice el pago o se cumpla la obligación;

VI. Transmisión de dominio o constitución de derechos de cualquier naturaleza sobre los títulos representativos de partes sociales o acciones de personas morales por un valor igual o superior al equivalente a tres mil doscientas diez veces el salario mínimo vigente en el Distrito Federal, al día en que se realice el pago o se cumpla la obligación, o

activos virtuales para dar “cumplimiento a obligaciones y, en general, liquidar o pagar, así como aceptar la liquidación o el pago, de actos u operaciones mediante activos virtuales”. Es decir, dándole un trato similar al del efectivo en cuanto a cumplimiento de obligaciones monetarias

Para dar cumplimiento a la prohibición previamente mencionada, el SAT define a los activos virtuales como:

“En singular o plural, al conjunto de datos almacenados en medios informáticos susceptibles de transmitirse electrónicamente que, sin ser moneda de curso legal en jurisdicción alguna, se utilizan como medio de cambio o unidad de cuenta para realizar operaciones de tipo comercial o económico o, en su caso, efectuar pagos.”

Esta definición es diferente a la establecida en la LRITF en su artículo 30, siendo bastante más amplia y con el claro objetivo de abarcar todo lo que pudiese ser usado como medio de pago o intercambio de valor. Asimismo, en el comunicado también se hace la diferenciación, tal como lo hace la FATF, de dinero virtual convertible y no convertible, únicamente imponiendo restricciones al primero.

Inicialmente la prohibición parece tener sentido y se entiende proporcional, dada la naturaleza semi-anónima del bitcoin²⁵⁶ y la anónima de otros activos virtuales. Empero, de este aviso surgen ciertas dudas que no son esclarecidas y que son fundamentales para la aplicación de la disposición. La más importante es cómo se determinará el precio de los activos virtuales para establecer si la operación en cuestión está, o no, superando los umbrales establecidos en el artículo 32 de la LFPIORPI.

VII. Constitución de derechos personales de uso o goce de cualquiera de los bienes a que se refieren las fracciones I, II y V de este artículo, por un valor igual o superior al equivalente a tres mil doscientas diez veces el salario mínimo vigente en el Distrito Federal, mensuales al día en que se realice el pago o se cumpla la obligación.

²⁵⁶ La percepción que tiene el público respecto a la supuesta anonimidad que da el uso de bitcoin es, hasta cierto punto, equivocada. Para más información ver (Ludwin, 2015)

Existen diversos métodos para hacer esto, una posibilidad es adoptar el precio que muestre un índice en tiempo real o una tasa de referencia de un determinado organismo, como el del CME Group²⁵⁷, el cual fue lanzado en noviembre de 2016 y provee una tasa de referencia e índice de precio basándose en los mercados *spot* utilizando métodos estandarizados y bajo supervisión independiente. Al momento de considerar esta solución se debe recordar que no existe un índice que presente el precio del bitcoin en pesos mexicanos, siendo la mayoría en dólares, por lo que la cantidad tendría que ser convertida en pesos tomando el tipo de cambio oficial publicado en el Diario Oficial de la Federación (“DOF”).

Por otro lado, otra manera de establecer el valor de un activo virtual como el bitcoin es mediante una supervisión directa del mercado por una autoridad mexicana debidamente facultada. Pero este segundo método trae a su vez nuevas interrogantes, ¿Qué sitios de intercambio serán consultados? En el mercado mexicano existen un número muy pequeño de dichas plataformas, ¿Estás serían suficientes? ¿Se recurriría a consultar los precios de plataformas que operen en otros países? En el caso de esta propuesta, se presume que los intercambios consultados deberían de cumplir con ciertos requisitos para ser considerados, que podrían ser en materia de volumen de operaciones, tiempo en operación, número de clientes o cualquier otro.

Continuando con los inconvenientes que presenta el comunicado, emerge la cuestión en el caso de que se publique un precio “oficial” si se considerará el mismo para todo el día o si este será actualizado en tiempo real para efectos de la anterior disposición y otras similares. Es relevante para la discusión mencionar que a lo largo de una sola jornada el bitcoin ha visto cambios importantes en su precio²⁵⁸.

Lo dicho con anterioridad es únicamente con relación al activo virtual bitcoin, sin embargo, hay muchos otros activos virtuales que se cotizan contra el peso, como el

²⁵⁷ El índice puede ser consultado en la siguiente dirección: <http://www.cmegroup.com/trading/cf-bitcoin-reference-rate.html>

²⁵⁸ (Coindesk, 2018)

ether, litecoin o ripple, entre otros. Asimismo, existe una enorme variedad de otros activos virtuales, de los cuales la mayoría se cotiza exclusivamente en intercambios extranjeros. Que, si bien su valor podría ser determinado tomando en cuenta su precio con relación al bitcoin, su precio varía enormemente entre diferentes plataformas de intercambio, por no hablar de jornada en jornada, con diferencias positivas o negativas de más del 100% de su valor²⁵⁹.

Es evidente que perduran numerosas dudas respecto del comunicado tal y cómo fue emitido. Una manera plausible para resolver el problema se podría basar en algún tipo de índice con carácter oficial para referencia de los usuarios, que contenga un precio de referencia para los activos más relevantes en términos de volumen o de capitalización de mercado y contra los cuales los contribuyentes puedan comparar los precios de sus activos menos populares, si es que son propietarios de alguno. En este punto, parece acertado lo hecho por el IRS en la materia²⁶⁰. A esta institución le es indiferente el cómo se determina el precio, mientras se haga de forma “razonable y se aplique de manera consistente”. Es decir, si el contribuyente decide tomar el precio del momento o del inicio del día es libre de hacerlo, siempre y cuando lo haga de manera consistente²⁶¹. Este experimento podría ir más allá y confiar en el contribuyente para que registre el valor de la operación sin ningún tipo de índice de referencia oficial mientras lo haga de una manera razonable y consistente. No obstante, esto traería problemas de certeza jurídica además de probatorios, sobre todo con activos no listados por intercambio nacionales, que ultimadamente podrían afectar al contribuyente.

²⁵⁹ Para confirmar lo anterior no se requiere más que visitar algún sitio como <https://coinmarketcap.com/> que muestra el cambio de precio diario de cientos de cripto activos.

²⁶⁰ (Internal Revenue Service, 2014)

²⁶¹ No obstante, la metodología usada por el IRS presenta grandes complicaciones en algunos rubros, ya que el evento que genera el impuesto no es la compra del activo y su subida de valor, si no la ganancia al efectuar una operación donde se utiliza. Es decir, si un contribuyente adquiere una unidad de bitcoin en \$7,000 USD y su valor sube a \$8,000 USD, no debe pagar impuestos por esto, pero si compra algo, aunque sea un refresco de menos de un USD debe de pagar impuestos por esa subida de valor. Debe de registrar el precio que tenía el activo virtual al momento de su compra y cuando se realizó la transacción, esto para cada operación, lo cual parece sumamente impráctico. (Orcutt, 2018)

Por lo demás, será complicado en la práctica dar seguimiento a este tipo de operaciones. No hay manera de que el SAT, o cualquier otra autoridad, sepa acerca de operaciones con activos virtuales, sino hasta que estos se intercambian por pesos en un *exchange*, lo cual puede nunca suceder.

VI.1.2. Banco de México, Comisión Nacional Bancaria y de Valores y Secretaría de Hacienda y Crédito Público

En primer lugar, se debe de mencionar que el Banco de México jugará un papel fundamental en la regulación de activos virtuales gracias a las facultades que le otorga la nueva LRITF, en especial las relativas a la emisión de normativa secundaria. La legislación previamente mencionada es meramente una ley marco cuyas disposiciones deben de ser complementadas con disposiciones de carácter general que emitirán con posterioridad diversas autoridades. En el caso particular de las IFPE y los activos virtuales, la autoridad encargada de emitir la gran mayoría de estas disposiciones es Banxico. Algunas de estas reglas son cruciales para la operación de una institución que opera con activos virtuales, siendo la cuestión más importante la potestad que tiene el Banco Central de autorizar la operación con ciertos activos y otorgar un permiso para operar con los que si están autorizados. Es decir, Banxico decide con que activos puede operar una Institución de Tecnología Financiera (“ITF”) y con cuales no, y si ésta puede hacerlo. Este es un poder enorme que deriva de una disposición sumamente desafortunada que será analizada en su debido momento. Pero antes de entrar en ese tema, es importante aclarar que antes de la publicación de la LRITF, Banxico emitió comunicados para establecer la posición de la institución hacia los activos virtuales.

En marzo del 2014, Banxico publicó un comunicado de prensa con título “Advertencias sobre el uso de activos virtuales como sucedáneos de los medios de pago en moneda de curso legal”²⁶². En este documento, la institución advierte del riesgo que representa el uso de activos virtuales, explicando que son “mecanismos de almacenamiento e intercambio de información electrónica sin respaldo de institución alguna”, dando una definición diferente a las establecidas por el SAT o la LRITF. Al mismo tiempo, mencionó que no son reconocidos como un medio de cambio oficial ni cómo depósito de valor o alguna otra forma de inversión. Asimismo,

²⁶² (Banco de México, 2014), Ver en línea en: <http://www.banxico.org.mx/informacion-para-la-prensa/comunicados/miscelaneos/boletines/%7B5D9E200E-2316-A4B8-92A9-3A5F74938B87%7D.pdf>

establece que no tienen poder liberatorio de obligaciones de pago, por lo que los comercios no están obligados a aceptarlos. De igual manera, establece que no existe ningún tipo de garantía de que quien adquiera este tipo de productos pueda recuperar su dinero y difícilmente procederá una acción legal en contra de algún tercero ya que no hay un emisor responsable. Por último, remata indicado que su precio está sujeto a una gran volatilidad y que su uso ha sido asociado a operaciones ilícitas. Juzgando por el contenido del comunicado, parece que en ese punto el principal objetivo de Banxico fue advertir al público respecto de ciertos aspectos negativos generalmente asociados con un activo virtual.

Posteriormente, el 13 de diciembre de 2017, se emitió un segundo comunicado de prensa, publicado conjuntamente por el Banco de México, la CNBV y la SHCP, titulado “Las autoridades financieras advierten de los riesgos asociados al uso de activos virtuales y a la participación en los esquemas de inversión conocidos como Oferta Inicial de Monedas o *“Initial Coin Offerings”*”²⁶³. Como su nombre lo indica, este reporte versa sobre los posibles riesgos que implica involucrarse en esquemas de ICOs. Este documento es relevante por varios motivos, el primero es que plantea la posibilidad de que algunas ICO, llevadas en México, podrían violar la Ley del Mercado de Valores²⁶⁴ y encuadrar en una conducta tipificada como delito financiero. No obstante, también aclara que la alerta que emite tiene naturaleza preventiva, y es prudente aclarar que a la fecha no es sabido de algún caso en el cual una autoridad mexicana haya perseguido a persona alguna que haya participado en un esquema ICO.

Subsecuentemente, Banxico reitera lo establecido en el reporte de marzo de 2014, haciendo hincapié en la gran volatilidad y la falta de respaldo de los activos virtuales. Por otra parte, en este documento la autoridad menciona, de manera indirecta y parcial, la existencia de diferentes categorías de activos virtuales y acepta de manera tácita que estos pueden tener una naturaleza diferente a la de una “moneda” o “dinero”. Los activos que no se considerarían como dinero serían aquellos a través

²⁶³ (Banxico; CNBV; SHCP, 2017)

²⁶⁴ Esta afirmación queda en duda con la posterior entrada en vigor de la LRITF.

de los cuales se “ofrezca el derecho de acceso a operar en una plataforma a desarrollar, la adquisición de la propiedad de los nuevos activos virtuales, o inclusive, representar la propiedad de bienes de alto valor”²⁶⁵. De igual manera, el documento hace alusión a un tipo diferente activo, los “*security tokens*” o “ficha valor”, los cuales ofrecen ciertos derechos sobre el proyecto a desarrollarse y parte de las ganancias que este pudiere llegar a generar.

En el mismo tenor, advierte que, dependiendo de las características particulares de la ficha o *token*, estos pueden constituirse como valores bajo la Ley del Mercado de Valores, y si es el caso, estar sujetos a las restricciones establecidas en ley²⁶⁶. Esto en conformidad con el artículo 2 de la ley previamente mencionada, que establece el concepto de valor de la siguiente manera:

Artículo 2.- Para efectos de esta Ley se entenderá por:

(...)

XXIV. Valores, las acciones, partes sociales, obligaciones, bonos, títulos opcionales, certificados, pagarés, letras de cambio y demás títulos de crédito, nominados o innominados, inscritos o no en el Registro, susceptibles de circular en los mercados de valores a que se refiere esta Ley, que se emitan en serie o en masa y representen el capital social de una persona moral, una parte alícuota de un bien o la participación en un crédito colectivo o cualquier derecho de crédito individual, en los términos de las leyes nacionales o extranjeras aplicables.

En otro orden de ideas, es positivo que exista un conocimiento por parte de las autoridades reguladoras acerca de las diferentes categorías de activos virtuales, entre los que se vislumbran los *tokens* de utilidad y los *tokens* valores. Junto con esta comprensión, al parecer hay un entendimiento de que deben de reglamentarse

²⁶⁵ *Ídem*

²⁶⁶ De igual manera, la vigencia de esta afirmación queda en duda a partir de lo dispuesto en la LRITF.

de manera diferente dada su naturaleza, tal como plantean la FINMA suiza. Desgraciadamente, esta división entre diferentes tipos de activos virtuales no es mencionada en la LRITF. No obstante, esta situación puede ser corregida en las disposiciones generales emitidas con posterioridad por Banxico. Por último y a manera de conclusión, el documento presenta la promesa de la próxima publicación de la LRITF, la cual presume abonará con un marco jurídico responsable para el espacio de la tecnología financiera.

A manera de síntesis, del comunicado se desprende un entendimiento²⁶⁷ por parte de las principales autoridades financieras, respecto a los distintos tipos de activos virtuales y sus diferencias, mostrando una evolución desde el primer comunicado de Banxico. Por lo tanto, parecería probable que dado que las autoridades reconocen diferentes tipos de activos virtuales eventualmente propongan una regulación desemejante para cada categoría. La nueva LRITF da un margen muy amplio a las autoridades, en particular a Banxico, para regular a los activos virtuales, por lo queda dentro de sus facultades el cómo hacerlo. Por último, es vital reiterar que las acciones de las autoridades responsables serán críticas para el desarrollo de la industria en los próximos años.

²⁶⁷ Se considera parcial dado que no hace referencia más que a dos tipos de activos virtuales en comparación de los múltiples que presentan la FATF o FINMA.

VI.2. Antecedentes y Reformas al Marco Jurídico Existente

Antes de que la LRITF fuera publicada, en el cripto-espacio existía una gran incertidumbre regulatoria que impedía la sofisticación y consolidación de la industria. Los puntos que provocaban mayor preocupación eran la protección al público, mecanismos de KYC y prevención de lavado de dinero. Además, existían dudas respecto a cuál era la figura idónea bajo la cual debían operar las plataformas de intercambio. Al momento de la realización del anteproyecto de la LRITF, estas inquietudes ya estaban sobre la mesa y por lo tanto fueron recogidas por los redactores de la ley. En consecuencia, dentro de los objetivos de crear una nueva legislación fue el otorgar un marco normativo en el cual se plasmaran claramente las obligaciones de las instituciones y los derechos de los usuarios, promoviendo el desarrollo de todo el sector de las tecnologías financieras, dándole certeza a la industria, promoviendo la inclusión financiera y colocando a México como cabeza de sector a nivel mundial.

En el caso mexicano, la legislación se desarrolló de la siguiente manera: El anteproyecto de la LRITF fue elaborado conjuntamente por la SHCP y la CNBV. Una vez concluido el borrador de la ley, fue circulado entre miembros del ecosistema y el sector bancario²⁶⁸ para que aportaran en la construcción de la propuesta. Subsecuentemente, el 9 de octubre del 2017 el Ejecutivo Federal firmó una iniciativa de decreto²⁶⁹, que recogía tanto el trabajo de las instituciones públicas como la opinión de la iniciativa privada, que fue enviada a la Cámara de Senadores.

Con posterioridad, el 12 de octubre del mismo año, la Mesa Directiva del Senado turnó el multicitado documento a las Comisiones Unidas de Hacienda y Crédito Público, de Ciencia y Tecnología y de Estudios Legislativos, Primera, de la Cámara de Senadores de la LXIII Legislatura del Honorable Congreso de la Unión, para su estudio y dictamen, mediante oficio número DGPL-1P3A.-1955²⁷⁰. Eventualmente,

²⁶⁸ (Estaño & Tolama, 2017)

²⁶⁹ (Comisiones Unidas de Hacienda y Crédito Público, de Ciencia y Tecnología y de Estudios Legislativos, 2017, p. 2)

²⁷⁰ (Comisiones Unidas de Hacienda y Crédito Público, de Ciencia y Tecnología y de Estudios Legislativos, 2017, p. 2)

se aprobó el proyecto de decreto el 5 de diciembre de 2017 con 107 votos a favor en el Pleno. En seguida, los documentos fueron remitidos a la Cámara de Diputados el 7 de diciembre de 2017. De esta manera, el dictamen correspondiente fue discutido en la Cámara Baja y fue aprobado con 286 votos a favor, 3 en contra y 63 abstenciones. Finalmente, la ley fue publicada en el DOF el 9 de marzo de 2018.

A través de esta iniciativa no sólo se proponía la creación de una nueva ley llamada Ley para Regular las Instituciones de Tecnología Financiera, sino que se propugnaba por diversas reformas en múltiples ordenamientos existentes. El documento contenía modificaciones a: la Ley de Instituciones de Crédito (“LIC”), la Ley del Mercado de Valores (“LMV”) la Ley General de Organizaciones y Actividades Auxiliares del Crédito (“LGOAAC”), la Ley para la Transparencia y Ordenamiento de los Servicios Financieros (“LTOSF”), la Ley para Regular las Sociedades de Información Crediticia (“LRSIC”), la Ley de Protección y Defensa al Usuario de Servicios Financieros (“LPDUSF”), la Ley para Regular las Agrupaciones Financieras (“LRAF”), la Ley de la Comisión Nacional Bancaria y de Valores (“Ley de la CNBV”) y la Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita (“LFPIORPI” o “Ley para prevenir el Lavado de Dinero”). Algunas de estas modificaciones afectan de manera directa la operación con activos virtuales, si bien no se encuentran en la LRITF como tal. En el siguiente capítulo se analizarán dichas reformas y, en su caso, su incidencia en el objeto del trabajo.

