Universidad Nacional Autónoma de México

Programa de Posgrado en Ciencias de la Administración

EL ANONIMATO DE *BITCOIN* Y EL LAVADO DE DINERO BAJO LA LEY FINTECH EN MÉXICO COMO PREVENCIÓN DEL LAVADO DE DINERO

T e s i s

Que para optar por el grado de:

Maestra en Finanzas

Presenta:

María del Pilar Márquez Rossano

Tutor:

Dr. Luis Alberto Gómez Alvarado

Facultad de Contaduría y Administración

Ciudad Universitaria, Ciudad de México, noviembre, 2022.

Universidad Nacional Autónoma de México
UNAM
Biblioteca Central
Dirección General de Bibliotecas de la UNAM

UNAM – Dirección General de Bibliotecas
Tesis Digitales
Restricciones de uso

DERECHOS RESERVADOS ©
PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

Dedicatorias

A **Dios,** *por haber hecho posible que alcanzara esta meta.*

Llena de alegría y agradecimiento, con todo mi corazón, le dedico mi Tesis a:

Mi madre A. **Alicia Rossano y Carrera**, *por ser un ejemplo de perseverancia, entrega y tenacidad.*

A mi tío **Armando Rossano** *por su constante apoyo, ánimo y su confianza en mí.*

A mi esposo **Álvaro** *y mi hija* **Greta,** *por su apoyo incondicional y por ser la motivación de mi vida.*

Pilar

Agradecimientos

A mi Alma Mater la ***Universidad Nacional Autónoma de México,*** *por ser mi fuente de inspiración y por formarme como una mujer que actúa bajo sus lineamientos éticos y científicos.*

A la ***Facultad de Contaduría y Administración,*** *División de Estudios de Posgrado, por haberme dado la oportunidad de obtener la formación académica en la Maestría en Finanzas.*

A mis ***maestros,*** *por compartir sus conocimientos y experiencia.*

Al ***Dr. Luis Alberto Gómez Alvarado*** *por su valiosa asesoría en el desarrollo de este trabajo.*

A mis ***sinodales*** *por su valiosa aportación a esta investigación.*

Al ***Dr. Fabián González Flores*** *por las horas dedicadas a discutir y analizar este trabajo.*

A las Maestras ***Rosario Higuera Torres*** *y* ***América Rocío Rivera Díaz*** *por su invaluable apoyo durante la coordinación en el Programa de Posgrado en Ciencias de la Administración.*

Índice General

Cuadros

Figuras

Resumen

El objetivo de esta investigación es identificar cómo se conserva el anonimato en las transacciones con *bitcoin*; evaluar si se vulnera el sistema *blockchain* para lavar dinero proveniente de actividades ilícitas, e identificar si la "Ley *Fintech*" considera aspectos regulatorios que permitan identificar las operaciones de mezcla, transaccionalidad e intercambio en el sistema *blockchain* en prevención y combate al lavado del dinero.

La principal aportación de esta investigación es que se explica desde un punto de vista informático y de manera sencilla, cómo se conserva el anonimato de los usuarios en las transacciones realizadas con *bitcoin* a través del sistema *blockchain*. Se pudo identificar que la forma de conservar el anonimato en las transacciones con *bitcoin*, es a través del intercambio de criptomonedas y servicios de mezcla en redes oscuras, y se pudo comprobar que, éstas técnicas, no vulneran el sistema de *blockchain* para el lavado de activos. Además, a pesar de que se piensa que al realizar una transacción con *bitcoin* y no proporcionar ningún dato personal, se obtiene cierto grado de anonimato, se comprueba, que resultó ser todo lo contrario, ya que gracias a la característica de transparencia de la tecnología *blockchain* y los beneficios que ofrece de integridad, trazabilidad e inmutabilidad; es que, mediante el análisis de *blockchain*, se pueden rastrear los flujos de fondos provenientes de actividades ilícitas, a delincuentes y proveedores de servicio.

También se comprobó que La "Ley *Fintech*", no considera disposiciones que, permitan identificar las operaciones de mezcla e intercambio en el sistema blockchain, en prevención y combate al lavado de dinero.

Esta investigación de tipo cualitativa se divide en cuatro capítulos. Capítulo 1. El riesgo del uso de las criptomonedas para el lavado de dinero. En este capítulo, se abordan los temas sobre las criptomonedas, sus características, uso legítimo, sistema descentralizado, prevención del lavado de dinero, las Recomendaciones del Grupo de Acción Financiera Internacional (GAFI) y la regulación mexicana. Se sientan las bases teóricas para el desarrollo de esta investigación. Capítulo 2. Análisis del impacto *bitcoin* en el ecosistema blockchain. En este capítulo se analiza el funcionamiento del *bitcoin*, el ecosistema *blockchain*, y las empresas *Fintech*. Capítulo 3. Efecto del anonimato de la tecnología *blockchain*. Aquí, describe el funcionamiento de la tecnología *blockchain*, su impacto en el sistema financiero, el uso del anonimato del *bitcoin*, y se hace un análisis de la normativa en prevención del lavado de dinero, donde se discute sobre a quién regular en una transacción con *bitcoin,* se analiza de forma comparativa la normativa de Estados Unidos, Europa y México, y también el alcance de la regulación de la "Ley *Fintech*", terminando con el panorama en México. Capítulo 4. Estudio de Casos. Como resultado, se presenta por cada uno de los casos en estudio, una breve descripción con su discusión y el resultado de la prueba de Hipótesis.

Introducción

Hoy en día, **la innovación tecnológica** -tema de interés para el ámbito económico y social- no excluye a las actividades ilícitas como es el caso del «lavado de dinero» debido a que no sólo afecta a nuestro país, también a la economía global, dado que podría alterar los precios de diferentes bienes y servicios; afectar a la libre competencia impactando a la sociedad al generar pérdidas de empleo y mermas en el crecimiento económico, pues los delincuentes no buscan obtener ganancias propias de un negocio, si no, simplemente ocultar los fondos ilícitos. Esta actividad puede llegar a desestabilizar a un país a distancia, debido a las transacciones que se realizan de *criptomonedas* (monedas electrónicas) mediante plataformas digitales eludiendo la presencia física de los participantes. Por lo tanto, es un problema que se presenta de forma internacional y las naciones unen sus esfuerzos para combatir este delito.

México se ha considerado como uno de los países con mayor corrupción y donde más prolífera el «lavado de dinero», pues aún y cuando existían candados en las Instituciones de Crédito (IC), se podía llevar a cabo esta actividad ilícita con gran facilidad (GAFI, 2018, Gobierno de México y UIF, 2020). Si bien es cierto, antes de la entrada en vigor de la Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita (LFPIORPI), la economía fluía con cierta abundancia, pero con mucha economía ilegal. Ahora, estas leyes ya se aplican, pero el gobierno y las autoridades deben perfeccionar las formas y los métodos para prevenir el lavado de dinero.