VI.3. Marco Jurídico Reformado

Previo al estudio de la LRITF, es vital examinar las modificaciones hechas al marco jurídico existente, ya que en algunas de estas modificaciones se encuentran disposiciones claves para la operación de activos virtuales por parte de una ITF²⁷¹. Es importante establecer que el resumen de las reformas presentado a continuación no es exhaustivo y que no tiene por objetivo serlo, sino que busca tocar los puntos más relevantes para el tema de la tesis.

Una vez establecida la anterior reserva, la primera ley alterada que objeto de estudio es la LIC, en la cual se reformaron los artículos 48 Bis 5, sexto párrafo; 52, primer y octavo párrafo; 57, octavo párrafo y 72 Bis, quinto párrafo, y se adicionan los artículos 103, fracción VII; 112 Sextus y 112 Séptimus. Por medio de estas modificaciones, se establece en la ley que las actividades de las ITF no se considerarán como captación directa o indirecta de acuerdo y por lo tanto no entran en la prohibición del artículo 103 de la LIC.

A la par, se modificó la LMV en su artículo 1, fracciones II y VI, y se adicionó el artículo 277 Bis 1. Lo anterior para retirar de la competencia de la CNBV la posibilidad de regular la oferta e intermediación de valores, tratándose de títulos ofrecidos a través de las ITF, al igual que los sistemas de negociación de dichos valores que permitan la realización de operaciones de estos, siempre y cuando estén administrados por una ITF. Paralelamente, fue adicionado el artículo 227 Bis 1, modernizando los servicios de asesoría de inversiones, en materia de asesoría automatizada y gestiones de inversión.

²⁷¹ Las reformas mencionadas pueden ser verificadas en la publicación del DOF de fecha: 09/03/2018 - Edición Matutina, Primera Sección, Poder Ejecutivo, SHCP. Decreto por el que se expide la Ley para Regular las Instituciones de Tecnología Financiera y se reforman y adicionan diversas disposiciones de la Ley de Instituciones de Crédito, de la Ley del Mercado de Valores, de la Ley General de Organizaciones y Actividades Auxiliares del Crédito, de la Ley para la Transparencia y Ordenamiento de los Servicios Financieros, de la Ley para Regular las Sociedades de Información Crediticia, de la Ley de Protección y Defensa al Usuario de Servicios Financieros, de la Ley para Regular las Agrupaciones Financieras, de la Ley de la Comisión Nacional Bancaria y de Valores y, de la Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita.

Del mismo modo, se alteró la LGOAAC en sus artículos 57, párrafo sexto y 81-A Bis, párrafo primero, y se adicionó el artículo 81-A Bis, en sus párrafos tercero, cuarto y quinto, recorriéndose los subsecuentes en su orden. En virtud de lo anterior, se dotó a la CNBV de facultades para realizar visitas de inspección y vigilancia en centros cambiarios, transmisores de dinero y sociedades financieras de objeto múltiple no reguladas. Conjuntamente, se obliga a los transmisores de dinero a constituir una ITF cuando “pretendan emitir fondos de pago electrónico o instrumentos de pago que almacenen fondos de pago electrónico, además de verificar que sus agentes relacionados y los terceros con los que contraten cumplan con las disposiciones relativas a la prevención de lavado de dinero con la finalidad de crear mayor transparencia.”²⁷²

De manera similar, se reformó la LTOSF en sus artículos 3º, fracciones V Bis, IX, XII, párrafo primero, XIII y XIV; 6º, párrafo primero; 18 Bis, fracción II, párrafo segundo; 43, primer párrafo; 44, segundo párrafo, fracción II y 49 Bis 2, párrafo primero, así como la denominación de la Sección VIII del Capítulo V. Adicionalmente, se adicionaron a los artículos 2º, la fracción III Bis; al 3º, las fracciones IV Bis, V Ter, XI Bis, XI Ter, XII, párrafo tercero; y al 49 Bis 2, el párrafo tercero. Por medio de estas reformas se cambió la definición de “Medio de Disposición” para que se entienda como uno de ellos las actividades realizadas por una ITF, imponiendo la obligación a las ITF de registrar sus comisiones ante el Banco de México. Adicionalmente, se facultó a la CNBV para sancionar a los “Participantes en Redes”.

En el mismo paquete se incluyó la reforma a la LRSIC en sus artículos 2º., fracción V, y 28, párrafo primero, incluyendo a las ITF dentro de la definición de “Entidad Financiera” (“EF”). Asimismo, se modernizó la forma de recabar el consentimiento de los Clientes de los Usuarios de una Sociedad de Información Crediticia mediante

²⁷² (Comisiones Unidas de Hacienda y Crédito Público, de Ciencia y Tecnología y de Estudios Legislativos, 2017, p. 7)

el uso de la firma electrónica permitiendo que una sociedad de información crediticia pueda proveer su información a los Usuarios.

Igualmente, se alteró la LPDUSF, para que incluyera a las ITF en la definición de “Institución Financiera”, contenida en el artículo 2º, fracción IV. Además, se adicionó un párrafo en lugar del cuarto al artículo 50 Bis, recorriéndose el párrafo subsecuente. Otra de las modificaciones consiste en no imponerles a las ITF la obligación de tener oficinas o sucursales para la atención de sus clientes dada su naturaleza y vocación digital. Exclusivamente “deberán señalar los datos de contacto de su Unidad Especializada en un lugar visible y de fácil acceso al público general en el medio electrónico que utilicen para ofrecer sus servicios”²⁷³.

Por otra parte, se reformó la LRAF en sus artículos 3º, párrafo primero, y 12, párrafo primero. A través del primer artículo se permitió que las ITF sean parte de grupos financieros y se añadió una prohibición a que las ITF que formen parte de un grupo financiero puedan tener un nombre similar al de los otros miembros del grupo, con el objetivo de que el público no se confunda acerca de los mecanismos de protección con los que cuenta cada una de las instituciones. Asimismo, se cambió la Ley de la CNBV en su artículo 3º, fracción IV, inciso a) para que también incluya dentro de la definición de una EF a las ITF.

Por último, pero no menos importante, se alteró la LFPIORPI en su artículo 3º, fracción VI y 15, fracción I, y se adicionó la fracción XVI al artículo 17. De manera semejante a otras leyes, se introdujo a las ITF dentro de la definición de una EF. Además, se añadió la obligación de las ITF de establecer medidas y procedimientos para prevenir y detectar actos, omisiones u operaciones que pudieran ubicarse en los supuestos previstos en diversos ordenamientos señalados en la ley, así como identificar usuarios y clientes de conformidad con lo establecido en el artículo 58 de la LRITF, que hace referencia a disposiciones de carácter general aún no emitidas.

²⁷³ Ley de Protección y Defensa al Usuario de Servicios Financieros, Artículo 50 Bis, párrafo cuarto.

De igual manera, se instituye como actividad vulnerable, y por lo tanto sujeto a identificación, el ofrecimiento habitual y profesional de intercambio de activos virtuales por parte de sujetos distintos a las EF. Por otro lado, el ordenamiento también clasifica como actividad vulnerable el proveer medios para custodiar, almacenar, o transferir activos virtuales distintos a los reconocidos por el Banco de México en términos de la LRITF, si es que este servicio es prestado por una persona diferente a una EF.

Es decir, si una entidad no registrada como ITF de manera habitual y profesional administra u opera, facilita o realiza operaciones de compra o venta activos virtuales propiedad de sus clientes o provee medios para custodiar, almacenar, o transferir activos virtuales distintos a los reconocidos por Banxico, estará realizando una actividad vulnerable y, por lo tanto, sujeta a identificación en términos del artículo 18 de la LFPIORPI. Dada la enorme importancia del artículo se transcribe a continuación para ser analizado a más detalle:

Artículo 17. Para efectos de esta Ley se entenderán Actividades Vulnerables y, por tanto, objeto de identificación en términos del artículo siguiente, las que a continuación se enlistan:

I. a **XV.** [...]

XVI. El ofrecimiento habitual y profesional de intercambio de activos virtuales por parte de sujetos distintos a las Entidades Financieras, que se lleven a cabo a través de plataformas electrónicas, digitales o similares, que administren u operen, facilitando o realizando operaciones de compra o venta de dichos activos propiedad de sus clientes o bien, provean medios para custodiar, almacenar, o transferir activos virtuales distintos a los reconocidos por el Banco de México en términos de la Ley para Regular las Instituciones de Tecnología Financiera. Se entenderá como activo virtual toda representación de valor registrada electrónicamente y utilizada entre el público como medio de pago para todo tipo de actos jurídicos y cuya transferencia únicamente puede

llevarse a cabo a través de medios electrónicos. En ningún caso se entenderá como activo virtual la moneda de curso legal en territorio nacional, las divisas ni cualquier otro activo denominado en moneda de curso legal o divisas.

Serán objeto de Aviso ante la Secretaría cuando el monto de la operación de compra o venta que realice cada cliente de quien realice la actividad vulnerable a que se refiere esta fracción sea por una cantidad igual o superior al equivalente a seiscientos cuarenta y cinco Unidades de Medida y Actualización.

En el evento de que el Banco de México reconozca en términos de la Ley para Regular las Instituciones de Tecnología Financiera activos virtuales, las personas que provean los medios a que se refiere esta fracción, deberán obtener las autorizaciones correspondientes en los plazos que señale dicho Banco de México en las disposiciones respectivas.

[...]

[...]

Este artículo plantea serias interrogantes concernientes a su aplicación que pueden, y deben, ser contestadas en la regulación secundaria. Una de las dudas más preocupantes es la que surge con relación a los desarrolladores que conciban una cartera o *wallet* de activos virtuales. Es necesario recordar que las carteras o *wallets* en el contexto de activos virtuales no son equivalentes a las carteras de *e-money*. Retomando la definición de A. Antonopoulos “[las carteras en el contexto de bitcoin] Se tratan de aplicaciones que sirven como la interfaz de usuario primaria, controlando el acceso a los activos de un usuario²⁷⁴, manejando las llaves y

²⁷⁴ Si bien no los almacena, ya que las carteras de activos virtuales no “almacenan” valor si no que manejan las llaves que permiten verificar que es el usuario el que envía la transacción.

dirección de este, verificando el “balance” y creando y firmando transacciones utilizando las respectivas llaves privadas”²⁷⁵. En el caso de Ethereum las carteras cumplen con aún más funciones, ya que a través de ellas se pueden programar Contratos Inteligentes, y por lo tanto *dApps*. Por lo tanto, se reitera que una cartera en el entorno de los activos virtuales no debe de considerarse análoga a una *wallet* de *e-money*.

De lo anterior, se desprende la afirmación de que el artículo transcrito con anterioridad regula de una manera equivocada a quienes provean los medios (de manera profesional y habitual) para custodiar, almacenar, o transferir activos virtuales distintos a los reconocidos por la ley. Podría darse el caso, si ether no es “reconocido” por el Banco de México, que un desarrollador que lance al mercado una nueva “cartera”, la cual permita programar Contratos que corran en la cadena de Ethereum sería responsable de reportar operaciones²⁷⁶ que superen el umbral establecido, dado que para activar un Contrato se necesita “transferir” ether a la cuenta del Contrato para activarlo o por mantener ether en la aplicación. La norma podría llegar al extremo de aplicar a fabricantes de *wallets* hardware, que proveen los medios al usuario para “almacenar” sus activos virtuales de manera “profesional”. De ahí que la prohibición pareciera ser completamente desproporcionada y en detrimento de la innovación.

Avanzando en el análisis, se presenta un segundo problema. La ley sólo establece un límite a las operaciones de compra o venta, y no indica cuál será el límite cuando se trate de almacenamiento, transferencia o custodia, por lo que hay una laguna al respecto. Aún más, la obligación de informar de ciertas operaciones que superen un determinado umbral hace retomar la controversia respecto a la determinación del precio del activo con fines de dar cumplimiento a la obligación que fue comentada en capítulos anteriores. Además, otro punto en el que la ley no es clara es si el supuesto de actividad vulnerable aplica únicamente a la “facilitación o realización de operaciones de compra o venta” por parte de entidades no financieras

²⁷⁵ (Antonopoulos, 2017, p. 145)

²⁷⁶ Esta asunción es contingente a la emisión de la regulación secundaria

cuando se traten de activos virtuales no “reconocidos” por el Banco de México o si el supuesto también incluye a operaciones con activos virtuales reconocidos por parte de entidades de la misma naturaleza.

Por último, en una nota positiva, la norma autoriza de manera tácita una manera diferente de operar un intercambio no contenida en la LRITF. De acuerdo con el artículo, hay dos maneras de operar con activos virtuales, dejando a un lado las operaciones entre privados, una reglamentada en la LRITF y otra contenida en el artículo, que, si bien impone la carga regulatoria de reportar una actividad considerada como vulnerable, podría permitir las actividades de un bróker.

Se debe reiterar que los inconvenientes que se señalan en la anterior ley están sujetos a ser modificados, de manera positiva o negativa, por medio de las disposiciones de carácter general. Los plazos para la emisión de dichas reglas varían conforme a la institución que las emite y el tema que regulen. No obstante, de acuerdo a las disposiciones transitorias de la LRITF los plazos son conocidos y son presentados a continuación, acomodados en un cuadro para una más fácil comprensión:

Autoridad Responsable	Artículos que mencionan las disposiciones generales por ser emitidas	Plazo
SHCP	Artículo 58	Seis meses
	Artículo 82, fracción VI	Doce Meses
CNBV	Artículos 18, fracción I; 36, fracción IV; 39, fracciones VI, XI, XII y XVI; 44; 45; 48, primer párrafo, para las reglas relacionadas con contabilidad y plan de continuidad de negocio;	Seis Meses
	Artículos 18, fracción IV; 54; 56, segundo párrafo; 57; 73; 82, fracción VI; 89, fracción IV y 116	Doce Meses
	Artículos 55 y 76	Veinticuatro Meses
CONDUSEF ²⁷⁷	Artículos 57 y 82, fracción VI	Doce Meses
CONSAR ²⁷⁸ y CNSF ²⁷⁹	Artículos 82, fracción VI y 116	Doce Meses
	Artículo 76	Veinticuatro Meses
Banco de México	Artículos 26 y 44	Seis Meses
	Artículos 30; 32; 46; 57; 82, fracción VI y 116	Doce Meses

²⁷⁷ Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros

²⁷⁸ Comisión Nacional del Sistema de Ahorro para el Retiro

²⁷⁹ Comisión Nacional de Seguros y Fianzas

	Artículo 76	Veinticuatro Meses
CNBV y Banxico	Artículos 48, 54, 56, segundo párrafo y el convenio previsto en el artículo 71	Doce Meses ²⁸⁰

A menos de que se especifique lo contrario, los plazos corren a partir de la entrada en vigor de la ley.

²⁸⁰ No se especifica a partir de que fecha

Por último, se muestra una tabla condensada que presenta todas las modificaciones a regulaciones existentes como consecuencia de la entrada en vigor de la LRITF.

Ley Reformada	Artículo(s) Modificado(s)	Artículo(s) Adicionado(s)	Sentido de la Modificación²⁸¹
Ley de Instituciones de Crédito	<ul style="list-style-type: none"> • 48 bis 5, 6º p. • 52, 1º y 8º p. • 57, 8º p. • 72 bis, 5º p. 	<ul style="list-style-type: none"> • 103, fracc. VII • 112 Sex • 112 Sép 	<p>1) Establecer una excepción para que las actividades realizadas por o a través de las ITF no se consideren como captación directa o indirecta conforme a ese ordenamiento; y</p> <p>2) Permitir la comunicación a través de medios electrónicos autorizando el uso de la firma electrónica para expresar conformidad.</p>
Ley del Mercado de Valores	<ul style="list-style-type: none"> • 1, fracc. II y VI 	<ul style="list-style-type: none"> • 277 bis 1 	<p>1) Precisar que la oferta e intermediación de los títulos emitidos por las ITF serán regulados por la LRITF y no por la LMV, al igual que los sistemas de negociación de valores relacionados con la operación de estos; y</p> <p>2) Modernizar el funcionamiento de los asesores en inversiones respecto a los servicios automatizados de asesoría y gestión de inversión.</p>
Ley General de Organizaciones y Actividades Auxiliares del Crédito	<ul style="list-style-type: none"> • 57, 6º p. • 81-A Bis 1º p. 	<ul style="list-style-type: none"> • 81-A Bis, 3º, 4º y 5º p. 	<p>1) Dotar de facultades expresas a la CNBV de regular la información que pueda requerir en ejercicio de sus funciones de vigilancia tratándose de centros cambiarios, transmisores de dinero y sociedades financieras de objeto múltiple no reguladas con la finalidad de evitar impugnaciones; y</p>

²⁸¹ De acuerdo con el respectivo dictamen de las Comisiones Unidas de Hacienda y Crédito Público, de Ciencia y Tecnología y de Estudios Legislativos (Comisiones Unidas de Hacienda y Crédito Público, de Ciencia y Tecnología y de Estudios Legislativos, 2017, p. 7)

			2) Obligar a los transmisores de dinero a constituir una ITF cuando pretendan emitir fondos de pago electrónico o instrumentos de pago que almacenen fondos de pago electrónico, además de verificar que sus agentes relacionados y los terceros con los que contraten cumplan con las disposiciones relativas a la prevención de lavado de dinero con la finalidad de crear mayor transparencia.
Ley para la Transparencia y Ordenamiento de los Servicios Financieros	<ul style="list-style-type: none"> • 3, fracc V Bis, IX, XII, p. 1º, XIII y XIV • 6 p. 1º • 18 bis, fracc. II, p. 2º 	<ul style="list-style-type: none"> • 2, fracc III Bis • 3, fracc. IV Bis, V Ter, XI Bis, XI Ter, XII p. 3º • 49 bis 2, p. 2º 	<p>1) Modificar la definición de Medios de Disposición para comprender en esta a las actividades de las ITF;</p> <p>2) Incluir a las ITF en el registro de cobro de comisiones del Banco de México como medida de protección en favor de sus usuarios; y</p> <p>3) Dotar de facultades a la CNBV para sancionar a los Participantes en Redes.</p>
Ley para Regular las Sociedades de Información Crediticia	<ul style="list-style-type: none"> • 2, fracc V • 28 p. 1º 		<p>1) Incluir a las ITF en la definición de “Entidad Financiera”; y</p> <p>2) Modernizar la forma en que las Sociedades de Información Crediticia recaban la autorización expresa del cliente debido a la operación natural de las ITF.</p>
Ley de Protección y Defensa al Usuario de Servicios Financieros	<ul style="list-style-type: none"> • 2, fracc. IV p. 4º 	<ul style="list-style-type: none"> • 50, p. 4º 	<p>1) Incluir a las ITF en la definición de “Institución Financiera”; y</p> <p>2) Establecer una excepción en favor de las ITF con relación a la obligación de contar con sucursales u oficinas para atender consultas y reclamaciones de sus clientes conforme a ese</p>

			ordenamiento debido a que, por la forma de operar de estas plataformas, no cuentan normalmente con oficinas para dar cumplimiento a esa disposición.
Ley para Regular las Agrupaciones Financieras	<ul style="list-style-type: none"> • 3 p.1º • 12 p. 1º 		<p>1) Permitir que las ITF puedan formar parte de Grupos Financieros; y</p> <p>2) Establecer la prohibición expresa para que las ITF no puedan utilizar denominaciones iguales o semejantes a las de otras entidades financieras aún y cuando sean integrantes del mismo Grupo Financiero, con la finalidad de evitar confusiones en el público sobre los mecanismos de protección con los que sí cuentan otras entidades financieras.</p>
Ley de la Comisión Nacional Bancaria y de Valores	<ul style="list-style-type: none"> • 3, fracc IV, inciso a) 		<p>1) Incluir a las ITF en la definición de “Entidad Financiera”.</p>
Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita	<ul style="list-style-type: none"> • 3 fracc. VI • 15 fracc. I 	<ul style="list-style-type: none"> • 17, Fracc. XVI 	<p>1) Añadir como actividad vulnerable el ofrecimiento habitual y profesional de intercambio de activos virtuales por parte de entidades distintas a las autorizadas en la Ley para Regular las Instituciones de Tecnología Financiera.</p>

VI.4. Ley para Regular las Instituciones de Tecnología Financiera

El objetivo del presente apartado es estudiar a detalle los artículos relacionados con los activos virtuales de la LRITF, con la intención de hacer un análisis a detalle de estos. La examinación tiene la intención tanto de evaluar la ley por separado como de compararla con otras experiencias internacionales en la materia. Asimismo, se tomará en cuenta lo dicho en los capítulos II y III para, en los casos que sea necesario, considerar si el marco jurídico es adecuado o no lo es.

La LRITF fue redactada con los principios de inclusión²⁸² e innovación financiera, protección al consumidor, preservación de la estabilidad financiera, promoción de la sana competencia, neutralidad tecnológica, prevención de lavado de dinero y de financiamiento al terrorismo²⁸³ como ejes rectores de la misma. A su vez, la ley tiene por objeto regular los servicios financieros que prestarán las Instituciones de Tecnología Financiera. En consecuencia, la legislación contempla la figura de las ITF, que pueden organizarse y operar bajo la denominación de Instituciones de Financiamiento Colectivo o Instituciones de Fondos de Pago Electrónico.

De igual manera, en la ley se permite el uso de un esquema llamado Modelo Novedoso el cual es un espacio jurídico tipo “*sandbox*”, que permite cierta libertad regulatoria, y al que se pueden acoger personas morales que tengan una propuesta innovadora cuya ejecución requiera de autorización, registro o concesión, permitiendo la experimentación. Esta autorización será otorgada con limitantes en cuanto a número de clientes y tiempo de operación, entre otros. El beneplácito para operar bajo un esquema *sandbox* podrá otorgarse a entes previamente supervisados (como instituciones de crédito) o a cualquier sujeto, con cada permiso teniendo características disímiles. Asimismo, la legislación contempla la operación

²⁸² Curiosamente, a pesar de que busca bancarizar a la población, para poder operar con una ITF es requisito contar con una cuenta bancaria, salvo contadas excepciones.

²⁸³ (Comisiones Unidas de Hacienda y Crédito Público, de Ciencia y Tecnología y de Estudios Legislativos, 2017) ver en línea en: http://www.senado.gob.mx/sgsp/gaceta/63/3/2017-12-05-1/assets/documentos/Dict_Hacienda_Ley_Fintech.pdf

con activos virtuales por parte de Instituciones de Crédito e ITF, sujetando la misma a las disposiciones de carácter general emitidas por Banxico.

Por otro lado, es importante recalcar que la ley tiene como objetivo establecer un marco regulatorio, planteando bases y mínimos, en el entendido que la regulación más detallada será emitida con posterioridad por diferentes órganos de acuerdo a las fechas que marca la misma ley. No obstante, que una gran parte de la reglamentación del sector se encuentre en disposiciones de carácter general puede considerarse como una ventaja, ya que permite mucha mayor flexibilidad para adaptarse al constante cambio al que está sujeta la industria²⁸⁴. Empero, lo anterior puede ser un arma de dos filos, dado que existe el riesgo de provocar cierto grado de incertidumbre regulatoria al dejar la puerta abierta a la constante modificación de las disposiciones de carácter general.

²⁸⁴ (Comisiones Unidas de Hacienda y Crédito Público, de Ciencia y Tecnología y de Estudios Legislativos, 2017, p. 3)

VI.4.1. Instituciones de Financiamiento Colectivo

La LRITF regula dos tipos de ITF: las Instituciones de Financiamiento Colectivo (“IFC”) y las Instituciones de Fondos de Pago Electrónico (“IFPE”). En este capítulo serán abordadas las primeras y en el subsiguiente las segundas. La reglamentación de las IFC se encuentra primordialmente en el Capítulo I de la Ley titulado “De las Instituciones de Financiamiento Colectivo” del Título II “De las ITF y sus Operaciones”. Sus funciones fundamentales son definidas en los artículos 15 y 16 de la ley, que a la letra indican:

Artículo 15.- Las actividades destinadas a poner en contacto a personas del público en general, con el fin de que entre ellas se otorguen financiamientos mediante alguna de las Operaciones señaladas en el siguiente artículo, realizadas de manera habitual y profesional, a través de aplicaciones informáticas, interfaces, páginas de internet o cualquier otro medio de comunicación electrónica o digital, solo podrán llevarse a cabo por las personas morales autorizadas por la CNBV, previo acuerdo del Comité Interinstitucional, como instituciones de financiamiento colectivo.

Artículo 16.- Los Clientes de una institución de financiamiento colectivo que intervengan en las actividades previstas en el artículo anterior serán denominados inversionistas y solicitantes. Se consideran inversionistas a las personas físicas o morales que aporten recursos a los solicitantes. Se consideran solicitantes a las personas físicas o morales que hubieren requerido tales recursos a través de la institución de financiamiento colectivo.

Los Clientes de una institución de financiamiento colectivo podrán efectuar entre ellos y a través de dicha institución las Operaciones siguientes:

I. Financiamiento colectivo de deuda, con el fin de que los inversionistas otorguen préstamos, créditos, mutuos o cualquier otro financiamiento causante de un pasivo directo o contingente a los solicitantes;

II. Financiamiento colectivo de capital, con el fin de que los inversionistas compren o adquieran títulos representativos del capital social de personas morales que actúen como solicitantes, y

III. Financiamiento colectivo de copropiedad o regalías, con el fin de que los inversionistas y solicitantes celebren entre ellos asociaciones en participación o cualquier otro tipo de convenio por el cual el inversionista adquiera una parte alícuota o participación en un bien presente o futuro o en los ingresos, utilidades, regalías o pérdidas que se obtengan de la realización de una o más actividades o de los proyectos de un solicitante.

Los actos jurídicos que se realicen para la celebración de las Operaciones a que se refiere este artículo se reputarán actos de comercio.

Las Operaciones a que se refiere este artículo se denominarán en moneda nacional. Asimismo, las instituciones de financiamiento colectivo podrán realizar las referidas Operaciones en moneda extranjera o con activos virtuales, en los casos y sujeto a los términos y condiciones que el Banco de México establezca mediante disposiciones de carácter general que para tal efecto emita.

Los títulos que se ofrezcan a través de estas instituciones no podrán estar inscritos en el Registro Nacional de Valores.

Asimismo, las instituciones de financiamiento colectivo podrán realizar aquellas actividades para facilitar la venta o adquisición de los derechos o títulos intercambiados que documenten las Operaciones referidas en las fracciones I a III de este artículo. La CNBV, con el objeto de proteger a los inversionistas, establecerá disposiciones de carácter general para tal efecto.

Como se desprende de los artículos anteriores, estas instituciones brindan servicios de financiamiento no convencionales a través de medios electrónicos. Este tipo de instituciones funcionan como una especie de intermediario (o bróker de información) que utilizando métodos digitales pone en contacto a personas con recursos cuyo interés es invertir en proyectos de individuos que a su vez requieren capital. Los clientes de una institución de este tipo pueden denominarse inversionistas y/o solicitantes. Los primeros son aquellos que aportan recursos para que el proyecto de los segundos sea financiado. En ambos casos, los sujetos pueden ser personas físicas o morales. Su funcionamiento se autoriza mediante acuerdo del Comité Interinstitucional, una “instancia colegiada integrada por servidores públicos de la SHCP, de Banxico y de la CNBV”²⁸⁵.

Las actividades que podrán efectuar son las establecidas en las fracciones I a III del artículo 16. La fracción primera alude al financiamiento colectivo de deuda, que se traduce en cualquier tipo de operación financiera causante de pasivo directo o contingente a los solicitantes. La fracción segunda menciona el financiamiento colectivo de capital, conocido en inglés como “*equity crowdfunding*” mediante este mecanismo, los inversionistas adquieren títulos representativos de capital del solicitante a cambio de una aportación de capital. Por último, la fracción tercera alude al financiamiento colectivo de copropiedad o regalías por medio del cual un inversionista puede hacerse acreedor a una parte alícuota o participación en un bien presente o futuro o en los ingresos, utilidades, regalías o pérdidas que se obtengan de la realización de una o unas determinadas actividades por el solicitante. Las

²⁸⁵ Artículo 4, fracción VI de la LRITF

anteriores operaciones se podrán verificar en moneda nacional o activos virtuales, sujeto a disposiciones generales emitidas por Banxico con posterioridad.

Para la realización de estas actividades, las IFC están autorizadas para emitir títulos representativos. Estos títulos no tendrán que estar inscritos en el Registro Nacional de Valores (“RNV”) establecido en el artículo 2 de la LMV, fracción XXI. De igual manera, estos títulos no se registrarán por lo establecido en la LMV en virtud de su artículo 1º, fracción segunda, que establece:

Artículo 1.- La presente Ley es de orden público y observancia general en los Estados Unidos Mexicanos y tiene por objeto desarrollar el mercado de valores en forma equitativa, eficiente y transparente; proteger los intereses del público inversionista; minimizar el riesgo sistémico; fomentar una sana competencia, y regular lo siguiente:

[...]

II. La oferta e intermediación de valores, salvo tratándose de títulos ofrecidos a través de las instituciones de tecnología financiera”

[...]

Sin embargo, los títulos si están sujetos a las disposiciones de carácter general que pueda publicar la CNBV. Además de emitirlos, las instituciones están autorizadas para realizar “aquellas actividades para facilitar la venta o adquisición de los derechos o títulos intercambiados que documenten las Operaciones referidas en las fracciones I a III de este artículo”. Lo cual también es plasmado en la fracción sexta del artículo 1º de la LMV que autoriza la operación de la siguiente manera:

(...)

VI. El desarrollo de sistemas de negociación de valores que permitan la realización de operaciones con estos, salvo tratándose de los sistemas ofrecidos a través de las instituciones de tecnología financiera.

(...)

Dicho lo anterior, los artículos precedentes son de suma importancia dada la autorización que contiene el artículo 16 de realizar las operaciones referidas con anterioridad con activos virtuales²⁸⁶. Teniendo en cuenta lo permitido por las fracciones del multicitado artículo bien se podría estar frente un par de artículos profundamente significativos para el desarrollo de eventos generados de activos virtuales, como lo es un *ICO*. Para clarificar, un *ICO* se lleva a cabo, en la mayoría de las ocasiones, con la principal finalidad de recaudar fondos para un determinado proyecto. Originalmente estaban asociados casi exclusivamente con proyectos vinculados con la tecnología *blockchain*, pero con el tiempo esta relación se ha ido desvaneciendo. Una institución creada bajo la modalidad de IFC permitiría el surgimiento y mantenimiento de una plataforma a través de la cual se fondeen proyectos mediante *ICOs*. Los *tokens* generados a través de un fondeo de este estilo podrían ser *security tokens*, que representen capital o deuda, o *utility tokens*, encuadrados en el tipo de actividad permitida en la fracción tercera.

Hay que mencionar además que se podría caminar hacia una *tokenización* de la economía ya que nada impide que cualquier título, ya sea de deuda o representativo de capital social, sea representado por un *token* para “facilitar su venta o adquisición” tal como lo refiere el mismo artículo 16 en su último párrafo. Mas aún, los posibles títulos o derechos generados a partir de estos financiamientos no serían regulados por la LMV sino por la nueva LRITF, mucho mejor equipada para lidiar con las situaciones que puedan surgir derivado de un evento generador de *tokens*.

Sin embargo, existe un inconveniente si se decidieran emitir activos virtuales en un esquema como el descrito con anterioridad. El Banco de México tiene la facultad de “reconocer” (autorizar) los activos virtuales con los que puede operar una ITF, por lo tanto, sería necesario que “reconociera” los *tokens* producto de un *ICO* realizado por una IFC para que se pudiera operar con ellos, posiblemente asfixiando al sector.

²⁸⁶ En los casos y sujeto a los términos y condiciones que el Banco de México establezca mediante disposiciones de carácter general que para tal efecto emita.

No obstante, las posibilidades son ilimitadas si se aplican las disposiciones de manera creativa y es explotado el enorme potencial que presentan este par de artículos.

En resumidas cuentas, a pesar de que pudiese no ser la intención del legislador, estos artículos podrían ser la base del surgimiento de una prolífica industria de *ICOs* en territorio mexicano, una regulación que, aunque contingente a lo que establezcan con posterioridad las disposiciones de carácter general, es, hasta cierto punto, única en el mundo. En caso de que efectivamente se trate de lo que se piensa, la manera en la que se resuelve el acercamiento a los *ICOs* es sumamente superior a la manera tan incierta en la que se están aplicando las normas de valores tradicionales en los EE. UU. Es razonable llegar a la conclusión que ciertos *tokens* se comportan de manera casi idéntica a valores y por lo tanto deben de ser regulados de manera similar. Empero, la manera en la cual lo hace la SEC crea una gran incertidumbre en el mercado. Las acciones para hacer cumplir la ley no son plenamente explicadas y tal parece que se quiere cuasi legislar sobre la marcha, sin que sea completamente claro en que ocasiones un token pre o post producto será considerado o no como un valor.

En contraste, y contingente a los que diga la regulación secundaria, México estaría a la delantera al crear un espacio reglamentario mucho más amigable al cripto-espacio. Incluso, se podría hablar de una mejor norma que la aplicada en la jurisdicción suiza, que impone a ciertos emisores de tokens obligaciones similares a las de un emisor de valores tradicional.

Por otra parte, su aplicación al espacio de los *ICOs* genera ciertas incógnitas, como la cuestión relacionada con la negociación de los *tokens* emitidos como respaldo de una contribución de un determinado proyecto. ¿Estos podrán ser negociados únicamente en la plataforma de la institución que fungió como intermediaria para la realización del fondeo? o ¿Se crearía un prolífico mercado secundario? Una lectura del último párrafo del artículo 16 hace que la balanza se incline por la segunda opción, dado que la ley explícitamente menciona que las IFC podrán realizar aquellas actividades para facilitar la venta o adquisición de los derechos o títulos

intercambiados que documenten las operaciones referidas en las fracciones I a III del propio artículo, hace mención de todas las operaciones, no únicamente las realizadas a través de su plataforma. Podría ser que en un futuro existan IFC cuyo único objeto sea mantener un intercambio de *tokens* generados a partir de fondeo de algún proyecto.

Paralelamente, el artículo 19 es destacable ya que también se refiere a otro tipo de actividades que tienen autorizadas las IFC. Sobre todo, al mencionar actividades conexas estrictamente necesarias para la operación de un negocio, como la solicitud de préstamos, o la adquisición de bienes muebles e inmuebles necesarios para la realización de sus actividades, empero, en su fracción tercera expresa una posibilidad que dándole una adecuada interpretación pudiese ser relevante:

Artículo 19.- Las instituciones de financiamiento colectivo, además de las actividades que le son propias, podrán llevar a cabo únicamente las siguientes:

[...]

III. Habilitar y permitir el uso de canales de comunicación electrónicos mediante los cuales los inversionistas y solicitantes puedan relacionarse a través de la interfaz, página de internet o medio de comunicación electrónica o digital que utilice para realizar sus actividades;

[...]

De nuevo parece que la fracción está autorizando la creación de un “canal de comunicación” en la cual se puedan comunicar inversionistas y solicitantes. Lo más probable es que la intención del legislador fuera permitir la creación de una especie de página web o aplicación para comunicación entre todas las partes involucradas. Pero utilizando esta afirmación como sustento se podría perfectamente justificar la creación de un intercambio descentralizado para *tokens* eventualmente emitidos a través de un *ICO* realizada a través de una o varias IFC. Aunque bien esta

posibilidad es poco probable ya que muy seguramente se refiere a una especie de chat de soporte para los usuarios de la plataforma.