En lo que concierne al contexto social, a pesar de que existen entes reguladores como la Comisión Nacional Bancaria y de Valores (CNBV) y la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (Condusef); además de un marco jurídico sustentado principalmente por la "Ley *Fintech"*; y, diversas plataformas digitales con aplicaciones informativas de difusión sobre las criptomonedas, los ciudadanos siguen sin tener un conocimiento real sobre el funcionamiento de las criptomonedas y los posibles riesgos y consecuencias de su uso, incluso se puede llegar a obtener opiniones favorables inciertas por parte de las autoridades sobre las entidades con opacidad en sus operaciones o fraude, y esto por el mismo desconocimiento en materia del anonimato de *bitcoin* y el «lavado de dinero».

De igual manera, no solo importan las regulaciones, cabe señalar la importancia de cómo se conserva el anonimato de *bitcoin* mediante la estructura de su sistema *blockchain*, que involucra la transparencia y seguridad, elementos claves para la comunidad de las criptomonedas.

Derivado de las consideraciones anteriores, abordar el tema sobre el anonimato de *bitcoin* y la aplicación de su sistema *blockchain* puede aportar material para discusión y futuras investigaciones puesto que, así como existen ahora varias asociaciones en pro de las criptomonedas y la tecnología *blockchain,* también existen estudiosos que afirman algunas vulnerabilidades de seguridad en el sistema *blockchain* y otros que afirman una deficiencia en el

interés por aumentar el nivel de digitalización en México para contar con un gobierno efectivamente electrónico y una regulación eficiente para prevenir y combatir el lavado de dinero.

Así pues, la brecha digital; el desconocimiento sobre el mundo de las criptomonedas; la falta de especialistas en tecnologías de la información *blockchain* y el limitado entendimiento que se tiene sobre su uso indebido que se puede llevar a cabo, no permite mirar todo el ámbito que comprende el anonimato de los usuarios del *bitcoin* e identificar aquellos factores de riesgo que no están incluidos en la regulación para coadyuvar en la prevención y combate al lavado de dinero con activos virtuales.

Por lo tanto, comprender cómo se realizan las transacciones con *bitcoin* y la anonimidad de las mismas es esencial, ya que identificar el historial de transacciones anteriores es un elemento clave en un programa antilavado de activos. Si no es posible rastrear la cadena de propiedad, quiere decir que los *bitcoins* han pasado por un proceso de anonimato, lo que podría generar una alerta para las entidades obligadas, como es el caso de las Instituciones de Tecnología Financiera (ITF) e Instituciones de Crédito (IC).

Antecedentes

Dalia Grybauskaité, ex presidenta de Lituania, al presentar el informe provisional del panel sobre Responsabilidad, Transparencia e Integridad Financiera Internacional para lograr la Agenda 2030 de la ONU, señaló que alrededor de 1.6 billones de dólares, que representa el 2.7% del PIB mundial, se pierden por el lavado de dinero por parte de delincuentes, incluidos los narcotraficantes y el crimen organizado; además, explica que sólo son estimaciones de la actividad debido a que; al ser un delito que opera en secrecía, dificulta tener un dato exacto. (Saldivar B., 2020).

Por lo que respecta a México el delito de lavado de dinero, ha ido en aumento, cada año se blanquean entre 15 mil y 50 mil millones de dólares, primordialmente a través el sistema financiero, cifra reconocida por autoridades mexicanas como la Secretaría de Hacienda y Crédito Público (SHCP), la CNBV y la Procuraduría General de la República (PGR). (González, 2016). Por otro lado, el INGEGI, (2013) determinó que el lavado de dinero alcanzó un monto equivalente a 1.6 por ciento del Producto Interno Bruto (PIB), con un incremento del 20% anual.

Actualmente, con el desarrollo e innovación tecnológica ha encontrado un nuevo canal para estar fuera del alcance de la supervisión de las autoridades, a través de plataformas digitales no reguladas conocidas como *Fintech* (González, 2016), páginas *web* y el uso de criptomonedas (principalmente *bitcoin)* que por ser monedas electrónicas descentralizadas han contribuido a mantener el anonimato a los usuarios y delincuentes al realizar transacciones sin el riesgo de ser rastreados, lo que representa un gran peligro para fomentar un mayor crecimiento en el narcotráfico y delitos de cuello blanco (fraude y corrupción), poniendo en riesgo la estabilidad de los sistemas financieros, el desarrollo económico del país y la economía global.

El GAFI reconoce los riesgos de lavado de dinero que implican las monedas virtuales al ser “una nueva herramienta poderosa para los delincuentes” (FATF, 2014, p. 3).

Por tal motivo, en México, surge la LFPIORPI, y luego la “Ley *Fintech*” y sus Disposiciones de Carácter General que se refieren en su artículo 58, para regular y poner candados en los servicios que prestan las *Fintech* tanto en sus operaciones, autorizaciones, pagos electrónicos y operaciones con activos virtuales, sin embargo, ésta no ha sido suficiente para prevenir o combatir el lavado de dinero, a causa de las vulnerabilidades existentes en algunas características propias de *bitcoin*, como en su sistema *blockchain* donde opera y el uso de plataformas que se encuentran fuera del sistema financiero, así como en las páginas *web* (*Deep Web/ Dark Web*) (en español red oscura), han encontrado la forma de disfrazar el origen y destino de los recursos y perder la rastreabilidad de las transacciones para dificultar la identificación oportuna de las actividades sospechosas.

Adicionalmente, la ausencia de un gobierno electrónico con un desconocimiento sobre la operación, el funcionamiento de *bitcoin* y su sistema *blockchain* para operar la criptomoneda, son factores que han ido sumando limitantes en la detección e investigación de la actividad de lavado de dinero por parte de las autoridades y profesionales, también para poder contar con una

regulación eficiente, acorde a los continuos avances de la tecnología y la creación de nuevas estrategias para el lavado dinero.

Planteamiento del Problema

El anonimato es la característica más controvertida de *bitcoin*, para algunas organizaciones e investigadores como Fernando Navarro Cardoso (Profesor Titular de Derecho Penal de la Universidad de Las Palmas de Gran Canaria), el anonimato promueve el lavado de dinero, se hace referencia a dicha característica, como aquella que muestra su "potencial uso delictivo", mientras que algunos otros investigadores lo niegan, como es el caso de Gaspare Jucan Sicignano (investigador italiano de derecho penal), quien afirma que "*bitcoin* no promueve el lavado de dinero, sino todo lo contrario, lo evita", ya que afirma que es un sistema seguro e inmutable donde se puede seguir la trazabilidad de las transacciones, las cuales no se pueden modificar ni eliminar.