Por otro lado, un punto que podría ser utilizado para defensa de la postura contraria, es el párrafo segundo de la fracción primera del artículo 18, que prohíbe ofertar proyectos que están siendo ofertados en ese mismo momento en otra IFC. La interpretación de este artículo podría parecer que se presta a que un proyecto únicamente pueda ser ofertado en un IFC a la vez, pero el espíritu de la disposición se antoja otro. La prohibición parece referirse a que esta limitante únicamente aplica mientras se da el fondeo del proyecto, sin embargo, no habla sobre la comercialización de títulos o derechos que se emitan derivados de ese fondeo.

Hay que mencionar, además que, aunque la legislación mexicana no impone obligaciones relacionadas con emisoras de valores tradicionales a las IFC, estas si que cuentan con cargas que deben de cumplir, señaladas en el artículo 18. Entre estas destacan: obligaciones de dar a conocer información exhaustiva a los inversionistas, incluyendo el criterio de selección de los proyectos, información acerca del desarrollo del proyecto, entre otros. Es decir, la cargas que se le imponen a la plataforma son similares a las de una emisora de valores o deuda, pero mucho menos gravosas.

Por todo lo mencionado con anterioridad, es posible que se esté frente a una regulación que, debidamente utilizada por todos los participantes del mercado, podría ser única en el mundo y profundamente revolucionaria, si bien su aplicación está sujeta a lo que con posterioridad dicten las autoridades en normas secundarias.

VI.4.2. Instituciones de Fondos de Pago Electrónico

La LRITF en su Título II “De las ITF y sus Operaciones”, Capítulo II “De las Instituciones de Fondos de Pago Electrónico”, regula a las Instituciones de Fondos de Pago Electrónico (“IFPE”). Su reglamentación inicia en los artículos 22, 23 y 24. El primero de ellos define a una IFPE de la siguiente manera:

Artículo 22.- Los servicios realizados con el público de manera habitual y profesional, consistentes en la emisión, administración, redención y transmisión de fondos de pago electrónico, por medio de los actos que a continuación se señalan, a través de aplicaciones informáticas, interfaces, páginas de internet o cualquier otro medio de comunicación electrónica o digital, solo podrán prestarse por las personas morales autorizadas por la CNBV, previo acuerdo del Comité Interinstitucional, como instituciones de fondos de pago electrónico:

- I. Abrir y llevar una o más cuentas de fondos de pago electrónico por cada Cliente, en las que se realicen registros de abonos equivalentes a la cantidad de fondos de pago electrónico emitidos contra la recepción de una cantidad de dinero, en moneda nacional o extranjera, o de activos virtuales determinados;
- II. Realizar transferencias de fondos de pago electrónico entre sus Clientes mediante los respectivos abonos y cargos en las correspondientes cuentas a que se refiere la fracción I de este artículo;
- III. Realizar transferencias de determinadas cantidades de dinero en moneda nacional o, sujeto a la previa autorización del Banco de México, en moneda extranjera o de activos virtuales, mediante los respectivos abonos y cargos en las correspondientes cuentas a que se refiere la fracción I de este artículo, entre sus Clientes y aquellos

de otra institución de fondos de pago electrónico, así como cuentahabientes o usuarios de otras Entidades Financieras o de entidades extranjeras facultadas para realizar Operaciones similares a las que se refiere este artículo;

IV. Entregar una cantidad de dinero o activos virtuales equivalente a la misma cantidad de fondos de pago electrónico en una cuenta de fondos de pago electrónico, mediante el respectivo cargo en dicha cuenta, y

V. Mantener actualizado el registro de cuentas a que se refiere la fracción I de este artículo, así como modificarlo en relación con el ingreso, transferencia y retiro de fondos de pago electrónico, de acuerdo con lo señalado en las fracciones I, II, III y IV del presente artículo, según corresponda.

El artículo anterior contempla una nueva figura bajo la cual pueden operar instituciones que realicen funciones de “emisión, administración, redención y transmisión de fondos de pago electrónico” a través de plataformas digitales o electrónicas. Asimismo, en las fracciones de la I a la IV se desmenuzan los actos a través de los cuales se llevan a cabo estas actividades.

La primera fracción señala una de las actividades que puede efectuar una IFPE; abrir y llevar cuentas de fondos de pago electrónico por cada cliente, en las cuales se reflejen sus abonos en moneda nacional o extranjera y activos virtuales determinados. La segunda fracción se refiere a la posibilidad de transferir de manera electrónica fondos entre sus clientes, reflejando cargos y abonos. La tercera se relaciona estrechamente con la anterior ya que autoriza estos mismos traspasos, pero entre clientes de diferentes IFPE e incluso desde y hacia otras EF que no se consideren IFPE. La cuarta menciona la necesidad de que la cantidad entregada de dinero o activos virtuales sea igual al balance reflejado en una cuenta de fondos de

pago electrónico a nombre del cliente. Por último, la fracción quinta hace mención de la obligación de las IFPE de llevar un registro de cuentas de sus clientes y los movimientos de estas.

Este artículo es de suma relevancia para el presente trabajo. La manera en la cual la LRITF lidia con los *exchanges*, al autorizar una figura específica para su constitución, es por mucho superior a la manera en la cual el mismo tema a sido tratado en los EE. UU. En el caso del vecino país del norte, la industria se encuentra atrapada en definiciones que en ocasiones pueden parecer contradictorias. Por una parte, la mayoría de los intercambios han tomado la forma de un MSB a falta de una mejor opción, lo cual presenta el gran inconveniente de, además de no ser una figura adecuada para las necesidades legales y operativas de un negocio de esa naturaleza, ser regulada a nivel estatal, por lo que se tienen que realizar trámites en cada localidad en la que se desee operar. Mientras, la opinión de la SEC es que los operadores que traten con activos virtuales, que, de acuerdo con ellos, tengan características de valores deberían adoptar la forma de plataforma de intercambios de valores.

En contraste, la regulación mexicana ofrece un permiso federal, válido para toda la república, lo cual, es mucho más adecuado, sobre todo partiendo de considerar la naturaleza móvil de un negocio como lo es un intercambio de activos virtuales, que puede operar con cualquier cliente en cualquier parte, mientras exista una conexión a Internet.

Prosiguiendo con el análisis, la siguiente fracción digna de un estudio minucioso es la tercera. El apartado menciona la posibilidad de transferir activos virtuales, sujeto a las debidas restricciones, no sólo a otros clientes de esta IFPE que maneja su cuenta, sino de otras IFPE, e incluso a Entidades Financieras que no sean una ITF, como Instituciones de Crédito. Esta disposición es muy vanguardista, ya que es muy poco común que se permita a las instituciones bancarias en cualquier parte del mundo operar con estos activos. Permitir que las EF, que no sean ITF, participen en el mercado es un paso acertado, en cuanto a que dotará a las autoridades de mayor visibilidad de lo que pasa en los mercados, similar a la experiencia de la

CFTC, que puede ser útil para la determinación de precios o prever riesgos financieros, además de fomentar la competencia entre operadores de activos virtuales. La autorización se establece de manera expresa en el Título IV “De las Autorizaciones Temporales y Operación con Activos Virtuales”, Capítulo III “De la Operación de Entidades Financieras con Activos Virtuales”, artículo 88, el cual se transcribe a continuación:

Artículo 88.- Las instituciones de crédito podrán, con la previa autorización del Banco de México, realizar operaciones con los activos virtuales que sean determinados por el propio Banco de México mediante disposiciones de carácter general, de entre aquellos que cumplan las características mencionadas en el último párrafo del artículo 30 de esta Ley. Dichas operaciones estarán sujetas en cuanto a sus condiciones y restricciones, a las disposiciones de carácter general que para tal efecto emita el Banco de México.

Hace sentido que se autorice la operación con activos virtuales por parte de más participantes desde el punto de vista regulatorio, ya que es deseable que existan el mayor número posible de puntos de contacto entre el sistema financiero tradicional y el cripto-espacio. Lo anterior dado que, es muy complicado y no deseable limitar a los activos virtuales directamente, que han probado ser un punto de escape importante al estricto escrutinio al que normalmente está sujeto el movimiento de dinero. Una manera de combatir esto es involucrando más al sistema financiero tradicional, dado que es muy probable que quien desee utilizar activos virtuales para fines ilícitos busque intercambiarlos por moneda fiduciaria en algún punto.

Pese a lo anterior, siguen existiendo esquemas por medio de los cuales es posible evadir la regulación y que permiten utilizar activos virtuales en operaciones ilícitas facilitando a delincuentes la creación de un ecosistema en el cual los activos pueden ser usados como medio de pago sin tocar el sistema financiero tradicional. Hay diversas maneras de hacer lo anterior²⁸⁷, a modo de ejemplo se mencionan algunas.

²⁸⁷ (Becerra, 2018)

En un primer escenario, un sujeto recibe cualquier activo virtual en grandes cantidades, como puede ser Monero²⁸⁸ o Zcash. La persona lo vende o permuta, por medio de una operación de carácter privado a cambio de efectivo o cualquier otro bien, que después puede ser revendido. Posteriormente, el dinero producto de la reventa es depositado en cuentas de empresas fantasmas, con lo que se oculta el origen de la riqueza, disfrazándola de las utilidades obtenidas por la venta del bien. El dinero puede ser gastado con posterioridad, con la tranquilidad que proviene de una fuente “lícita”.

Asimismo, otra forma de operar con activos virtuales de procedencia ilícita es mediante la compra de tarjetas de regalo utilizando activos virtuales a través de sitios que no requieren de una identificación por parte del usuario. Una vez que el crédito ha sido adquirido es revendido, utilizando el esquema previamente mencionado. Una forma más que se ha vuelto cada vez más complicada conforme pasa el tiempo, en parte por los esfuerzos de distintos gobiernos, es el intercambio de activos virtuales, por moneda fiduciaria utilizando plataformas que no requieren registro. Este esquema es cada vez más irrealizable porque hay cada vez menos *exchanges* que permiten operar a sus usuarios sin ningún tipo de comprobación de identidad, sobre todo cuando se trata de grandes cantidades de activos virtuales. Por la anterior razón mucha gente recurre a foros o sitios de internet en los cuales se facilita contactar a otros individuos interesados en una compraventa directa y, en ocasiones, en persona de activos virtuales.

Este tipo de esquemas están circunscritos, generalmente, a activos criptográficos que tienen una naturaleza anónima como Monero o Zcash. La utilización de activos como ether o bitcoin es cada vez menor, en parte por su naturaleza semi-anónima que ha traído como consecuencia que incluso se analice la posibilidad de introducir ciertas direcciones o llaves públicas en una lista negra²⁸⁹ que le impediría al propietario de éstas comerciar con los valores contenidos en ella, siempre y cuando

²⁸⁸ Una cripto-moneda que hace énfasis en mantener la privacidad de sus usuarios y las transacciones que realizan, no obstante, existen dudas respecto a la protección que ofrece a los usuarios. (Möser, 2018)

²⁸⁹ En el caso del Departamento del Tesoro de los EE. UU. se trataría de la *Specially Designated Nationals And Blocked Persons List*, (“SDN”)

puedan ser asociadas a un individuo con cierto grado de certidumbre. No obstante, en realidad se estaría marcando a la persona y todas las direcciones relacionadas con ella y no las “cuentas” como tal. Es el gobierno de los EE. UU. quien ha anunciado que tomarán medidas de este tipo, haciendo lo necesario para impedir la operación con las carteras marcadas, notificando a la Oficina de Control de Activos u “OFAC” por sus siglas en inglés²⁹⁰. El bloqueo se llevará a cabo mediante la inscripción del identificador de la cartera y el activo virtual que se maneja a través de ella.

La integración de esta lista parece ser un paso necesario para disuadir la utilización de activos virtuales en actividades ilícitas, pero al juzgar su instrumentación parece ser francamente insuficiente. No se requiere gran esfuerzo para trasladar los fondos de una dirección a otra, por lo que se deberían de bloquear todas las llaves públicas que a su vez celebren transacciones con la bloqueada, lo que es perfectamente posible utilizando el registro permanente e inmodificable que es una cadena de bloques. Pero a su vez, esta prohibición únicamente será efectiva en determinados casos, ya que existen servicios que permiten esconder la dirección de origen o destino de una transacción o incluso activos virtuales que por su naturaleza son prácticamente imposibles de rastrear²⁹¹.

Retomado el análisis del artículo 22, el mismo presenta grandes incógnitas respecto a la posible operación de un intercambio descentralizado de activos virtuales. En este tipo de plataformas, el operador no custodia los activos virtuales de los usuarios, ya que las “llaves privadas” de la cartera las posee el usuario y nadie más tiene acceso a sus fondos, lo que da un mayor control y confidencialidad, pero conlleva el riesgo de que, si las pierde, nadie más puede recuperar los fondos de esa cuenta, nadie. Por lo que, si se pierde el acceso del usuario a su cartera, la institución estaría imposibilitada de recuperar sus fondos, incumpliendo con la dispuesto en la fracción IV, además que le sería complicado mantener un registro

²⁹⁰ (OFAC, 2017)

²⁹¹ Esta afirmación debe de ser matizada, gracias a avances en la comprensión de la tecnología y nuevas técnicas por parte de las autoridades investigadoras los espacios en los que se pueden mover activos virtuales de manera inadvertida son cada vez menos. Para más información ver: (Ludwin, 2015)

pormenorizado como lo marca la fracción V. Asimismo, otro elemento inherente a la naturaleza de un intercambio descentralizado es que no es el operador quien vende o compra los activos, este simplemente funge como un intermediario que contacta a un comprador y a un vendedor y los conecta mediante su sistema. En general, tal parece que más que apegarse a la figura de una IFPE un intercambio descentralizado tendría que constituirse bajo la “figura” del artículo 17 de la LFPIORPI que impone menos obligaciones²⁹², ya que la naturaleza de este tipo de plataformas se antoja incompatible con varios puntos del artículo 22. Empero, esta afirmación podría ser refutada con base en lo dicho el artículo 25, que será examinado con posterioridad.

Prosiguiendo con el estudio de las IFPE, el artículo 23 también hace referencia a los activos virtuales. En primer lugar, define a los fondos de pago electrónico como “aquellos fondos que estén contabilizados en un registro electrónico de cuentas transaccionales”, que mantenga una IFPE. Después, hace referencia que estos también podrán quedar referidos a activos virtuales al ser emitidos contra la recepción de activos virtuales, quedando el balance establecido a partir de depósitos que haga el cliente denominados en algún activo virtual,

En el siguiente artículo, el 24, se hace una diferenciación tácita entre activos virtuales convertibles y no convertibles, en concordancia con la clasificación plasmada en el documento “Dinero Virtual, Definiciones Clave y Riesgos Potenciales en Materia de Lavado de Dinero y Financiamiento al Terrorismo”²⁹³ de la FATF²⁹⁴, discutido en el Capítulo IV. A estos no se les llama explícitamente activos virtuales no convertibles, sino que únicamente no los considera como fondos de pago electrónico. Esta distinción se refiere a que los activos virtuales convertibles, pueden ser fácilmente transformados en moneda de curso legal. Mientras, los no convertibles, no pueden serlo, por lo menos utilizando canales oficiales.

²⁹² El artículo referido no contiene una figura como tal bajo la cual se pueda organizar un intercambio, pero al amparo de la disposición podría operar un bróker de activos virtuales, únicamente con la obligación de reportar las operaciones que sobrepasen el umbral.

²⁹³ Discutido en el capítulo IV

²⁹⁴ (Financial Action Task Force, 2014)

Por último, el artículo 25 también es significativo para el tema, sobretodo las fracciones VI y XI. El artículo declara lo siguiente

Artículo 25.- Las instituciones de fondos de pago electrónico, además de las Operaciones y actividades a que se refiere esta Ley, pueden únicamente realizar conforme a lo previsto en el presente ordenamiento, las siguientes:

[...]

VI. Realizar operaciones con activos virtuales, en términos de lo dispuesto en esta Ley;

XI. Poner en contacto a terceros con la finalidad de facilitar la compra, venta o cualquier otra transmisión de activos virtuales, sujeto a lo dispuesto en esta Ley;

[...]

La fracción VI no presenta grandes novedades, considerando que ya fue plenamente establecido la posibilidad de una IFPE de operar con activos virtuales. La diferencia podría venir en su redacción. En el artículo 4 de la ley se define en la fracción XVIII el término “Operaciones” como “los actos de carácter financiero o de pagos a que se refiere la presente Ley, que una ITF puede ofrecer o realizar con el público o, que a través de ellas se realizan entre Clientes, en términos de esta Ley;”.

La fracción XI parece ir encaminada a intercambios descentralizados. Como fue mencionado anteriormente en el Capítulo, parece que la figura de las IFPE no se ajusta totalmente a la idea de un intercambio descentralizado ya que estos últimos se asemejan más un intermediario o bróker que a un operador de activos virtuales. Por lo tanto, la naturaleza de una plataforma descentralizada trae muchas consecuencias que deberían de ser consideradas al momento de imponerle una

regulación. Una plataforma de intercambio descentralizado únicamente pone de su parte la infraestructura digital para que una parte publique una oferta de venta y otra satisfaga dicha orden, sin que en ningún punto los activos toquen sus manos. El problema surge cuando se vuelve evidente que la esencia de un intercambio descentralizado y de un centralizado son completamente diferentes. El primero puede soportar el peso económico que implica una regulación más pesada y su operación requiere de la recolección de ciertos datos, el segundo no necesita una base de datos de los usuarios para su operación. Si bien en ningún momento se propugna porque estas plataformas escapen de toda regulación²⁹⁵, es importante tener en cuenta su naturaleza al momento de reglamentar sus actividades.

²⁹⁵ Aunque aún no es clara la dirección que tomara la regulación en los EE. UU., se espera que la reglamentación en materia de reporte de información financiera que se le aplicó a los intercambios centralizados se les aplique a los descentralizados.