Por ello, la incógnita para muchos profesionales sobre la vulnerabilidad o invulnerabilidad en la seguridad y trazabilidad de la tecnología *blockchain* y el anonimato de *bitcoin*. Aspecto importante que debe tener claro y entendido todo profesional participante en la lucha contra el lavado de dinero y delitos de cuello blanco, ya que dicha incertidumbre lleva a una regulación insuficiente en materia de prevención y combate al lavado de dinero.

Al no ser posible rastrear los movimientos realizados por este medio, las criptomonedas pueden usarse para el intercambio de bienes y servicios ilícitos por parte de organizaciones delictivas. Ahora bien, la falta de una eficiente regulación por parte de las autoridades de este mercado puede ocasionar desestabilidad financiera y económica provocando la salida de capitales a otros mercados.

Derivado de las consideraciones anteriores, se plantea la necesidad de comprender desde un punto de vista informático y de manera sencilla, cómo se conserva el anonimato de los usuarios en las transacciones realizadas con *bitcoin* a través del sistema *blockchain*, identificar si se vulnera su seguridad e inmutabilidad, mediante el uso de técnicas y herramientas utilizados con periodicidad de ocurrencia; así como analizar si el enfoque de la "Ley *Fintech*" considera escenarios sobre los sistemas operativos de las criptomonedas; en este caso, para *blockchain* en la prevención y combate del lavado de dinero.

Con este trabajo se propone identificar y explicar la tecnología *blockchain* y sus características para conservar el anonimato de las transacciones realizadas con *bitcoin* y evaluar si efectivamente se vulnera la seguridad e inmutabilidad para incurrir en el lavado de dinero y si, aun así, se logra la trazabilidad de las transacciones. Además, identificar si el enfoque que tiene la regulación de la "Ley *Fintech*" considera escenarios sobre los sistemas operativos de las criptomonedas; en este caso para *blockchain*, en la prevención y combate del lavado de dinero.

Pregunta de investigación

Derivado de la problemática antes descrita, surgen las siguientes preguntas de investigación.

- *¿Puede ser vulnerada la seguridad e inmutabilidad del sistema blockchain, en las transacciones con bitcoin para lavar dinero?*

- *¿Cómo son utilizadas las transacciones con bitcoin para lavar dinero, empleando técnicas y herramientas para mantener el anonimato?*

- *¿Cuáles son los aspectos/temas regulados por la "Ley Fintech" sobre los sistemas operativos de las criptomonedas (como blockchain) para la prevención y combate al lavado de dinero?*

Hipótesis

Tomando en cuenta las preguntas de investigación y los objetivos, se plantea la siguiente hipótesis:

H1. Se vulnera la seguridad e inmutabilidad del sistema *blockchain* mediante la mezcla o el intercambio de las criptomonedas para conservar el anonimato en las transacciones con *bitcoin* para lavar dinero.

H2. La "Ley *Fintech*" considera aspectos regulatorios que previenen y combaten el lavado de dinero mediante disposiciones que permiten identificar las operaciones de mezcla, transaccionalidad e intercambio en el sistema *blockchain*.

Objetivo general

i. Identificar cómo se conserva el anonimato en las transacciones con "*bitcoin*" y si se vulnera el sistema *blockchain* para mantener el anonimato y encubrir fondos provenientes de actividades ilícitas, dificultando su rastreo.

ii. Determinar si la regulación de la "Ley *Fintech*" permite identificar operaciones de mezcla, transaccionalidad e intercambio en el sistema *blockchain*, en prevención y combate al lavado del dinero.

Objetivos específicos

a. Analizar las principales características, elementos y participantes de *bitcoin* y la tecnología *blockchain*, su funcionamiento y riesgos en las plataformas digitales, así como su uso en el sector financiero e impacto en la economía mexicana.

b. Determinar el funcionamiento de las empresas *Fintech*, los servicios que brindan y su participación en el sector financiero.

c. Identificar y analizar las técnicas y herramientas informáticas más comunes que se utilizan en transacciones con *bitcoin* a través del sistema *blockchain* para conservar el anonimato al momento de lavar dinero, e identificar la existencia de indicadores de alerta relacionados con el anonimato del cliente (usuarios).

d. Identificar si la regulación de la "Ley *Fintech*" considera dichas, técnicas y herramientas informáticas utilizadas en transacciones con *bitcoin* y el sistema *blockchain* para conservar el anonimato, en prevención y combate al lavado de dinero.

e. Conocer el estándar internacional, así como la regulación en Estados Unidos, la Unión Europea y México, en la lucha contra el Lavado de Activos y la Financiación del Terrorismo.

Tema de Investigación

La investigación se enfoca en conocer y analizar cómo funciona el anonimato de *bitcoin* y su sistema *blockchain* que lo integra, así como, técnicas y herramientas aplicadas con el propósito de vulnerar dicha tecnología y mantener el anonimato en las transacciones para el lavado dinero proveniente de actividades ilícitas. Así mismo, se realiza un breve análisis de la regulación de la "Ley *Fintech*" y los aspectos que contempla en pro de la prevención y combate al lavado de dinero.

La línea de investigación de este trabajo, aborda aspectos relacionados con el uso de la criptomoneda *bitcoin* y su anonimato para encubrir fondos de actividades ilícitas y su incorporación en la economía legal en México.

También, se hace un enfoque a las pequeñas y medianas empresas de tecnología financiera y casas de intercambio (*exchange*) ya que han sido un medio para encubrir o limpiar fondos provenientes de actividades ilícitas para ingresarlos en el sistema financiero nacional y en la economía legal, incurriendo a lo que comúnmente se denomina «lavado de dinero».

Además, se involucran temas relacionados con la tecnología *blockchain* y la Ley para Regular las Instituciones de Tecnología Financiera (LRITF, 2018) "Ley *Fintech*", debido a que son elementos claves en prevención y combate al lavado de dinero.

Palabras clave: Criptomonedas, *bitcoin*, tecnología *blockchain*, anonimato, lavado de dinero, servicios de mezcla, lavandería, *mixer*, *tumbers*, intercambio.

Metodología

La metodología que se utilizó para el desarrollo del presente trabajo de investigación es de tipo cualitativo, al realizar una revisión y análisis documental de fuentes secundarias como libros, revistas, trabajos de investigación, artículos e informes, desde diferentes perspectivas para documentar el marco de referencia y el marco teórico sobre el estudio descriptivo de las principales características, elementos y participantes en las transacciones con *bitcoin* y la tecnología *blockchain*, su funcionamiento y riesgos en las plataformas digitales y en el sector financiero, así como su participación en la economía mexicana.

Además, el estudio pretende describir el uso de la tecnología *blockchain* y el *bitcoin* para lavar dinero mediante la aplicación de técnicas y herramientas tecnológicas para perder el rastro de los recursos provenientes de actividades ilícitas conservando el anonimato de los delincuentes.

También, tiene el propósito de realizar un análisis comparativo de la regulación en materia de prevención de lavado de dinero con activos virtuales en los países de Estados Unidos, la Unión Europea y México y concluir sobre el alcance que tiene la regulación de la "Ley *Fintech*" en México, principalmente sobre los sistemas operativos de las criptomonedas como blockchain, en prevención del lavado de dinero, y financiamiento al terrorismo.

Primero se abordará la Hipótesis 1 y luego la Hipótesis 2.

La Hipótesis 1 de este trabajo es : Sí se vulnera la seguridad e inmutabilidad del sistema *blockchain* mediante la mezcla o el intercambio de las criptomonedas para conservar el anonimato en las transacciones con *bitcoin* para lavar dinero, y para poder probar ésta hipótesis, se utilizó la metodología de estudio de casos múltiple que se describe brevemente a continuación, con una finalidad exploratoria, descriptiva y explicativa sobre casos de lavado de dinero a través del anonimato de *bitcoin* identificados, reportados y judicializados, por las autoridades competentes.

Estudio de casos múltiples

Primeramente, es de relevancia mencionar que, Stake (1995) menciona que: "*el objetivo de la investigación cualitativa es la comprensión, centrando la indagación en los hechos*".

Para poder comprobar si se vulnera o no la seguridad e inmutabilidad del sistema *blockchain*, mediante la mezcla o el intercambio de criptomonedas para conservar el anonimato en las transacciones con *bitcoin*, se requiere conocer de forma descriptiva y detallada cómo funcionan las técnicas y herramientas utilizadas para mezclar o el intercambiar criptomonedas en los casos de estudio escogidos para su análisis, por ello es que se seleccionó la metodología de estudio de casos múltiples de tipo cualitativo, debido a que esta metodología, permite adentrarnos al detalle en la explicación y descripción de fenómenos que ayudan a fortalecer y desarrollar teorías

ya existentes, o bien, generar nuevas explicaciones o enfoques. Que, al aplicarse, se recomienda considerar el principio de triangulación, que no es más que el uso de dos o más métodos de recolección de datos para estudiar un fenómeno particular para garantizar la validez y fiabilidad de la investigación basada en estudio de casos (múltiples).

La triangulación consiste en utilizar múltiples fuentes, tanto primarias como secundarias, que permitan contraponer todos los datos obtenidos, convergiendo y estableciendo relaciones entre sí (Documentos, entrevistas, observación, grupos de enfoque, cuestionarios y escalas, etcétera) (Enrique, y Barrio, S/F).

Antes de explicar en qué consiste la metodología de estudio de casos múltiples, primero se abordará la metodología de estudio de casos, para una mayor comprensión.

El estudio de casos

De acuerdo a Cebreiro y Fernández (2004), se recomienda realizar un estudio de casos cuando el objeto que se quiere investigar está difuso, es complejo o controvertido. Para analizar aquellos problemas o situaciones que presentan múltiples variables y que están estrechamente vinculados al contexto en el que se desarrollan.

Para Yacuzzi (2005), los casos son particularmente válidos cuando se presentan preguntas del tipo "cómo" o "por qué", cuando el investigador tiene poco control sobre los acontecimientos y cuando el problema a estudiar es incipiente.

Para Jiménez y Comet (2016), el estudio de casos hace que el investigador comprenda que el objetivo es llegar a la verdad del fenómeno. Debemos tener en cuenta que, dentro de la complejidad de un estudio de casos como enfoque metodológico, la intención es dar respuesta a cómo y por qué ocurre el o los hechos, focalizando a los fenómenos en estudio, haciendo que la exploración sea profunda y el conocimiento obtenido sea más amplio.

Por su parte, Yin (1994), señala que el estudio de casos es una investigación que estudia un fenómeno contemporáneo dentro de su contexto de la vida real, especialmente cuando los límites entre el fenómeno y su contexto no son claramente evidentes.

De los estudios cualitativos de casos se esperan descripciones abiertas y comprensión mediante la experiencia y realidades múltiples. (Denzyn y Linconln, 1994). Y a través de éstos, se recogen de forma descriptiva distintos tipos de informaciones cualitativas, las cuales no aparecen reflejadas en números si no en palabras. Lo fundamental en esta metodología es realzar incidentes clave, en términos descriptivos. (Cebreiro y Fernández, 2004).

Stake (1995) menciona que “*el objetivo de la investigación cualitativa es la comprensión, centrando la indagación en los hechos*”.

Por otro lado, un estudio de casos evaluativo, comprende la descripción y explicación para llegar a emitir juicios sobre la realidad objeto de estudio; (Pérez, 2004).

El estudio de casos múltiple

El estudio de casos múltiple, es una metodología cualitativa de investigación que se caracteriza por centrarse en procesos de búsqueda, indagación y análisis sistemático de uno o más casos. Entendiéndose por caso, a aquella situación única que tiene interés para ser investigada.

Stake (1998), señala que el estudio de caso colectivo (estudio de casos), se enfoca en el estudio paralelo de varios casos con la misma problemática o situación, pero en diversas personas, empresas, o cualquier otro sujeto de estudio. El propósito es utilizar cada caso como una herramienta, para conocer la situación en su conjunto, sobre un mismo aspecto. Además, sostiene que "*el objetivo de la investigación cualitativa es la comprensión, centrando la indagación en los hechos*".

El estudio de casos múltiple permite explorar más de una unidad de análisis proporcionando las bases para la generalización, sobre todo, si el mismo fenómeno es evidente en varios contextos diferentes, es posible que puede revelar una tendencia más amplia que es significativa en una escala más amplia. (Rule & Mitchell, 2015).

Por su parte, Ponce (2018), menciona que: "*indagar más de un caso, aporta criterios de validez interna, externa y confiablidad a los datos, permitiendo lidiar en mejor medida con los problemas asociados al rigor científico".*

Ragin (1992; 2011) consideran el estudio de casos múltiple como un método comparativo, porque permite examinar los patrones similares y diferenciales entre un número moderado de casos, donde centra su atención en la correspondencia que existe entre las diferentes partes de cada caso y en encontrar aspectos comunes que les permitan considerar los múltiples casos como manifestaciones de la misma cosa.

Por ello, el estudio de casos consiste en compilar toda la información disponible, agruparla evaluarla y estimar un tamaño de efecto resumen bajo un análisis de varios casos individuales, según (Bolaños y Calderón, 2014).

De acuerdo al Modelo de estudio de caso (Yin,2014, p.60), se divide en tres fases:

I. Definición y diseño

Desarrollar teoría: para relacionar el estudio con la teoría previa y con la intención de explicar, desarrollar el estudio de casos múltiples, y para ello se realiza:

a. Selección de casos.

b. Diseño de protocolo de recogida de datos: define proceso, efectos durante el proceso y técnicas de recogida de datos.