VI.4.3. Capítulo Tercero, “De las Operaciones con Activos Virtuales”

VI.4.3.1. Artículo 30

El Capítulo Tercero del Título Segundo de la LRITF es el apartado más importante del marco jurídico mexicano, relativo a los activos virtuales. Dada la relevancia del capítulo, el análisis de cada artículo se hará por separado en una sección propia. A continuación, es reproducido su primer artículo, el 30, para su análisis:

Artículo 30.- Para efectos de la presente Ley, se considera activo virtual la representación de valor registrada electrónicamente y utilizada entre el público como medio de pago para todo tipo de actos jurídicos y cuya transferencia únicamente puede llevarse a cabo a través de medios electrónicos. En ningún caso se entenderá como activo virtual la moneda de curso legal en territorio nacional, las divisas ni cualquier otro activo denominado en moneda de curso legal o en divisas.

Las ITF solo podrán operar con los activos virtuales que sean determinados por el Banco de México mediante disposiciones de carácter general. En dichas disposiciones, el Banco de México podrá establecer plazos, términos y condiciones que deberán observar las ITF para los casos en que los activos virtuales que este haya determinado se transformen en otros tipos o modifiquen sus características.

Para realizar operaciones con los activos virtuales a que se refiere el párrafo anterior, las ITF deberán contar con la previa autorización del Banco de México.

El Banco de México para la determinación de los activos virtuales tomará en cuenta, entre otros aspectos, el uso que el público dé a las unidades digitales como medio de cambio y almacenamiento de valor, así como, en su caso, unidad de cuenta; el tratamiento que otras jurisdicciones les den a unidades digitales particulares como activos virtuales, así como

los convenios, mecanismos, reglas o protocolos que permitan generar, identificar, fraccionar y controlar la replicación de dichas unidades.

En su primer párrafo, el artículo transcrito propone el uso del término activo virtual y una definición de este, aclarando que en ningún caso se entenderá como moneda de curso legal, divisas o cualquier otro activo denominado en moneda de curso legal o divisas. Primeramente, es de reconocerse un acierto en la denominación del objeto a regular como activo virtual, de acuerdo con lo argumentado en el capítulo “Taxonomía de los Activos Virtuales”. Dicho término es correcto ya que la velocidad de desarrollo del escenario de los activos virtuales hace complicado utilizar un término más restrictivo. Los vocablos activo y virtual son adecuados para abarcar una amplia gama de conceptos que de otra manera no podrían ser contenidos en un mismo grupo.

Ahondando en el tema, como fue discutido en el capítulo “Taxonomía de los Activos Virtuales”, utilizar la palabra activo es apropiado dado que, de acuerdo con Burniske y White, el concepto de dinero o moneda ha sido rebasado por el conjunto que componen los activos virtuales, considerando que el objetivo de una moneda es ser utilizada como medio de pago, unidad de cuenta y depósito de valor²⁹⁶. Por ejemplo, el uso que le da la comunidad al activo virtual más popular, bitcoin, es muy diferente al del dinero²⁹⁷. Actualmente, su uso va más encaminado a ser un activo especulativo gracias a su gran volatilidad, lo cual paradójicamente lo hace pésima unidad de valor y depósito de este.

Por otro lado, existen ciertos activos virtuales creados con posterioridad al bitcoin que si son utilizados de manera habitual de manera similar al dinero. Del mismo modo, han surgido otros activos que no son y nunca han tenido la intención de

²⁹⁶ (Burniske & Tatar, 2018, p. 84)

²⁹⁷ Al respecto, se menciona que la red Bitcoin en momentos de mucha afluencia hace que sean imprácticas las transacciones de cantidades relativamente menores de bitcoin por motivo de las comisiones cobradas por los mineros o incluso por razones de eficiencia energética.

funcionar como el dinero. El apareamiento de esta multitud de activos tuvo como consecuencia el intento de clasificarlos en diversas categorías. El intento de diferenciación es registrado tanto de manera doctrinal²⁹⁸, por organizaciones no gubernamentales²⁹⁹, en otras jurisdicciones³⁰⁰ e inclusive por autoridades mexicanas³⁰¹. Así, aunque la manera de clasificar varía de acuerdo con el autor, es indiscutible que existen activos virtuales de diferentes características con funciones desemejantes y que no pueden ser regulados de la misma manera. Desafortunadamente, en este artículo la LRITF no se reconocen estas diferencias y en consecuencia se comete una serie de desaciertos.

En síntesis, a pesar de que el término con el cual se nombre a los activos virtuales es acertado, la manera en la cual se les define no es la correcta. Se les denomina un medio de pago cuya transferencia únicamente puede llevarse a cabo a través de medios electrónicos. Consistentemente a lo largo del trabajo es señalado, que si bien ser un medio de pago es la función de algunos activos virtuales, no es la de todos. ¿Qué objeto tiene llamarles activo virtual, si de todas maneras se asimilará su definición a la de una cripto-moneda³⁰² en sentido estricto? Las cripto-monedas son una subclasificación de activos virtuales. En ese sentido, la definición contenida en el artículo 30 es sumamente desafortunada ya que no contempla, por ejemplo, a los *tokens* utilizados ya sea como instrumento de inversión o de utilidad, dejando la puerta abierta a problemas posteriores. Otro error del artículo es el considerar a las palabras virtual y digital como intercambiables. Como es mencionado en el capítulo “Taxonomía de los Activos Virtuales”, Virtual se refiere a aquello que no tiene una equivalencia en el mundo material, en contraste de lo digital, que es una representación computacional de algo que puede o no existir en el plano físico.

²⁹⁸ (Burniske & White, 2017), (Howden, 2015)

²⁹⁹ (Financial Action Task Force, 2014, p. 5)

³⁰⁰ (FINMA, 2017)

³⁰¹ (Banxico; CNBV; SHCP, 2017)

³⁰² De acuerdo con la clasificación de (Burniske & Tatar, 2018)

No obstante, se debe mencionar que también hubiera sido un error plasmar en la ley alguna clasificación, dado que como es reconocido a lo largo del trabajo, el campo de los activos virtuales es un espacio en constante evolución en el cual lo que es válido un día puede no serlo al siguiente. Por lo tanto, el regulador mexicano debería optar por una clasificación contenida en disposiciones de carácter general, de fácil modificación, basándose en la doctrina y en el caso suizo, que contemple una regulación diferenciada para cada grupo de activos, siempre atento a la evolución de la industria. La anterior reglamentación haría bien en reconocer que hay grupos de activos con características similares a las de un valor, a las del dinero, o activos que cumplen con una función específica dentro de una plataforma. Asimismo, se deben de considerar los activos que descansan sobre la tecnología *blockchain*, pero que son utilizados para fines nada relacionados con ser un medio de pago, como los coleccionables. El error del artículo fue el regular la totalidad de activos virtuales conforme a la definición de un sólo subgrupo de estos.

Paralelamente, la regla de la última parte del párrafo no debe de sorprender, ya que el no reconocimiento de los activos virtuales como moneda de curso legal o divisa es una postura mantenida de manera reiterada tanto por autoridades nacionales como extranjeras. Generalmente, este punto es motivo de preocupación para las personas que desean involucrarse con activos virtuales, sin embargo, debe de entenderse que ni el bitcoin, ni ningún otro activo virtual (con la posible excepción del Petro Venezolano o la cripto-moneda emitida por la República de las Islas Marshall) tiene ni ha tenido la intención de ser una moneda de curso legal respaldada por un estado. Aun así, es interesante que existan personas que utilizan esta información para provocar miedo en posibles usuarios de activos virtuales con el fin de alejarlos.

Por otra parte, el párrafo segundo contiene uno de los mayores tropiezos de la presente legislación al permitir que sea el Banco de México el que “determine” (un eufemismo para autorizar) con qué activos virtuales pueden operar las ITF y EF no

ITF. La facultad otorgada a Banxico va contra la naturaleza del objeto a regular, es impráctica y contraproducente, como es argumentado a continuación.

Antes que nada, es necesario recordar el objeto y en el contexto en el cual nace bitcoin, el primer activo virtual y precursor de todos los demás. El crypto-activo empezó a existir junto con las consecuencias de la crisis financiera del 2008, un periodo de gran desconfianza en las instituciones de banca tradicional y el sistema financiero, que se percibían como culpables de la debacle. En ese escenario, Bitcoin se presentó como una alternativa al control financiero centralizado, ya fuera ejercido por bancos centrales, procesadores de pagos, o cualquier otro, argumentando que no debería de existir un único punto de fallo, y que dichas instituciones no deberían de tener tanto poder sobre la vida económica de la gente.

En consecuencia, los crypto-activos se basan en principios fundamentalmente diferentes a los que rigen al sistema financiero tradicional. Se cimientan en el concepto de descentralización, en toda la extensión de la palabra. No hay una autoridad central³⁰³, ni hay necesidad de depositar toda la confianza en una sola entidad o persona. En su lugar, la seguridad del sistema descansa en manos de los usuarios finales de la red. Incluso es diferente desde un punto de vista arquitectónico en relación con los sistemas de pagos actuales³⁰⁴. Los activos virtuales, especialmente el bitcoin, transfieren valor mediante un mecanismo “push” y no “pull” como sucede con otros modos de pago. Un traslado de valor usando bitcoin no es una autorización de hacer un cargo (o “jalar”) en el balance una cuenta, sino que el valor se saca o “empuja” fuera de la misma. Gracias a esta manera de operar, una transacción no expone la identidad de la cuenta o la identidad de quien la realiza, ya que hay ciertas “carteras” que generan una llave pública para cada transferencia.

³⁰³ Esto es discutido bajo el argumento que para el mantener el software de la red en estado óptimo con actualizaciones periódicas se requiere de un cierto grado de centralización, como un repositorio de Github.

³⁰⁴ (Antonopoulos, 2014)

Asimismo, desde el punto de vista operativo, al tratarse de una red descentralizada no hay necesidad de una supervisión central. No hay un punto único de falla que requiera constante inspección. El sistema se defiende a si mismo mediante criptografía y el ofrecimiento de incentivos a los mineros y los usuarios de este. Por lo tanto, al permitir que una institución, en este caso el Banco de México, regule un activo que descansa sobre una red descentralizada se debilita el modelo y se reduce su capacidad de innovación. No se debe de regular la tecnología ni a los activos, sino a sus operadores y aunque la ley pareciera seguir este principio, el artículo 30 se acerca peligrosamente a una reglamentación directa.

El principal objetivo de la descentralización es dejar a un lado la confianza en las instituciones, que pueden fallar, o incluso trabajar en contra de los intereses de la población, y pasar a un sistema que se base en incentivos y en certeza matemática. Por lo que, desde un punto de vista filosófico y conceptual, parecería contradictorio que un icono de la centralización como lo es Banxico regule lo que nació descentralizado, en claro desafío del sistema financiero mundial y al concepto mismo de la soberanía monetaria. No obstante, es importante mencionar que dentro del desacierto que representa que el organismo regule la materia, existe un lado positivo. La institución es un baluarte de la estabilidad, por lo que en caso de que tome una decisión que resulte positiva para la industria es altamente probable que esta decisión permanezca, más allá de los vaivenes políticos de la nación.

De igual manera, las nuevas facultades de Banxico son ineficaces si se ven desde un punto de vista práctico. El mercado de activos virtuales se comprende de miles de activos con diferentes nombres y características. Se antoja imposible que una institución como Banxico pudiera dedicar los recursos suficientes como para monitorear un espacio de tal magnitud. En este tenor, en todo caso la regla debería ir en sentido contrario, indicando que las ITF no podrán operar con los activos virtuales que no autorice el banco central, permitiendo por defecto la operación de aquellos que no estén prohibidos. Considerando el avance de la tecnología y la variedad de proyectos será imposible que se mantenga al día la supuesta lista de

activos autorizados por la autoridad. Existen cientos de activos virtuales a los cuales el público desea tener acceso y es imposible que la autoridad los mantenga vigilados a todos y si los veta o no los reconoce sin una razón válida, la industria será la principal afectada. Paralelamente, se reitera que la regulación es excesiva, ya que si bien hay casos documentados de fraude en el cripto-espacio, sobre todo en materia de *ICOs*, hay otras maneras de proteger al público. Por ejemplo, en esos casos podría ser posible tomar un acercamiento más integral en el cual se emprendiera una acción contra el proyecto que esté celebrando el *ICO* en cuestión, y como consecuencia de esta persecución se prohibiera en particular el activo virtual que pudiera haberse emitido.

Todavía más, si el objetivo es que la población no acceda a ciertos activos virtuales, la prohibición puede resultar ser insuficiente. Una vez que el usuario tiene acceso a casi cualquier activo virtual, como el bitcoin, puede trasladarlo a un intercambio en el extranjero, sin que pueda ser impedido por las autoridades. Una vez fuera del país, el sujeto podrá adquirir otros activos sin ninguna restricción ni protección por parte del Estado Mexicano. En resumidas cuentas, una mala aplicación del artículo puede tener el efecto contrario de proteger al público al obligarlos a operar en el extranjero, donde no tendrá ningún tipo de protección. Este mismo razonamiento puede ser utilizado como argumento contra la sobrerregulación de intercambios mexicanos, los cuales, si se ven abrumados por los requisitos a cumplir, pueden verse tentados a cambiar su domicilio a una jurisdicción más amigable y operar desde ahí, dándole servicio a ciudadanos de todas nacionalidades, incluyendo mexicanos, sin que se les pueda impedir.

Mas aún, no es claro cómo determinará Banxico con cuáles activos virtuales pueden operar las ITF y con cuales no. Los criterios que se mencionan de manera somera en el artículo 30 no son suficientes para brindar certeza a la industria. Si bien sería un desacierto que en la ley se plasmaran a detalle los mecanismos de selección, la manera en la que se desarrollaron dichos criterios en la legislación tampoco es óptima. En primer lugar, únicamente considera el uso que le da el público a los

activos virtuales como “medio de cambio, almacenamiento de valor o unidad de cuenta” esto es un desacierto, ya que como se argumenta anteriormente, el objeto de los activos virtuales no sólo es funcionar como dinero. Paralelamente, la redacción del apartado hace que surjan numerosas incógnitas como ¿Qué sucedería si un activo con el que se operaba anteriormente se desautoriza? A qué obligaciones estarían sujetas las ITF y EF que operen con dichos activos, ¿Podrían ser sujetos a alguna responsabilidad por parte de sus clientes? Una posible determinación en la materia por parte del Banco de México presenta serias dudas que pueden impactar profundamente la operación de una IFPE que opere con activos virtuales.

Por otra parte, en la instrumentación de la disposición, es muy importante tener mucho cuidado con lo que digan los participantes de la industria en lo individual. En otras jurisdicciones con normas similares existen casos en los cuales³⁰⁵ se da un agresivo cabildeo para desautorizar activos que ciertas empresas no pueden listar por razones técnicas con el fin de evitar que la competencia lo haga, en detrimento del público.

Asimismo, cabe señalar que si bien puede ser positivo hasta cierto punto familiarizarse con las reglas que regulan la generación, identificación, fraccionamiento y control de la replicación de activos virtuales. Dichos protocolos están contenidos en documentación sumamente técnica, desde un punto de vista computacional, y, por lo tanto, se debe de evaluar hasta que punto Banxico, como institución primordialmente económica y financiera está preparada para afrontar el reto que dicha revisión supone.

Del mismo modo, es problemático señalar que el Banco de México tomará en cuenta para autorizar la operación con ciertos activos virtuales considerando el uso que se les dé, ¿Cómo es posible esto si en teoría el público mexicano no puede acceder a ellos ya que está prohibido que las ITF y las EF comercien con ellos, antes de ser

³⁰⁵ (Powell, 2018)

reconocidos? Esta podría ser una manera razonable de determinar la autorización respecto de la primera ola de activos que ya se utilizan, pero una vez liberada un “lista” con autorizados, en teoría sería complicado acceder a los no autorizados. A pesar de todo lo anterior, es salvable de la disposición que se establezca cómo un factor para el reconocimiento el observar el desarrollo de otras jurisdicciones para determinar el camino de la industria en México.

Al respecto de las anteriores observaciones, el trabajo de la ONG Coin Center³⁰⁶ es sumamente relevante para la adopción de las mejores prácticas en la legislación nacional. Proporciona valiosa información a los tomadores de decisiones que puede ser utilizada para determinar la viabilidad de un activo virtual, sobre todo cuando hay un evento generador de monedas, tal como un *ICO*, involucrado. Estos documentos pueden servir como base para un marco de referencia básico que norme la emisión de disposiciones generales en materia de activos virtuales. Por ejemplo, las publicaciones realizadas por la organización tocan el tema de la revisión de protocolos controladores de activos virtuales, haciendo hincapié en los bajos riesgos que pueden representar los modelos completamente descentralizados, los proyectos montados en cadenas no propias, activos virtuales que son emitidos a través de un esquema de minería competitiva y computadoras virtuales distribuidas (como *EVM*) y *App Coins* o *tokens* de utilidad. Por el contrario, advierte de los riesgos de activos virtuales cerrados o con poca transparencia en su operación, de los activos virtuales distribuidos en su gran mayoría en una preventa y con una comunidad muy centralizada de validadores de transacciones³⁰⁷.

Lo presentado con anterioridad es sólo una pequeña muestra de numerosas propuestas que presenta la organización y que son muy valiosas para la construcción de disposiciones de carácter general relacionadas con la “determinación” de activos virtuales.

³⁰⁶ (Van Valkenburgh, 2016)

³⁰⁷ *Ibidem*, p. 53

VI.4.3.2. Artículo 31

Respecto al siguiente artículo, el 31, es significativo analizar el contenido del primer párrafo, que plantea lo siguiente:

Artículo 31.- Las ITF que operen con activos virtuales deberán estar en posibilidad de entregar al Cliente respectivo, cuando lo solicite, la cantidad de activos virtuales de que este sea titular, o bien el monto en moneda nacional correspondiente al pago recibido de la enajenación de los activos virtuales que corresponda. Estas operaciones deberán liquidarse en los términos y sujeto a las condiciones que, al efecto, establezca el Banco de México mediante disposiciones de carácter general.

[...]