II. Recogida y análisis

a. Realizar el estudio de las condiciones del caso 1, caso 2, y casos restantes; y para ello realizar: entrevistas, observaciones y/o análisis documental.
b. Redactar un informe por cada caso individual: analizar los distintos casos e ir replicando las conclusiones o resultados que se van a alcanzar.

III Análisis y conclusiones

a. Conclusiones cruzadas de los casos, analizando cada uno de los casos.
b. Desarrollar implicaciones políticas.
c. Informe cruzado de los casos, donde se aglutina toda la información recabada.

Este procedimiento, se tomó como guía para el desarrollo del estudio de los casos de esta investigación, como se describe a continuación:

Selección de casos

Para el desarrollo de esta investigación, se seleccionaron casos de empresas prestadoras de servicio de activos virtuales y casos de lavado de dinero por la delincuencia organizada (narcotráfico).

Las empresas a estudiar corresponden a Proveedores de Servicio de Activos Virtuales (VASP, siglas en inglés) que operan como intercambiadores o mezcladores de criptomonedas, ya que representan una pieza importante en el uso de técnicas y herramientas para conservar el anonimato en transacciones con *bitcoin*, y los casos de lavado de dinero por delincuentes (narcotraficantes) a estudiar, corresponden a lavado de dinero con criptomonedas que están asociados con el anonimato de *bitcoin*. Todos ellos investigados y judicializados en México, bajo la “Ley *Fintech*”.

Sin embargo, al realizar la búsqueda y recopilación de información, se observa que los entes reguladores mexicanos en la materia, no cuentan con información ni datos estadísticos públicamente disponibles. Y en el caso de la Fiscalía General de la República (FGR) en México, tampoco tiene información o no es pública. Por su parte, la Unidad de Inteligencia Financiera (UIF), a la fecha del presente trabajo, ha publicado un solo caso con tipología “AV en México” en el que se utilizaron VASPs para la comisión de operaciones con recursos de procedencia ilícita y la compra de (USD COIN); lo que representa una limitante para el desarrollo de la presente investigación.

Por lo tanto, la selección de casos se basó en un muestreo teórico, no estadístico, tratando de escoger aquellos casos reportados que ofrecen una mayor oportunidad de comprender y

entender mejor los mecanismos, técnicas y herramientas utilizados para conservar el anonimato en las transacciones con *bitcoin* y su efecto en la seguridad del *blockchain* y que permitan una generalización analítica. Y para poder reforzar la validez de la información, se seleccionaron cinco casos de lavado de dinero mediante el anonimato de *bitcoin*, realizados por empresas prestadoras de servicio internacionales de activos virtuales y cuatro casos de delincuentes (narcotraficantes) en México.

Derivado de lo anterior, el método de recolección de datos, sobre los nueve casos seleccionados; fue a través de consultas de información internacional públicamente disponible en diversas fuentes oficiales y formales, como el sitio *web* del gobierno de Estados Unidos " Red de Ejecución de Delitos Financieros del Tesoro de los EE. UU"; sitios *web* de instituciones internacionales dedicadas al combate y prevención del lavado de dinero y delitos financieros como Antilavado de Dinero (ALD), Financial Action Task Force (FATF), de la Agencia de la Unión Europea para la Cooperación Policial (EUROPOL) y Naciones Unidas; el sitio *web* de importante editorial en línea estadounidense Siff Davis; así como sitios *web* de noticias especializado en *bitcoin* y monedas digitales; de agencias de noticias como Bloomberg (Nueva York), Reuters (Reino Unido), Decrypt.co (periodismo, de para adopción de *blockchain*) y Criptonoticias ; sitio *web* de análisis y noticias destacadas del sector tecnológico; publicaciones de CipherTrace (primera firma forense de *blockchain* del mundo); el Informe del GAFI "Activos Virtuales, Señales de alerta de LD/FT", además, el sitio *web* de la UIF del gobierno de México y sitios *web* de los periódicos de México El Economista y La Jornada.

Por lo anterior, de la información pública, se escogieron cinco empresas VASP internacionales de intercambio y/o mezcla de criptomonedas que ofrecieron servicios de anonimizar transacciones y que han sido investigadas y juzgadas por autoridades internacionales, además de que exponen las técnicas y herramientas que fueron utilizadas para conservar el anonimato, y cuatro casos identificados de cárteles de México de lavado de dinero con criptomonedas investigadas y juzgadas por las autoridades mexicanas, donde dos de ellos exponen las técnicas y herramientas utilizadas para conservar el anonimato y los otros dos casos exponen la detención de los delincuentes como resultado de la aplicación de la "Ley *Fintech*"; con el propósito de revisar y analizar la experiencia de cada caso que se reproduzca en los otros y así, verificar los resultados y clarificar sus determinantes y poder precisar las relaciones causales del fenómeno que se está estudiando. Los casos seleccionados se muestran en el cuadro I y II.

Cuadro I

Estudio de casos: Empresas Prestadoras de Servicio Internacionales de Activos Virtuales

	Caso	País	Empresa de Servicio (Modelo de negocio)	Periodo de operación	Técnica utilizada para lavar dinero	Autoridad Internacional	Importe de recursos lavados con *bitcoins* (en USD)
1	**Helix y Coin Ninja**	Estados Unidos	Intercambiador de monedas virtuales convertibles y Mezclador de bitcoin	Helix 2014 - 2017 Coin Ninja 2017 - 2020	Intercambio Mezcla o rotación	Investigados por FinCen. Imputados por el Departamento de Justicia de Estados Unidos	$311,000,000
2	**BestMixer.io**	Luxemburgo y paises bajos	Mezclador de criptomonedas líder en el mundo	2018 - 2019	Mezcla/ Vaso para mezclar fondos de criptomonedas	Investigado por Servicio de Información e Investigación Fiscal de los Países Bajos (FIOD), en estrecha cooperación con Europol y las autoridades de Luxemburgo	200,000,000
3	**Bitcoin Fog**	Estados Unidos	Servicio de Mezcla	2011 - 2021	Mezcla de criptomonedas	Investigado por el Servicio de Impuestos Internos (IRS) por el Imputado por el Departamento de Justicia de Estados Unidos	336,000,000
4	**BTC-e**	Bulgaria, sujeto a las leyes de Chipre	Intercambio de monedas virtuales	2011 - 2017	Intercambio de monedas	Investigado por Unidad de Recuperación de Activos de Nueva Zelanda	4,000,000,000
5	**Binance**	China	Intercambio de monedas virtuales	2017 A la fecha	Intercambio de monedas	Investigado por el Servicio de Impuestos Internos (IRS) por el Imputado por el Departamento de Justicia de Estados Unidos	2,350,000
							$4,849,350,000

Fuente: Elaboración propia de Fincen, 2020; Osborne, 2019; Nikhilesh, 2021; CipherTrace, 2021; Schönberg, 2021.

Cuadro II

Estudio de casos: Delincuentes (Narcotraficantes) en México

	Casos de México	Estado	Actifidad	Técnica utilizada para lavar dinero	Autoridad	Importe de recursos lavados con *bitcoins* (en Pesos MX)
1	CJNG y Cartel de Sinaloa	Guadalajara Sinaloa	Narcotraficante	Técnica conocida como "pitufo"	Unidad de Inteligencia Financiera	No se especifica
2	Ignacio Santoyo	Playa del Carmen	Red de Prostitución	Intercambio en plataforma	Unidad de Inteligencia Financiera	$441,000
3	Héctor Ortiz	Guanajuato	Narcotraficante	Intercambio en plataforma	Unidad de Inteligencia Financiera	No se especifica
4	Zaragoza	Jalisco y Michoacán	Narcotraficante	Intercambio Compra de AV Triangulación de recursos Movimientos internacionales de efectivo mediante instituciones bancarias y plataformas de AV	Unidad de Inteligencia Financiera	No se especifica
						$441,000

Fuente: Elaboración propia. Oré, 2020; Chipolina, 2020; Gutiérrez, 2022; UIF, 2020.

Los nueve casos seleccionados son un estudio exploratorio sobre las técnicas y herramientas utilizadas para conservar el anonimato de las transacciones con *bitcoin* para lavar dinero, al ser

de los que fueron publicados y con mayor información detallada sobre los hechos de lavado de dinero con *bitcoin*.

Cómo se muestra en las tablas 3.1, cabe resaltar que el importe total de lavado de dinero con *bitcoin* por parte de las empresas prestadoras de servicio internacionales de activos virtuales es por 4,849,350,000 USD, lo cual representa el 5.6% del PIB mundial 2021, equivalente a 86,6 billones de USD a precios constantes (Banco Mundial, 2022).

Y por lo que respecta a México, en la tabla 3.2, solamente en el caso de Ignacio Santoyo se reporta el monto de lavado de dinero con *bitcoin* por $441,000 pesos Mx, lo que representa el 0.002% del PIB de México en 2021, que equivale a $17,8 billones de pesos Mx a precios constantes (Statista Research Department, 2022).

Evidencia

Considerando que el objeto de estudio en esta investigación es el anonimato del *bitcoin* en el sistema *blockchain* para lavar dinero ilícito, hechos ilegales que se cometen en secrecía, por delincuentes y VASP no registradas ni reguladas, a través del uso de redes oscuras, no es factible realizar entrevistas e investigación de campo, por el riesgo y peligro que representa.

Por lo tanto, la fuente de evidencia que se utilizó en esta investigación, es la evidencia documental como base única para el estudio de los casos seleccionados, la cual contempla informes, reportes y artículos públicos en los sitios *web* oficiales, que se señalan más adelante (en el apartado de selección de muestra), sobre la investigación y judicialización por las autoridades competentes, tanto de México como internacionales. Lo anterior, considerando que la información completa y detallada sobre los casos de estudio que son relativamente recientes, se encuentra integrada y archivada en carpetas de investigación en resguardo con acceso restringido por parte de las autoridades correspondientes de cada caso en particular, situación que representa una limitante para el desarrollo de esta investigación.

Para este estudio, se llevó a cabo un análisis documental sistemático que se describe más adelante en el apartado de análisis de información.

Análisis de la información

- Para el estudio de los casos, se elaboró una matriz para los casos de empresas prestadoras de servicio internacionales de activos virtuales y otra para los casos de delincuentes (narcotráfico), que permitieran examinar, categorizar y combinar la información recolectada por cada caso en estudio y facilitar el análisis de información cruzada de las evidencias por cada caso, y de forma global, dando validez a esta investigación, donde las categorías se definieron considerando como factores causativos del anonimato en las transacciones con *bitcoin* para lavar dinero, a las técnicas y herramientas utilizadas para conservar el anonimato.

- La información se organizó en tablas, donde las filas se registraron los casos concretos analizados y en las columnas se anotó los factores característicos, explicativos y descriptivos de las técnicas y herramientas que se utilizaron dentro del sistema *blockchain* para conservar el anonimato de los usuarios y demás datos mencionados en el párrafo anterior.

- Con la información recopilada:

    a. En la matriz de los casos de empresas en estudio se definieron algunas columnas para identificar algunos datos, como: su giro de negocio, país de origen, periodo de operación, la(s) técnica(s) y herramienta(s) utilizada(s) para la anonimización de transacciones o fondos, la autoridad internacional que investigó el caso, la cantidad de *bitcoins* lavados que hayan identificado y reportado las autoridades y su equivalente en Dólares, así como cargos imputados a las mismas, y revelaciones hechas por dichas autoridades, por señalar algunos.

    b. Para los casos de delincuentes (narcotráfico) en México, se elaboró una matriz donde se definieron algunas columnas para identificar y recolectar algunos datos como el estado o localidad de origen, su actividad, las técnicas y herramientas utilizadas para lavar dinero, autoridades que investigó el caso, las labores realizadas para rastrear y detectar a los delincuentes e importe de recursos lavados con *bitcoin*.

Resultados

Después de analizar la información sobre los casos de las empresas prestadoras de servicios internacionales de activos virtuales Helix y Coin Ninja, BestMixer.io, *Bitcoin* Fog, BTC-e, BINANCE, y de los casos de delincuentes (narcotráfico), como resultado, en el Capítulo 4, se presenta por cada uno de los casos en estudio, una breve descripción y su discusión del caso con la aprobación o rechazo de la Hipótesis H1; y al final, un cuadro resumen sobre el cumplimiento de la hipótesis H1 por las empresas prestadoras de servicio y otro por los casos de delincuentes(narcotráfico) en México.

La Hipótesis 2 de este trabajo es: La “Ley *Fintech*” considera aspectos regulatorios que previenen y combaten el lavado de dinero mediante disposiciones que permiten identificar las operaciones de mezcla, transaccionalidad e intercambio en el sistema *blockchain*.

Para probar esta hipótesis, se llevó a cabo un breve análisis comparativo de trabajos de investigación, reportes y normatividad aplicable, sobre a quién regular en las transacciones con *bitcoin*; sobre normatividad en la materia, aplicable en Estados Unidos, la Unión Europea y México; y finalmente, sobre el alcance de la regulación de la “Ley *Fintech*”, mismo que se describe en el Capítulo 3.

Capítulo 1.
El riesgo del uso de las criptomonedas para el lavado del dinero

1.1 Introducción

La modernización de la tecnología financiera ha llevado a desarrollar nuevas tendencias como el uso y funcionamiento las criptomonedas tema que genera muchas dudas y desconfianza debido, en gran medida, por su anonimato de quiénes las realizan y la falta de respaldo por parte del gobierno. Las criptomonedas surgen de la necesidad de poder tener representado el dinero de uno en algo más confiable.