Hay dos cuestiones dignas de ser examinadas. En primer lugar, la relación que guarda el artículo con los intercambios descentralizados. Su naturaleza no es compatible con este artículo. En un intercambio descentralizado los activos están bajo la custodia del usuario por lo que un eventual operador de una plataforma de estas no podría estar en posibilidades de entregar al cliente sus activos virtuales. Dicho de otra manera, en un intercambio descentralizado sólo el usuario tiene acceso a sus fondos, por lo que aún si utiliza una cartera de la plataforma no sería posible que se le devolvieran los fondos. Con esto en mente, se refuerza el argumento de que la figura adecuada para una plataforma de intercambio descentralizado no es la de una IFPE, sino el esquema de Modelo Novedoso o el artículo 17 de la LFPIORPI.

Paralelamente, se debe de reconocer una limitación técnica a la que se ven sujetos ciertos intercambios. Por motivos de seguridad, algunos intercambios no tienen grandes cantidades de activos virtuales en una cartera online o *hot wallet* ya que

hacerlo los convertiría en blancos atractivos de atacantes maliciosos. El único objeto de este tipo de carteras es satisfacer las ordenes inmediatas de compra o venta de los usuarios. Las reservas principales de activos virtuales se mantienen en carteras no conectadas al internet, o *cold wallets*, por motivos de seguridad. Las implicaciones que esto tiene para el artículo es que en caso de que se dé una gran afluencia de operaciones de manera repentina e inesperada, una plataforma podría verse momentáneamente imposibilitada para satisfacer órdenes ya que sus reservas en la cartera online se verían agotadas y deba de pasar un tiempo antes de trasladar más fondos de la cartera *offline* a la *online*.

Una situación análoga sería lo que sucede con un cajero y una bóveda, el retiro de efectivo de un cajero es una opción más conveniente, si bien es posible que sea robado con mayor facilidad que una bóveda. Cuando al cajero se le acaba el efectivo tendrá que ser rellenado de dinero contenido en la bóveda, la cual es mucho más segura, pero de la cual no es posible que los clientes extraigan directamente su efectivo. Esta situación debe de ser contemplada al momento de emitir disposiciones generales, sin dejar a un lado que los operadores deben de ajustar sus protocolos para evitar, en la medida de lo posible, situaciones de este tipo.

VI.4.3.3. Artículo 32

A continuación, se transcribe el artículo 32 para su análisis:

Artículo 32.- El Banco de México definirá las características de los activos virtuales a que se refiere este Capítulo, así como las condiciones y restricciones de las Operaciones y demás actos que se pueden realizar con dichos activos, mediante disposiciones de carácter general que para tal efecto emita. Asimismo, el Banco de México establecerá las medidas a las que deberán sujetarse las ITF para la custodia y control que sobre los activos virtuales ejerzan al realizar tales Operaciones y actos.

Para efectos de este Capítulo, se entenderá por custodia y control de activos virtuales a la posesión de las firmas, claves o autorizaciones que sean suficientes para ejecutar las Operaciones a que se refiere esta Ley.

El artículo inicia con una afirmación interesante. Hace referencia a la posibilidad del Banco de México de “definir las características de los activos virtuales a que se refiere ese Capítulo”. Lo menos que se puede decir al respecto es que la manera en la que se redactó el artículo es desafortunada. Al parecer, el artículo podría hacer referencia a la facultad de Banxico de reconocer y por lo tanto clasificar activos virtuales de acuerdo a sus características.

Es incorrecto por parte del artículo suponer que el Banco puede determinar las características de un activo virtual. La institución puede reconocerlas y definir las como propias de un activo en determinado momento, para así saber si estas cambian, modificando la naturaleza del activo en cuestión. Lo anterior sería saludable, sobre todo si se propugna por una categorización flexible de activos virtuales que puede cambiar a causa de múltiples factores, incluso la afirmación de que Banxico tenga la posibilidad de reconocer las particularidades de un activo

virtual sería adecuada. Pero Banxico no puede “definir” las características de un activo.

La segunda parte del párrafo hace referencia a los estándares que deberán cumplir los operadores en materia de custodia y control de activos virtuales al momento de realizar operaciones. Del texto del artículo se desprende que existirán medidas emitidas por el Banco de México acerca de la custodia y control de llaves privadas. No sería posible para un descentralizado hacerlo porque no posee ni la custodia ni el control de dichas llaves, lo que acaba de dar al traste con la posibilidad de un intercambio descentralizado operado por una IFPE. Lo anterior dado que el objeto de una plataforma de este tipo es que el propio usuario mantenga custodia de sus llaves privadas.

Por último, es sumamente interesante el planteamiento que hace el segundo párrafo respecto a la custodia. Son muy contados, si no es que inexistentes, los ordenamientos jurídicos en el mundo que hacen referencia al problema de custodia y control en materia de intercambios de activos virtuales. El artículo define para efectos del marco legal mexicano a la custodia y control de activos virtuales cómo “posesión de las firmas, claves o autorizaciones que sean suficientes para ejecutar las Operaciones a que se refiere esta ley”, lo cual es un gran acierto que permitirá avanzar en la clarificación de términos.

VI.4.3.4. Artículo 33 y 34

Para proseguir con el análisis del capítulo, se reproduce el siguiente artículo:

Artículo 33.- Las ITF tendrán prohibido vender, ceder o transferir su propiedad, dar en préstamo o garantía o afectar el uso, goce o disfrute de los activos virtuales que custodien y controlen por cuenta de sus Clientes, excepto cuando se trate de la venta, transferencia o asignación de dichos activos por orden de sus Clientes.

Las ITF solo podrán participar en la operación, diseño o comercialización de instrumentos financieros derivados que tengan activos virtuales como subyacente, en los casos, condiciones y sujeto a los requisitos y autorizaciones que establezca el Banco de México en disposiciones de carácter general.

El artículo 33 inicia con la prohibición de las ITF de “vender, ceder o transferir su propiedad, dar en préstamo o garantía o afectar el uso, goce o disfrute de los activos virtuales que custodien y controlen por cuenta de sus Clientes” excepto si los clientes lo permiten. Lo anterior parece bastante obvio dado que los activos virtuales bajo la custodia de la ITF no son de su propiedad, por lo que no hay razón para que puedan disponer de ellos en ninguna manera y es congruente con la naturaleza de las IFPE, ya que como su nombre lo indica son instituciones de pago, no de inversión.

En otro orden de cosas, el segundo párrafo es de mucha trascendencia y muy prometedor para la industria. Hoy en día sólo existe un mercado con activos virtuales utilizados como subyacentes en el mundo regulado a nivel federal, el que se encuentra en los Estados Unidos de América con la CFTC como la autoridad responsable³⁰⁸. La implementación responsable de este apartado, y de las

³⁰⁸ (Giancarlo, 2018)

eventuales disposiciones de carácter general, podrían detonar el espacio y traer grandes cantidades de dinero institucional a los intercambios. Por medio de instrumentos financieros más sofisticados puede que inversionistas con un perfil tradicional se sientan más cómodos con productos conocidos y estén menos renuentes a involucrarse con ellos. Paralelamente, la implementación de futuros, por ejemplo, traería mayor visibilidad sobre lo que sucede en el mercado mexicano de activos virtuales, como lo que sucedió con la CFTC.

El siguiente artículo es el 34, que se copia para su estudio:

Artículo 34.- Las ITF que operen con activos virtuales deberán divulgar a sus Clientes, además de lo previsto en esta Ley, los riesgos que existen por celebrar operaciones con dichos activos, lo que deberá incluir, como mínimo, informarles de manera sencilla y clara en su página de internet o medio que utilice para prestar su servicio, lo siguiente:

- I. El activo virtual no es moneda de curso legal y no está respaldado por el Gobierno Federal, ni por el Banco de México;
- II. La imposibilidad de revertir las operaciones una vez ejecutadas, en su caso;
- III. La volatilidad del valor del activo virtual, y
- IV. Los riesgos tecnológicos, cibernéticos y de fraude inherentes a los activos virtuales.

El artículo 34 establece un número de advertencias que las ITF deben dar a sus clientes a manera de protección. Si bien poner sobre aviso al público de ciertas particularidades que presenta el ecosistema es responsable, se deben de hacer una aclaración. Los fraudes no son inherentes a los activos virtuales, entendiendo

inherente como inseparable. Si bien es cierto que, al ser una industria de muy reciente creación, poco regulada y en la cual hay muchos sujetos ignorantes de la misma, se presta a esquemas fraudulentos, de ahí hay un gran camino a decir que los fraudes son una parte innata de los activos virtuales.

VII. Conclusiones

El objetivo primordial de la presente tesis fue señalar que el acercamiento de la legislación mexicana al fenómeno regulatorio de los activos virtuales no fue el óptimo y en ese sentido, indicar las áreas de mejora del marco regulatorio. Lo anterior para contribuir en la construcción de soluciones para el fortalecimiento de la industria.

Para cumplir con el propósito de trabajo, en primer lugar, el documento se adentró en el origen y funcionamiento del primer activo virtual, bitcoin. Por lo tanto, en el Capítulo titulado “Bitcoin” fueron exploradas las características y particularidades del cripto-activo del mismo nombre. A lo largo del apartado, se expuso que se trata de un activo fundamentalmente diferente a lo visto en el sistema financiero tradicional. Tanto desde el punto de vista conceptual, al buscar ser un sistema de traslado de valor a distancia sin que la transacción tuviera que ser procesada por un intermediario financiero confiable, como desde el punto de vista técnico, dado que combinó una serie de tecnologías para crear un protocolo que sostuviera dichos traslados de valor. En resumidas cuentas, el capítulo se adentró en el funcionamiento del Bitcoin en un intento de entenderlo y así evaluar las normas que lo regulan.

El nivel de detalle al cual se analizó Bitcoin es necesario por dos razones principales. La primera es que Bitcoin es clave para entender a la mayoría de cripto-activos posteriores. Una vez que se comprende su funcionamiento es mucho más sencillo saber que son y cómo funcionan los activos que vinieron después. Asimismo, un conocimiento técnico detallado de Bitcoin permite a quien lo posee entender la verdadera revolución que suponen los activos criptográficos, reconociendo en que son similares a figuras existentes, y por lo tanto susceptibles a la misma regulación, y en que son diferentes, entendiendo que plantean ciertos problemas no resueltos por la regulación existente.

Posteriormente, en la sección titulada “La Evolución del Protocolo” se exploró cómo en un inicio se le intentaron dar diferentes usos a la red que permitía el traslado de bitcoins; empero, pronto fueron obvias sus limitaciones dado su diseño. Es por esto por lo que surge la plataforma Ethereum, la cual se basa en la misma tecnología que Bitcoin, pero es una implementación mucho más versátil del protocolo original.

De nueva cuenta, se debe de justificar el estudio detallado que se hizo de Ethereum. Primeramente, la plataforma es clave si se quiere entender el fenómeno de los *ICOs*, ya que sin ella no es posible pensar en la burbuja que se presentó a finales del año 2017 y que representó un antes y un después para el mundo de los cripto-activos. Asimismo, los principios sobre los cuales descansa el proyecto son similares a los que permiten el funcionamiento de activos virtuales de nueva generación. Por otro lado, su análisis es fundamental para entender las diferencias entre diferentes tipos de activos virtuales, como entre Bitcoin (sistema de pagos descentralizado) y el mismo Ethereum (computadora descentralizada global).

Teniendo en cuenta lo anterior, se debe de mencionar que el apareamiento de Ethereum fue un parteaguas para el cripto-espacio, al hacer posible la emisión de *tokens* o sub-monedas. Una de las características novedosas de estos, es que se “montan” en la cadena de Ethereum, por lo que los *tokens* no requieren de una infraestructura propia, facilitando en gran medida el proceso de su emisión. Además, los *tokens* pueden ser utilizados para diversos fines, como permitir el uso de un producto o servicio, servir como medio de pago dentro de un ecosistema en concreto o únicamente fondear el proyecto.

Paralelamente, más adelante en el capítulo, se abordó cómo es que surgió un nuevo esquema para distribuir *tokens* conocido como *ICO*, en el que prácticamente cualquier persona podía participar y a través del cual se recaudaban grandes cantidades de dinero. Igualmente, se exploró como es que dichas actividades se volvieron cada vez más reguladas en la medida que captaban la atención de las autoridades.

De la misma forma, en la siguiente sección, se planteó como con la llegada de activos virtuales cada vez más sofisticados resultó difícil encasillarlos dentro de una sola categoría. Como consecuencia de este nuevo fenómeno, surgió la necesidad de definir y diferenciar lo siguiente: en primer lugar, que el concepto de activos virtuales como conjunto es fundamentalmente diferente a los activos existentes. La segunda, que no todos los activos son iguales, siendo necesario aceptar que son diferentes unos a otros. Por lo que, primeramente, fue necesaria la creación de un término suficientemente amplio que permitiera englobar dichos conceptos, pero que fuera lo suficientemente preciso para cargar algún significado e importancia. En un intento de resolver la segunda cuestión, los autores C. Burniske y J. Tatar plantearon una categorización que dividía a los cripto-activos en tres categorías principales, que después serían expandidas a cuatro. Asimismo, se reconocía que hay diferencias en cuanto a uso y diseño entre “criptos” y que no era posible encasillarlos de manera permanente en una sola clasificación, debido a que esta podía cambiar dependiendo de la evolución de cada activo.

El hecho de reconocer diferencias entre activos debió traer grandes consecuencias en materia regulatoria al propugnar por una reglamentación diferente para cada clase de activo; sin embargo, mientras que en ciertas jurisdicciones se tomó en cuenta lo anterior, en otros casos fue ignorado.

En el siguiente apartado se abordó como las agencias reguladoras de los EE. UU. decidieron tomar el segundo camino. La SEC equiparó a la gran mayoría de *ICOs* con una oferta de valores; a los *tokens* emitidos a través de ellos como valores y los intercambios en los que se comerciaban como plataformas de operación de valores. Todo ello con consecuencias regulatorias. A su vez, FinCEN entendió a las plataformas de intercambio como MSB. La decisión se presenta como un error dado que la naturaleza de un intercambio simplemente no es compatible con la de un servicio de transmisión de dinero y por lo tanto, operar bajo dicho esquema presenta grandes inconvenientes, como la obligación de obtener un permiso a nivel estatal.

Por último, la CFTC equiparó al bitcoin como una *commodity* al considerarlo como un subyacente en un contrato de futuros. Estos encasillamientos son contradictorios y no permiten una operación adecuada de las plataformas de intercambios al propiciar un ambiente de incertidumbre. Claramente, hubo un entendimiento desacertado acerca del fenómeno por parte de las autoridades estadounidenses, dado que si bien hay ciertos casos donde proyectos que involucren activos virtuales son muy similares a esquemas existentes, en otros, se presenta una verdadera innovación que reclama ser abordada de manera diferente desde el punto de vista regulatorio. Adicionalmente, es evidente que al día de hoy no existen consensos acerca de como regular el cripto-espacio.

Seguidamente, en el capítulo “Panorama Nacional”, se estudió el caso mexicano. En esta sección se intentó mostrar, en primer lugar, como hubo una evolución en la actitud de las autoridades respecto a los activos virtuales. Primeramente, por parte del SAT, se establecieron restricciones al uso de activos virtuales similares al efectivo, en concordancia con la LFPIORPI por parte de las autoridades fiscales. Esto representó una limitación sumamente problemática considerando que no hay manera de establecer de manera cierta el precio en moneda nacional de un activo virtual, situación discutida en el Capítulo VI Sección 1.1. Más tarde, se mostró la actitud de instituciones como el Banco de México, el cual después tendría facultades regulatorias amplias sobre los activos virtuales, de acuerdo con la LRITF.

En el primer comunicado del Banco de México, se puede percibir un acercamiento con excesivo recelo, repitiendo advertencias hacia la volatilidad y el no respaldo de los activos. No obstante, en un aviso ulterior emitido por la CNBV, la SHCP y el mismo Banco se dio un reconocimiento tácito de los diversos tipos de activos; por ejemplo, aceptando la existencia de *tokens* de utilidad.

De igual manera, fueron abordadas las leyes que sufrieron modificaciones a causa de la promulgación de la llamada Ley Fintech. Dentro de la multitud de ordenamientos, uno de gran importancia es la LFPIORPI en su artículo 17, discutido

en la división VI.3., que contiene disposiciones respecto a activos virtuales y los casos en los cuales operaciones que los involucren pueden ser clasificadas como actividades vulnerables.

En seguida, se exploraron diversas disposiciones de la LRITF que tuvieran relación con los activos virtuales en el Capítulo VI.4. Primeramente, se dio un análisis de las IFC, las cuales podrían ser enormemente relevantes para el cripto-espacio dado que, existe la posibilidad de que esta figura pueda ser utilizada como una plataforma para la emisión de *tokens*. De igual manera, se presenta como un gran acierto el no clasificar como valores a los *tokens* emitidos por medio de esa figura, aún si su única función es capitalizar un proyecto. Gracias a esa disposición, los activos virtuales estarán sujetos a mucha mayor flexibilidad regulatoria, contrario a lo que sucede en los EE. UU. Lo anterior es contingente, claro está, a lo que establezcan las autoridades, en este caso la CNBV, en las disposiciones de carácter general emitidas con posterioridad.

En el caso de las IFPE, presentadas en el apartado VI.4.2., se dio un profundo estudio derivado de la importancia que presenta esta figura para la operación de activos virtuales en México. Su relevancia deriva de que, si bien es posible que diversos entes operen con activos virtuales, como las EF o las IFC, ésta es la figura a la que se tendría que recurrir si se desea constituir un intercambio.

Se debe de mencionar, que a pesar de que la reglamentación de la institución presenta ciertos inconvenientes; se trata de un paso en la dirección correcta. Uno de los mayores aciertos, en comparación con el vecino país del norte, es que en México un intercambio tiene certeza regulatoria. En contraste, las agencias regulatorias de los EE. UU., impiden que los intercambios puedan operar con absoluta seguridad y les obliga a registrarse como un MSB. En el mismo orden de ideas, se presenta la dificultad que representará el echar a andar un intercambio descentralizado; ya que, aunque parecería que las disposiciones relacionadas con las IFPE podrían ser aplicables a esta misma figura, en este trabajo es defendido

que la naturaleza de un intercambio descentralizado es contraria a lo dispuesto en las disposiciones de una IFPE.