Después de la crisis financiera mundial que se vivió en el año 2008 derivada por los delitos cometidos por los bancos de Estados Unidos que originaron una crisis crediticia e hipotecaria; la crisis energética, el derrumbe de bolsas y mercados de valores; y la posible recesión global, se empiezan a crear las criptomonedas que cada vez van llamando más el interés y la aceptación de las personas en todo el mundo.

En el siguiente capítulo se presenta la contextualización de las criptomonedas, sus principales características, categorías, uso legítimo y los riesgos inherentes por su uso en el sistema centralizado y descentralizado. Asimismo, el marco regulatorio que impera para la prevención de lavado de dinero en apego a las Recomendaciones del GAFI y las disposiciones regulatorias mexicanas.

1.2 Criptomonedas

Para comprender qué son las criptomonedas, primero se debe conocer qué es una moneda digital y una moneda virtual. La moneda digital se almacena y se transfiere de forma electrónica y se basa en un código binario, es una representación digital que puede ser usada en el mercado de bienes tangibles, como es el caso del sistema de pago *PayPal* (1998), moneda digital, en función de una moneda de curso legal. Por su parte, una moneda virtual es ficticia y su objetivo es el mercado virtual, es decir, no se pueden utilizar para la compra de bienes reales.

Por lo tanto, las criptomonedas son monedas digitales, ya que se utilizan en la compra y venta de bienes reales, también tienen convertibilidad en dinero real y se pueden adquirir en casas de cambio, cuyo valor se determina por la oferta y demanda en el mercado. A continuación, se mostrarán la definición de criptomoneda por algunos autores:

Satoshi Nakamoto (2008), define una moneda electrónica como una cadena de firmas digitales y señala que cada propietario transfiere la moneda firmando digitalmente un "hash"[1] de la transacción anterior y la clave pública del siguiente propietario y agregándolas al final de la moneda. Un beneficiario puede verificar las firmas para verificar la cadena de propiedad. (p.2)

Según Lansky (2016), investigador de la criptomoneda de la Universidad de Finanzas y Administración, una criptomoneda es un tipo de moneda digital basada en principios criptográficos con una única combinación de tres características: produce anonimidad, son independientes de una autoridad central y proveen protección del problema del "doble gasto"[2].

El GAFI (2014), define a la moneda virtual como:

> Una representación digital de valor que puede ser comercializada digitalmente y funciona como: I. Un medio de cambio; II. Una unidad de cuenta; y, III. Un depósito de valor, la cual no tiene curso legal (es decir, cuando se ofrece a un acreedor, es una oferta válida y legal de pago en ninguna jurisdicción). (p.6)

En 1998, Wei Dai, criptógrafo y miembro de la comunidad cypherpunk[3], muy conocido por sus aportes al campo de estudio en el mundo de las criptomonedas publicó una propuesta precursora del *bitcoin*, la moneda digital "*b-money*", bajo un sistema de efectivo electrónico distribuido y anónimo, usando "*Hashcash*"[4] con el fin de realizar la "minería" que en su momento no despertó gran interés.

Como señala Cruz (2018), desde un punto de vista informático, las criptomonedas son un espacio restringidos por algoritmos cifrados, que tienen lugar en una base de datos, cuya red funciona a través de un mecanismo *peer to peer* (punto a punto), el cual permite crear y compartir la criptomoneda entre los usuarios directamente, sin intermediarios a lo largo de toda la operación.

1.2.1 Principales características.

De acuerdo a Cruz (2018) las principales características de las criptomonedas son las siguientes:

- Irreversibles: Quiere decir que una vez realizado el envío y la configuración de recibido e integrado en los bloques, la transacción no se puede revertir.

[1] "hash"- Es un algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija.

[2] "doble gasto". Consiste en la posibilidad de que una misma criptomoneda sea duplicada y utilizada repetidas veces. Alexander Ramírez 2020.

[3] Cypherpunks. Resistencia a la pérdida de la privacidad del usuario en los tiempos de Internet.

[4] "Hash Cash". Sistema inventado en 1997 por el criptógrafo inglés Adam Back que pretendía poner freno a los envíos de spam masivo. La idea era imponer un coste no monetario al envío de cada correo.

- Anónimas: Esto es que, la mayoría de las criptomonedas que actualmente se utilizan son entradas por medio de un identificador numérico o una dirección IP[5] que no depende de un nombre o identificador personal.
- Rápidas y accesibles: Es decir, que los datos que componen a las criptomonedas, se transmiten a través de una red de información *peer to peer* (punto por punto), donde su verificación y confirmación se realiza en pocos minutos después de haberse realizado la transacción, aunque ésta se realice desde un lado a otro del planeta.
- Seguridad: las criptomonedas prometen seguridad en transferencia y verificación a través de complejos algoritmos matemáticos encriptados; no obstante, el continuo avance de la seguridad informática crea dudas sobre las vulnerabilidades de la red.

1.2.2 Categorías

En 2009, Satoshi Nakamoto crea la primera criptomoneda bajo el nombre de «*bitcoin*» mediante el esquema de *peer-to-peer electronic cash system* quien decidió incluirla como referencia en su artículo titulado: "*Bitcoin: A Peer-to-Peer Electronic Cash System*", publicado en 2008, desarrollando y perfeccionando la propuesta de Wei Da. A partir del auge que empezó a tener la criptomoneda se han creado un gran número de criptomonedas que circulan en la red, de las cuales las más conocidas se muestran en el cuadro 1.1.

Cuadro 1.1
Criptomonedas más conocidas

No.	Año de creación	Nombre	Siglas	Fundador
1	2009	Bitcoin	BTC, XBT	Satoshi Nakamoto
2	2011	Namecoin	NMC	Vinced
3	2011	Litecoin	LTC	Coblee
4	2012	Peercoin	PPC	Sunny King
5	2012	Ripple	XRP	Chris Larsen et Jed McCaleb
6	2013	Dogecoin	DOGE	Jackson Palmer et Billy Markus22
7	2014	BitShares	BTS	
8	2014	Dash	DASH	Evan Duffield
9				
10	2014	Monero	XMR	
11				
12				
13	2014	SolarCoin	SLR	Fondation SolarCoin
14				
15	2014	MaidSafeCoin	MAID	David Irvine
16	2015	Factom	FCT	
17	2015	Ether	ETH	Vitalik Buterin
18	2016	Lisk	LSK	Max Kordek
19	2017	DeepOnion	ONION	
20	2017	Mercoin	MRN	
21	2018	Scolcoin	SCOL	Desarrolladores colombianos

Fuente: Recuperado en https://es.wikipedia.org/wiki/Criptomoneda

[5] Dirección IP: Es el número que uno escoge o se asigna dentro de la red, es la manera que tiene Internet de saber quién es quién. Es como una matrícula para identificarse cuando uno está conectado

La plataforma en la que opera el *bitcoin* propone un nuevo tipo de dinero que incluye criptografía para controlar su creación y todo tipo de transacciones, lo que quiere decir que las transacciones se hacen de usuario a usuario sin ninguna autoridad centralizada y bajo un protocolo de seguridad alto. Todas las monedas digitales posteriores al *bitcoin* cuentan con características y protocolos diferentes pero todas ellas similares y basadas al *bitcoin* (Mora, 2006).