Por último, en el apartado “De las Operaciones con Activos Virtuales” se analizó a detalle el capítulo de la LRITF del mismo nombre, iniciando con el artículo 30, al cual se le hicieron múltiples críticas. Una de las más importantes es el reproche que se hace de la definición errónea que se les da a los activos virtuales. En un intento de aportar a la discusión, junto con la respectiva crítica se propone una clasificación de activos virtuales con regulación diferenciada para cada categoría. Se expone una clasificación dúctil que podrían seguir las autoridades que permitiría mantener cierto control, sin obstaculizar el desarrollo de la tecnología. Igualmente, otro aspecto criticado son las facultades que tiene el Banco de México para autorizar la operación de activos virtuales por parte de las ITF. Dichas facultades se clasifican como contradictorias, inútiles, imprácticas e incluso contraproducentes. Al respecto, se sugiere seguir las mejores prácticas internacionales en la materia, tal como las marcadas por ONG como Coin Center.

En el apartado siguiente, se hacen observaciones relativas a algunos intercambios que tendrán que cambiar su operación para cumplir con la normativa. A la par, se cuestiona lo establecido en el artículo 32, en el cual se le otorga una serie de facultades a Banxico que le permitirían “determinar” las características de un activo virtual. Por último, se concluye con los artículos 33 y 34 que hablan sobre la posibilidad de productos financieros derivados y la imposibilidad de que los operadores que resguardan los activos virtuales dispongan de aquellos que son propiedad de los usuarios.

En este punto, es justo afirmar que en diversos puntos la LRITF es adecuada, como en el planteamiento de reglamentar a los operadores de activos virtuales en lugar de regular a los activos directamente, o en cuanto a que la ley no limita el uso o compraventa entre particulares de activos virtuales, siempre y cuando las transacciones no sean de manera habitual y o profesional. A la par, es notable el

esfuerzo de emitir un marco jurídico hecho a la medida de la industria, en lugar de adecuar el existente. No obstante, también puede aseverarse sin temor a caer en un error que la ley presenta grandes áreas de mejora en la sección relativa a la operación de activos virtuales. Esto trae, paradójicamente, la consecuencia de que la ley aumente el riesgo de comerciar con activos virtuales en ciertos aspectos.

Una de las causas raíz de los problemas regulatorios que se dependen de la ley es un entendimiento equivocado del cripto-espacio. Es necesario que las agencias gubernamentales, de México y del mundo, entiendan que los problemas relacionados con activos virtuales no se deben solamente a la falta de regulación, sino que son ocasionados en gran medida por la ignorancia de los involucrados en la materia. Una solución viable al problema anterior consiste en un acercamiento multifacético; similar el emprendido por la agencia estadounidense CFTC. Como es discutido en la sección V.1.2., la institución está realizando el mayor esfuerzo pedagógico en su historia por educar a la población respecto a los potenciales peligros y beneficios de los activos virtuales.

Aquel que desee involucrarse con este tipo de activos debe de entender que hay un riesgo inherente a ellos; sin embargo, también debe comprender que no necesariamente es el del fraude. Por lo tanto, es necesario reiterar que se trata de una tecnología sumamente reciente y el conocimiento de ésta entre el público es limitado; no obstante, la falta de educación no puede ser suplida por un exceso de regulación. En otras palabras, si lo que en verdad se desea es proteger al público, es necesario hacer un esfuerzo por educarlo respecto al tema.

Paralelamente, las autoridades deben de ser muy cuidadosas de no caer en esquemas de sobrerregulación que lejos de proteger a la colectividad, den la impresión a ciertos clientes de encontrarse más protegidos de lo que en realidad están. Consiguientemente, las leyes nuevas no analizadas a profundidad pueden agregar a la confusión en el sector y hacer más difícil la operación de las empresas

manejan activos virtuales además de añadir costos innecesarios³⁰⁹ a la operación de empresas que manejan activos virtuales. Un ejemplo de ello, en el caso mexicano, es que, por la premura de emitir una ley en la materia, se dejaron fuera de la LRITF temas claves del cripto-espacio, como una reglamentación específica de los *ICOs*. Asimismo, no fue posible plasmar en la ley el resultado de la discusión respecto a los diferentes tipos de tokens que se dio en EE. UU. y Suiza.

En otro orden de ideas, es de vital importancia que el regulador entienda que el negocio del intercambio de activos virtuales tiene una naturaleza móvil, lo que implica que el servicio se puede prestar desde cualquier parte del mundo donde exista una conexión a internet. Por lo tanto, las autoridades deben de ser especialmente cuidadosas en no propiciar una fuga de dichos negocios; por el contrario, sería conveniente diferenciar el panorama mexicano creando incentivos que atraigan la inversión. Además, es transcendental que las autoridades no caigan en el error de pensar que es posible limitar la operación de ciertos activos virtuales con mucha popularidad. Es clave recordar que los cripto-activos fueron creados para resistir la regulación; y si bien ésta es necesaria, un exceso de ella podría empujar a los usuarios a la clandestinidad o imponer barreras de entrada tan altas que impidan la competencia o causen la huida de los operadores existentes.

Por otra parte, es notorio que existe una enorme preocupación por parte del regulador con relación a la posibilidad de que los activos virtuales puedan ser usados en esquemas de fraude, lavado de dinero o financiamiento de grupos criminales. Si bien es muy importante que el Estado muestre una reacción proporcionada a este fenómeno, resulta alarmante ver la respuesta legislativa que ha existido sin que siquiera se haya dado un caso de involucramiento directo de activos virtuales con actividad criminal en territorio mexicano. Teniendo en cuenta lo anterior, es preocupante pensar qué acciones tomarán las autoridades cuando un acontecimiento del estilo efectivamente suceda. En cuanto al fraude, surge la pregunta si es un problema que se debe de intentar resolver en la LRITF, o cualquier

³⁰⁹ (Orcutt, 2018)

otra legislación específica del sector. Existe legislación anterior, la contenida en los códigos penales, que ataca directamente el problema. Antes de tomar decisiones precipitadas los reguladores deben de ser pacientes con la industria y observar que rumbo toma ésta, observando las particularidades del mercado mexicano y evitar a toda costa saltar a conclusiones en materia de delitos.

El reto en la materia no es menor y el acercamiento regulatorio debe de ser cauteloso; priorizando temas como la protección al público, ya sea que se le considere inversionista o consumidor, y la prevención en materia de lavado de dinero o financiamiento de grupos criminales. Asimismo, se debe procurar mantener al mínimo la discrecionalidad y buscar un balance entre protección e inclusión. Mientras tanto, es fundamental que las autoridades responsables se sigan familiarizando con la tecnología y mantengan una debida coordinación.

Subsecuentemente, es necesario seguir construyendo en aspectos clave para la industria de intercambios de activos virtuales. Algunos de estos son: mecanismos claros para selección de activos listados, velocidad de ejecución de órdenes, interfaz del usuario amigable, mercados en línea las veinticuatro horas; completa transparencia en materia de costos, riesgos, restricciones y limitaciones, mecanismos internos de control, seguridad informática además de protección de vanguardia en materia de datos personales y activos virtuales. Estos puntos deben de ser considerados, si bien no reglamentados rigurosamente, ya que son de suma importancia para los propios miembros de la industria a nivel internacional³¹⁰.

Es probable que estemos frente a una revolución financiera sin precedentes. En consecuencia, existe la oportunidad de descentralizar el poder financiero en beneficio del público y ésta debe de ser aprovechada. Tal como en muchas otras áreas del conocimiento, hay avances que permiten ser optimistas respecto al futuro y puede que los activos virtuales hagan lo propio para el mundo financiero.

³¹⁰ (Powell, 2018)

Por último, se concluye el presente trabajo con una frase del presidente de la CFTC J. Christopher Giancarlo expresada en una comparecencia frente al Senado de los EE. UU. en 2018, que bien podría resumir lo planteado en esta tesis: “Les debemos a las nuevas generaciones respetar su entusiasmo respecto a las cripto-monedas con una respuesta regulatoria considerada y balanceada, no con rechazo o descarte; sin embargo, debemos de castigar duramente a aquellos que intenten abusar de ese entusiasmo mediante fraude y manipulación.” [sic.]

VIII. Bibliografía

A lo largo del trabajo fue utilizado el sistema Harvard – Anglia 2008 de citación.

Libros

Antonopoulos, A. M., 2017. *Mastering Bitcoin*. 2ª edición ed. Sebastopol: O'Reilly.

Batiz-Benet, J., Santori, M. & Clayburgh, J., 2017. *The SAFT Project: Toward a Compliant Token Sale Framework*.: Protocol Labs.

Burniske, C. & Tatar, J., 2018. *Cryptoassets: The Innovative Investor's Guide to Bitcoin and Beyond*. 1ª edición ed. New York: Mc Graw Hill Education.

Burniske, C. & White, A., 2017. *Bitcoin: Ringing the Bell for a New Asset Class*, New York: Ark Invest Research.

Maupin, J., 2017. *Blockchains and the G20: Building an Inclusive, Transparent and Accountable Digital Economy*, Waterloo: Centre for International Governance Innovation.

Poelstra, A., 2016. *A Treatise on Altcoins*. [En línea] Disponible en: <https://download.wpsoftware.net/bitcoin/alts.pdf> [Último acceso: 28 Febrero 2018].

Real Academia Española; Consejo General del Poder Judicial, 2016. *Diccionario del Español Jurídico*. 1ª edición ed. Barcelona: Espasa Libros.

Real Academia Española, 2014. *Diccionario de la Lengua Española*. 23ª edición ed. Madrid: Espasa Calpe.

Schueffel, P., 2017. *The Concise Fintech Compendium*. 1ª edición ed. Friburgo: School of Management Fribourg // University of Applied Sciences and Arts Western Switzerland.

Van Valkenburgh, P., 2016. *Framework for Securities Regulation of Cryptocurrencies v1*, Washington D.C.: Coin Center.

Fuentes Hemerográficas

Chohan, U. W., 2017. Initial Coin Offerings (ICOs): Risks, Regulation, and Accountability. *Notes on the 21st Century*.

Chohan, U. W., 2017. The Double-Spending Problem and Cryptocurrencies. *Notes on the 21st Century*.

Commodity Futures Trading Commission, 2017. Review and Compliance Checklist for virtual currency product self-certifications.pdf. *Federal Register*, 82(243), pp. 60335-60341.

Bonneau, J. y otros, 2015. *SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies*. San Jose, IEEE Symposium on Security and Privacy, pp. 104-121.

Greer, R., 1997. What is an Asset Class, Anyway?. *The Journal of Portfolio Management*, 23(2), pp. 86-91.

Hayes, A. S., 2017. Cryptocurrency Value Formation: An empirical study leading to a cost of production model for valuing Bitcoin. *Telematics and Informatics*, 34(7), pp. 1308-1321.

Howden, E., 2015. The Crypto-Currency Conundrum: Regulating an Uncertain Future. *Emory International Law Review*, 29(4), pp. 742-798.

IETF, 2018. *IETF*. [En línea] Disponible en: <https://www.ietf.org/standards/rfcs/>

Möser, M. e. a., 2018. An Empirical Analysis of Traceability in the Monero Blockchain. *Proceedings on Privacy Enhancing Technologies*, Volumen 1, pp. 1-21.

Testimonios

Antonopoulos, A. M., 2014. *Opening Remarks—Canadian Senate Testimony on Bitcoin*. [En línea] Disponible en: <https://decentralize.today/opening-remarks-canadian-senate-testimony-on-bitcoin-eb77f696ee5e>

[Último acceso: 18 Abril 2018].

Clayton, J., 2018. *Testimony on “Virtual Currencies: The Oversight Role of the U.S. Securities and Exchange Commission and the U.S. Commodity Futures Trading Commission”*, Washington D.C.

Comité de Banca, Vivienda y Asuntos Urbanos, 2018. *Virtual Currencies: The Oversight Role of the U.S. Securities and Exchange Commission and the U.S. Commodity Futures Trading Commission*. [En línea] Disponible en: <https://www.banking.senate.gov/public/index.cfm/2018/2/virtual-currencies-the-oversight-role-of-the-u-s-securities-and-exchange-commission-and-the-u-s-commodity-futures-trading-commission> [Último acceso: 6 Marzo 2018].

Giancarlo, J. C., 2018. *Written Testimony of J. Christopher Giancarlo Chairman, Commodity Futures Trading Commission Before the Senate Banking Committee*, Washington, D.C.

Massad, T., 2014. *Testimony of CFTC Chairman Timothy Massad before the U.S. Senate Committee on Agriculture, Nutrition and Forestry, Washington, D.C.*

[En línea]

Disponible en: <https://www.irs.gov/pub/irs-drop/n-14-21.pdf>

[Último acceso: 6 Marzo 2018].

Reportes de Autoridades

Banxico; CNBV; SHCP, 2017. *Las autoridades financieras advierten de los riesgos asociados al uso de activos virtuales y a la participación en los esquemas de inversión conocidos como Oferta Inicial de Monedas o "Initial Coin Offerings.*

[En línea] Disponible en:

[https://www.gob.mx/cms/uploads/attachment/file/280134/Prensa Bitcoin IC OS v21Nov2017 v4 CNBV DGDR 004 -DGJ.pdf](https://www.gob.mx/cms/uploads/attachment/file/280134/Prensa_Bitcoin_ICOS_v21Nov2017_v4_CNBV_DGDR_004_-DGJ.pdf)

[Último acceso: 12 Abril 2018].

Banco de México, 2014. *Advertencias sobre el uso de activos virtuales como sucedáneos de los medios de pago en moneda de curso lega.* [En línea]

Disponible en: [http://www.banxico.org.mx/informacion-para-la-prensa/comunicados/miscelaneos/boletines/%7B5D9E200E-2316-A4B8-](http://www.banxico.org.mx/informacion-para-la-prensa/comunicados/miscelaneos/boletines/%7B5D9E200E-2316-A4B8-92A9-3A5F74938B87%7D.pdf)

[92A9-3A5F74938B87%7D.pdf](http://www.banxico.org.mx/informacion-para-la-prensa/comunicados/miscelaneos/boletines/%7B5D9E200E-2316-A4B8-92A9-3A5F74938B87%7D.pdf) [Último acceso: 7 Abril 2018].

CFTC Backgrounder on Oversight of and Approach to Virtual Currency Futures Markets, CFTC, 2018. *CFTC Backgrounder on Oversight of and Approach to Virtual Currency Futures Markets.* [En línea] Disponible en:

http://www.cftc.gov/idc/groups/public/@newsroom/documents/file/backgrounder_virtualcurrency01.pdf [Último acceso: 15 Marzo 2018].

CFTC, *CFTC Orders Bitcoin Options Trading Platform Operator and its CEO to Cease Illegally Offering Bitcoin Options and to Cease Operating a Facility for Trading or Processing of Swaps without Registering* (2015).

Comisiones Unidas de Hacienda y Crédito Público, de Ciencia y Tecnología y de Estudios Legislativos, 2017. *Dictamen de Iniciativa de Decreto de la Ley para Regular las Instituciones de Tecnología Financiera.* Ciudad de México.

European Securities and Markets Authority, 2017. *ESMA alerts investors to the high risks of Initial Coin Offerings (ICOs)*.

FinCEN, 2013. *Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies*. [En línea] Disponible en: <https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-persons-administering> [Último acceso: 6 Marzo 2018].

FinCEN, 2014. *Application of FinCEN's Regulations to Virtual Currency Mining Operations*. [En línea] Disponible en: <https://www.fincen.gov/resources/statutes-regulations/administrative-rulings/application-fincens-regulations-virtual-0> [Último acceso: 14 Marzo 2018].

Financial Action Task Force, 2014. *Virtual Currencies Key Definitions and Potential AML/CFT Risks*, Paris: FATF/OECD.

FINMA, 2017. *FINMA Guidance 04/2017 Regulatory treatment of initial coin offerings*, Berna.

FINMA, 2018. *Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs)*, Berna.

Internal Revenue Service, 2014. *IRS Virtual Currency Guidance: Virtual Currency Is Treated as Property for U.S. Federal Tax Purposes; General Rules for Property Transactions Apply*. [En línea] Disponible en: <https://www.irs.gov/pub/irs-drop/n-14-21.pdf> [Último acceso: 6 Marzo 2018].

Internal Revenue Service, 2014. *Notice 2014–21 IRS Virtual Currency Guidance, Internal Revenue Bulletin: 2014-16*. [En línea] Disponible en: <https://www.irs.gov/pub/irs-drop/n-14-21.pdf> [Último acceso: 27 febrero 2018].

OFAC, 2017. *Questions on Virtual Currency*. [En línea] Disponible en: https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_compliance.aspx#vc_faqs [Último acceso: 15 Abril 2018].

SEC's Office of Investor Education and Advocacy, 2016. *Updated Investor Alert: Fraudulent Stock Promotions*. [En línea] Disponible en: <https://investor.gov/news-alerts/investor-alerts/investor-alert-fraudulent-stock-promotions>

Securities and Exchange Commission, 2017. *Company Halts ICO After SEC Raises Registration Concerns*. [En línea] Disponible en: <https://www.sec.gov/news/press-release/2017-227> [Último acceso: 8 Marzo 2018].

Securities and Exchange Commission, 2017. *SEC Exposes Two Initial Coin Offerings Purportedly Backed by Real Estate and Diamonds*. [En línea] Disponible en: <https://www.sec.gov/news/press-release/2017-185-0> [Último acceso: 8 Marzo 2018].

Securities and Exchange Commission, 2018. *SEC Halts Alleged Initial Coin Offering Scam*. [En línea] Disponible en: <https://www.sec.gov/news/press-release/2018-8> [Último acceso: 8 Marzo 2018].

Securities and Exchanges Commission, 2017. *Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO*.

SEC Division of Enforcement and SEC Office of Compliance Inspections and Examinations, 2017. *SEC Statement Urging Caution Around Celebrity Backed ICOs*. [En línea] Disponible en: <https://www.sec.gov/news/public-statement/statement-potentially-unlawful-promotion-icos>
[Último acceso: 2 Marzo 2018].

Servicio de Administración Tributaria, 2015. *Respecto a la utilización de Activos Virtuales en los actos u operaciones establecidos en el artículo 32 de la Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita (LFPIORPI)*. [En línea] Disponible en: <https://sppld.sat.gob.mx/pld/interiores/noticias.html>
[Último acceso: 2018 Marzo 8].

Artículos Sitios Web

Catalini, C., 2017. *How Blockchain Applications Will Move Beyond Finance*. [En línea] Disponible en: <https://hbr.org/2017/03/how-blockchain-applications-will-move-beyond-finance> [Último acceso: 15 Febrero 2018].

Akita, F., 2017. *How does Bitcoin force consensus among Byzantine generals?*. [En línea] Disponible en: <http://www.akitaonrails.com/2017/11/01/how-does-bitcoin-force-consensus-among-byzantine-generals> [Último acceso: 1 Febrero 2018].

Barnett, C., 2017. *Inside the Meteoric Rise of ICOs*. [En línea] Disponible en: <https://www.forbes.com/sites/chancebarnett/2017/09/23/inside-the-meteoric-rise-of-icos/#4031a2df5670> [Último acceso: 22 Febrero 2018].

Berg, C., Davidson, S. & Potts, J., 2017. *The Blockchain Economy: A beginner's guide to institutional cryptoeconomics*. [En línea] Disponible en: <https://medium.com/@cryptoeconomics/the-blockchain-economy-a-beginners-guide-to-institutional-cryptoeconomics-64bf2f2beec4> [Último acceso: 18 Abril 2018].

Bully, C., 2018. *U.S. Securities Issues Surrounding ICO's*. [En línea] Disponible en: <https://twitter.com/cryptobully/status/964985901649743873?s=12> [Último acceso: 9 Marzo 2018].

Darko, E., 2017. *ICO Market Research: The Leading Blockchain Platforms Of 2017*. [En línea] Disponible en: <https://icowatchlist.com/blog/ico-market-research-leading-blockchain-platforms-2017/> [Último acceso: 8 Marzo 2018].

- del Castillo, M., 2017. *A 'Howey Test' for Blockchain? Why the SEC's ICO Guidance Isn't Enough*. [En línea] Disponible en: <https://www.coindesk.com/every-token-snowflake-secs-ico-guidance-isnt-enough/> [Último acceso: 9 Marzo 2018].
- Dixon, C., 2017. *Crypto Tokens: A Breakthrough in Open Network Design*. [En línea] Disponible en: <https://medium.com/@cdixon/crypto-tokens-a-breakthrough-in-open-network-design-e600975be2ef> [Último acceso: 18 Abril 2018].
- Dolan, Z., 2017. *Comments on Structuring Legally Compliant Token Sales*. [En línea] Disponible en: <https://twitter.com/ZoeJDolan/status/933139164647718913> [Último acceso: 19 Abril 2018].
- Eaglesham, J. & Paul, V., 2018. *Cryptocurrency Firms Targeted in SEC Probe*. [En línea] Disponible en: <https://www.wsj.com/articles/sec-launches-cryptocurrency-probe-1519856266> [Último acceso: 8 Marzo 2018].
- Estaño, A. & Tolama, J., 2017. *Los 14 Puntos Más Importantes del Anteproyecto de Ley Fintech*. [En línea] Disponible en: <https://expansion.mx/emprendedores/2017/04/10/los-14-puntos-mas-importantes-del-anteproyecto-de-ley-fintech> [Último acceso: 27 Marzo 2018].
- ghostyeti, 2016. *Interview with "Arvicco" Developer of Ethereum Classic*. [En línea] Disponible en: <https://steemit.com/crypto-news/@ghostyeti/interview-with-arvicco-developer-of-ethereum-classic> [Último acceso: 1 Marzo 2018].
- Hill, B. M., 2005. *To Fork or Not To Fork: Lessons From Ubuntu and Debian*.
- Higgins, S., 2017. *Switzerland Wants to Open a Sandbox to Attract More Blockchain Startups*. [En línea] Disponible en: <https://www.coindesk.com/switzerland-attract-more-blockchain-startups/> [Último acceso: 26 Marzo 2018].

Johnson, S., 2018. *Beyond the Bitcoin Bubble*. [En línea] Disponible en: <https://www.nytimes.com/2018/01/16/magazine/beyond-the-bitcoin-bubble.html?hp&action=click&pgtype=Homepage&clickSource=story-heading&module=first-column-region®ion=top-news&WT.nav=top-news> [Último acceso: 15 Febrero 2018].

Kaal, W., 2018. *Initial Coin Offerings: the top 25 jurisdictions and their comparative regulatory responses*. [En línea] Disponible en: <https://medium.com/@wulfkaal/initial-coin-offerings-the-top-25-jurisdictions-and-their-comparative-regulatory-responses-4b8c9ae7e8e8> [Último acceso: 1 Marzo 2018].

Kasireddy, P., 2017. *How does Ethereum work, anyway?*. [En línea] Disponible en: <https://medium.com/@preethikasireddy/how-does-ethereum-work-anyway-22d1df506369> [Último acceso: 15 Abril 2018].

Leathern, R., 2018. *New Ads Policy: Improving Integrity and Security of Financial Product and Services Ads*. [En línea] Disponible en: <https://www.facebook.com/business/news/new-ads-policy-improving-integrity-and-security-of-financial-product-and-services-ads> [Último acceso: 19 Febrero 2018].

Ludwin, A., 2015. *How Anonymous is Bitcoin?*. [En línea] Disponible en: <https://coincenter.org/entry/how-anonymous-is-bitcoin> [Último acceso: 19 Abril 2018].

Mizrahi, A., s.f. *A blockchain based property ownership recording system*. [En línea] Disponible en: <https://chromaway.com/papers/A-blockchain-based-property-registry.pdf> [Último acceso: 19 Abril 2018].

Morris, D., 2013. *Beyond bitcoin: Inside the cryptocurrency ecosystem*. [En línea] Disponible en: <http://fortune.com/2013/12/24/beyond-bitcoin-inside-the-cryptocurrency-ecosystem/> [Último acceso: 2 Marzo 2018].

Novosti, B., 2016. *A Crypto-Decentralist Manifesto*. [En línea] Disponible en: https://medium.com/@bit_novosti/a-crypto-decentralist-manifesto-6ba1fa0b9ede [Último acceso: 1 Marzo 2018].

Orcutt, M., 2018. *America's cryptocurrency tax policy is confusing everyone*. [En línea] Disponible en: <https://www.technologyreview.com/s/610859/americas-cryptocurrency-tax-policy-is-confusing-everyone/> [Último acceso: 15 Abril 2018].

Orcutt, M., 2018. *States that are passing laws to govern "smart contracts" have no idea what they're doing*. [En línea] Disponible en: https://www.technologyreview.com/s/610718/states-that-are-passing-laws-to-govern-smart-contracts-have-no-idea-what-theyre-doing/amp/?_twitter_impression=true [Último acceso: 15 Abril 2018].

Popper, N., 2017. *A Hacking of More Than \$50 Million Dashes Hopes in the World of Virtual Currency*. [En línea] Disponible en: <https://www.nytimes.com/2016/06/18/business/dealbook/hacker-may-have-removed-more-than-50-million-from-experimental-cybercurrency-project.html> [Último acceso: 1 Marzo 2018].

Popper, N., 2018. *Subpoenas Signal S.E.C. Crackdown on Initial Coin Offerings*. [En línea] Disponible en: <https://www.nytimes.com/2018/02/28/technology/initial-coin-offerings-sec.html> [Último acceso: 8 Marzo 2018].

- Popper, N., 2018. *There Is Nothing Virtual About Bitcoin's Energy Appetite*. [En línea] Disponible en: <https://www.nytimes.com/2018/01/21/technology/bitcoin-mining-energy-consumption.html> [Último acceso: 28 Febrero 2018].
- Powell, J., 2018. *Kraken's Position on Regulation*. [En línea] Disponible en: <https://blog.kraken.com/post/1561/krakens-position-on-regulation/> [Último acceso: 1 Mayo 2018].
- Reuters, 2018. *Swiss task force to look into blockchain oversight*. [En línea] Disponible en: <https://www.reuters.com/article/us-swiss-crypto/swiss-task-force-to-look-into-blockchain-oversight-idUSKBN1F71T6> [Último acceso: 26 Marzo 2018].
- Rizzo, P., 2016. *Ethereum Hard Fork Creates Competing Currencies*. [En línea] Disponible en: <https://www.coindesk.com/ethereum-hard-fork-creates-competing-currencies-support-ethereum-classic-rises/> [Último acceso: 1 Marzo 2018].
- Roberts, J. J., 2017. *Why Bitcoin Splits Are Both a Cash Windfall and a Tax Nightmare*. [En línea] Disponible en: <http://fortune.com/2017/11/16/bitcoin-cash-irs/> [Último acceso: 6 Marzo 2018].
- Van Valkenburgh, P., 2017. *What is "Blockchain" anyway?*. [En línea] Disponible en: <https://coincenter.org/entry/what-is-blockchain-anyway> [Último acceso: 19 Abril 2018].

- Van Valkenburgh, P., 2018. *FinCEN raises major licensing problem for ICOs in new letter to Congress*. [En línea] Disponible en: <https://coincenter.org/link/fincen-raises-major-licensing-problem-for-icos-in-new-letter-to-congress> [Último acceso: 14 Marzo 2018].
- Vigna, P., 2016. *Chiefless Company Rakes In More Than \$100 Million*. [En línea] Disponible en: <https://www.wsj.com/articles/chiefless-company-rakes-in-more-than-100-million-1463399393> [Último acceso: 1 Marzo 2018].
- Wang, K., 2017. *Governance in Blockchain Part I: The Bitcoin Experiment*. [En línea] Disponible en: <https://itnext.io/governance-in-blockchain-part-i-the-bitcoin-experiment-a8c633791e6d> [Último acceso: 1 Febrero 2018].
- Wilcox, Z. & Van Valkenburgh, P., 2016. *What is Zcash?* [En línea] Disponible en: <https://coincenter.org/entry/what-is-zcash> [Último acceso: 19 Abril 2018].
- Zamyatin, A., 2017. *On sharding blockchains*. [En línea] Disponible en: <https://github.com/ethereum/wiki/wiki/Sharding-FAQ> [Último acceso: 31 Enero 2018].

Artículos Noticiosos

Becerra, J., 2018. "Lava" crimen rastro con criptomonedas. *Reforma*, 10 Abril, p. 2.

De, N., 2018. *Swiss Government Supports Launch Blockchain Task Force*. [En línea] Disponible en: <https://www.coindesk.com/swiss-government-launches-blockchain-task-force/> [Último acceso: 26 Marzo 2018].

Hertig, A., 2017. *Crypto Collectables? Ethereum's Next Killer App Is on Its Way*. [En línea] Disponible en: <https://www.coindesk.com/crypto-collectables-ethereums-next-killer-app-is-on-its-way/> [Último acceso: 21 Febrero 2018].

Actas de Conferencia

Ethereum Foundation, 2016. *Ethereum Developer Conference, 2016 September 19 - 21, Shanghai, China. Vitalik Buterin, describes Ethereum*. [En línea] Disponible en: <https://www.youtube.com/watch?v=66SaEDzImP4&t=26s> [Último acceso: 20 Febrero 2018].

Newsome, J., Shi, E., Song, D. & Perrig, A., 2004. *The Sybil Attack in Sensor Networks: Analysis & Defenses*. Berkeley, Third International Symposium on Information Processing in Sensor Networks.

Wood, G., 2015. *DEVCON1 - Participación Dr. Gavin Wood*.

Casos

Securities and Exchange Commission v. W. J. Howey Co. (1946).

CFTC, 2016. *BFXNA INC. d/b/a BITFINEX.* [En línea] Disponible en: <https://www.cftc.gov/sites/default/files/idc/groups/public/@lrenforcementactions/documents/legalpleading/enbfxnaorder060216.pdf> [Último acceso: 21 Febrero 2018]

Marco Jurídico Mexicano

Ley para Regular las Instituciones de Tecnología Financiera

Ley de Instituciones de Crédito

Ley del Mercado de Valores

Ley General de Organizaciones y Actividades Auxiliares del Crédito

Ley para la Transparencia y Ordenamiento de los Servicios Financieros

Ley para Regular las Sociedades de Información Crediticia

Ley de Protección y Defensa al Usuario de Servicios Financieros

Ley para Regular las Agrupaciones Financieras

Ley de la Comisión Nacional Bancaria y de Valores

Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita

Documentos Técnicos

Anon., 2017. *Ethereum Homestead Documentation*, Ethereum community.

bitcoinwiki, 2016. *Prohibited Changes*. [En línea] Disponible en: https://en.bitcoin.it/wiki/Controlled_supply [Último acceso: 27 Febrero 2018].

bitcoinwiki, 2017. *Multisignature*. [En línea] Disponible en: <https://en.bitcoin.it/wiki/Multisignature> [Último acceso: 20 Febrero 2018].

bitcoinwiki, 2011. *Nonce*. [En línea] Disponible en: <https://es.bitcoin.it/wiki/Nonce> [Último acceso: 29 Enero 2018].

Buterin, V., 2013. *Ethereum White Paper*.

Buterin, V., 2016. *Hard Fork Completed*. [En línea] Disponible en: <https://blog.ethereum.org/2016/07/20/hard-fork-completed/> [Último acceso: 1 Marzo 2018].

ethers, 2017. *GitHub*. [En línea] Disponible en: <https://github.com/ethereum/EIPs/issues/16>

Hesiod Services LLC, 2013. *Bitcoin Mining*. [En línea] Disponible en: <https://www.bitcoinmining.com/> [Último acceso: 29 01 2018].

Khatwani, S., 2017. *Bitcoin Wallet: Everything a Beginner Needs to know*. [En línea] Disponible en: <https://coinsutra.com/bitcoin-wallet/> [Último acceso: 2 Marzo 2018].

Khatwani, S., 2018. *Bitcoin Private Keys: Everything You Need To Know*. [En línea]
Disponible en: <https://coinsutra.com/bitcoin-private-key/>
[Último acceso: 2 Marzo 2018].

Nakamoto, S., 2008. *Bitcoin: A Peer-to-Peer Electronic Cash System*.

Rosenfeld, M., 2012. *Overview of Colored Coins*. [En línea]
Disponible en: <https://bitcoil.co.il/BitcoinX.pdf> [Último acceso: 2 Marzo 2018].

Vogelsteller, F., 2015. *Git Hub*. [En línea]
Disponible en: <https://github.com/ethereum/EIPs/issues/20>

Wikimedia: The Free Encyclopedia, 2018. *Hash Function*. [En línea]
Disponible en: https://en.wikipedia.org/wiki/Hash_function [Último acceso: 31
Enero 2018].

Páginas Web de Referencia

Coindesk, 2018. *Bitcoin (USD) Price*. [En línea] Disponible en: <https://www.coindesk.com/price/> [Último acceso: 2 Abril 2018].

Anon., *Blockchain.info*. [En línea] Disponible en: <https://blockchain.info/es/charts/n-transactions-per-block> [Último acceso: 25 Enero 2018].

Brownworth, A., 2017. *Blockchain 101 - A Visual Demo*. [En línea] Disponible en: https://www.youtube.com/watch?v=_160oMzbIY8 [Último acceso: 26 Enero 2018].

Brownworth, A., 2017. *Blockchain 101 - Part 2 - Public / Private Keys and Signing*. [En línea] Disponible en: https://www.youtube.com/watch?v=xIDL_akeras [Último acceso: 26 Enero 2018].

Investopedia, 2016. *Asset*. [En línea] Disponible en: <https://www.investopedia.com/terms/a/asset.asp> [Último acceso: 2 Marzo 2018].

SEC, 2017. *Mission & Responsibilities*. [En línea] Disponible en: <http://www.cftc.gov/About/MissionResponsibilities/index.htm> [Último acceso: 9 Marzo 2018].

Burniske, C. & Tatar, J., 2018. *Cryptoassets – The Rise of a New Asset Class*. [En línea] Disponible en: <https://epicenter.tv/episode/218/>

Van Valkenburgh, P., 2018. *Where US Cryptocurrency Regulation is Heading*. [En línea] Disponible en: <https://epicenter.tv/episode/227/>

Material Adicional Recomendado

Listas de desarrolladores voluntarios del protocolo Bitcoin:
<https://github.com/bitcoin/bitcoin/graphs/contributors>

Código del Protocolo Bitcoin: <https://github.com/bitcoin/bitcoin/graphs/contributors>

Proyecto *Namecoin*: <https://namecoin.org/>

Lista de aplicaciones descentralizadas “*dApps*” creadas en Ethereum:
<https://www.stateofthedapps.com/>

Posibles usos no financieros de la tecnología *blockchain*:
<https://hbr.org/2017/03/how-blockchain-applications-will-move-beyond-finance>

Información adicional acerca de la Fundación Ethereum, organización que mantiene la plataforma del mismo nombre: <https://hbr.org/2017/03/how-blockchain-applications-will-move-beyond-finance>

Información acerca del cambio de un esquema PoW a uno PoS en Ethereum:
<https://blog.ethereum.org/2015/08/01/introducing-casper-friendly-ghost/>

Documentación relacionada con el proceso de programación de un Contrato Inteligente emisor de *tokens* en Ethereum: <https://www.ethereum.org/token>

Historia del Método ERC para mejora de la plataforma Ethereum:
<https://www.ethereum.org/token>

Explorador de la cadena de bloques de Ethereum, lo que permite ver las transacciones registradas en la base de datos: <https://etherscan.io/>

Información acerca del proyecto NEO: <https://etherscan.io/>

Artículo referente a la posible *tokenización* de la economía: <https://etherscan.io/>

Proyecto insignia de la nueva categoría de activo virtuales llamado *CryptoKitties*:
<https://www.cryptokitties.co/> y <https://www.coindesk.com/crypto-collectables-ethereums-next-killer-app-is-on-its-way/>

Pagina web con los recursos puestos a disposición por parte de la CFTC relativos al bitcoin: <http://www.cftc.gov/bitcoin/index.htm>

Índice de referencia que indica el precio de bitcoin:
<http://www.cmegroup.com/trading/cf-bitcoin-reference-rate.html>

Sitio web que muestra los cambios de valor y capitalización del mercado de activos virtuales: <https://coinmarketcap.com/>