Cuadro 1.2
Criptomonedas por Capitalización de Mercado

Nombre	Capitalización de mercado	Precio	Volumen (24h)	Acciones en circulación
Bitcoin	$111.576.210.822	$8,617.17	$4.430.847.776	17.362.525 BTC
Ethereum	$21.870.899.078	$212,27	$1.742.672.277	103.031.580 ETH
XRP	$21.612.975.350	$0,537562	$1.225.398.108	40.205.513.967 XRP
Bitcoin Cash	$9.828.269.257	$563,45	$767.980.331	17.443.138 BCH
EOS	$5.085.432.926	$5,61	$758.145.106	906.245.118 EOS

Fuente: Recuperado en https://es.wikipedia.org/wiki/Criptomoneda

1.2.3 Uso legítimo.

Respecto al uso legítimo, (GAFI, 2014), refiere que de igual forma que otros nuevos métodos de pago, las monedas virtuales «criptomonedas» tienen usos legítimos. Existen importantes empresas de capital de riesgo que invierten en moneda virtual de nueva creación. La moneda virtual tiene la capacidad de mejorar la eficiencia de pago, reducir los costos de transacción para los pagos y transferencias de fondos. Tal es el caso del «*bitcoin»* que funciona como una moneda global que puede evitar los cargos por cambio y es actualmente procesada a tasas/cargos menores que las tarjetas de crédito y débito tradicionales; además, pueden potencialmente proporcionar un beneficio a los sistemas de pago en línea existentes, como *Paypal*. GAFI (2014) afirma:

> La moneda virtual puede facilitar los micropagos permitiendo a los negocios monetizar en Internet bienes y servicios de muy bajo costo como juegos de una sola partida o descargas de música.
>
> Las monedas virtuales pueden del mismo modo facilitar las remesas internacionales y promover la inclusión financiera de otras maneras, a medida que se desarrollan nuevos productos y servicios basados en monedas virtuales que puedan servir potencialmente a las personas poco bancarizadas o desbancarizadas. Las monedas virtuales, - en particular el *bitcoin*- pueden mantenerse con la finalidad de servir como inversión.
>
> Estos beneficios potenciales deben ser analizados cuidadosamente, considerando también si se conservarán las ventajas en costos si la moneda virtual quedase sujeta a requisitos regulatorios similares a los que se aplican a otros métodos de pago, así como también, si estarán incluidas las tasas de cambio para hacer un retiro en moneda fiduciaria, y si la

volatilidad, la protección del consumidor y otros factores limitan su potencial en términos de inclusión financiera. (p.p. 12, 13)

1.3 Sistema centralizado y descentralizado

Dentro del mundo de las monedas digital existen las monedas centralizadas y descentralizadas, ésta última, característica propia de las criptomonedas. A continuación, se dará una breve descripción de ambas, con la finalidad de tener un claro entendimiento de las mismas.

Las monedas digitales centralizadas tienen una sola autoridad como administrador, es decir, que un tercero controla el sistema. El administrador emite la moneda; establece las reglas para su uso; mantiene un libro mayor de pagos central; y, tiene autoridad para canjear la moneda o retirarla de la circulación. Además, el tipo de cambio de una moneda digital convertible puede ser determinado por la oferta y demanda del mercado o fijado por el administrador a un valor establecido medido en moneda fiduciaria u otra reserva de valor, como el oro. (GAFI, 2014).

El comercio electrónico y los medios de pago vía internet como es el caso de Paypal y *safetyPay* los pagos y transferencias interbancarias, tanto en aplicaciones móviles y aplicaciones *web* de banca en línea, se mueven en torno a un sistema centralizado de un Banco Central con el respaldo del sistema financiero de cada país. (Cruz, 2018).

El sistema de pago de las monedas digitales descentralizadas (conocidas como criptomonedas) no está respaldado por ninguna autoridad central, ni se rige por algún marco normativo o institucional, es decir, no tienen autoridad de administración central ni supervisión o supervisión centralizada. (Cruz, 2018).

Cabe destacar que el mercado de las criptomonedas, cada vez se está posicionando más dentro del Sistema Monetario Internacional, debido a las grandes cantidades de masa monetaria que está concentrando a través de transacciones monetarias especulativas y del interés de las empresas de recibir pagos virtuales; sin embargo, su descentralización, ha limitado el control sobre la emisión, circulación y distribución de la masa monetaria. (Cruz, 2018).

1.3.1 Riesgos del sistema descentralizado.

El GAFI (2014), en su informe "*Monedas Virtuales*. *Definiciones claves y riesgos potenciales de LA/FT*", señala el lavado de dinero y financiamiento al terrorismo como un riesgo potencial del sistema descentralizado de las criptomonedas, donde refiere que:

El sistema descentralizado de las criptomonedas es potencialmente vulnerable a los riesgos de anonimato. Por mencionar un caso: por diseño, las direcciones *bitcoin* que operan como cuentas no tienen nombres ni ninguna otra identificación del cliente, y, por otro lado, el sistema no tiene ningún servidor o proveedor de servicio central. El protocolo de *bitcoin* (primera criptomoneda),

de la cual hablaremos más adelante, no requiere, ni proporciona la identificación y verificación de los participantes; así como tampoco crea registros históricos de transacciones asociadas a identidades del mundo.

No hay ningún órgano de control central y/o software antilavado de activos para monitorear e identificar transacciones sospechosas. Las autoridades o gobiernos no pueden identificar una ubicación central o entidad (administrador) para fines investigativos o de embargo de activos (aunque las autoridades pueden dirigirse a intercambiadores individuales para conseguir información de clientes que puedan tener). Es por esto que este sistema, ofrece un nivel potencial de anonimato que se ha probado imposible con otros métodos de pago como tarjetas de crédito y débito tradicionales o sistemas de pago en línea.

Por otro lado, la expansión globalizada de las criptomonedas incita a que incremente de igual manera los riesgos potenciales de lavado de activos o financiamiento al terrorismo; ya que se pueden acceder a los sistemas de moneda virtual a través de Internet (inclusive desde teléfonos celulares) y para hacer pagos transfronterizos, así como transferencias de fondos. Además, las monedas digitales, se basan generalmente en infraestructuras complejas que involucran a varias entidades, a menudo distribuidas en varios países, para transferir fondos o realizar pagos. Este tipo servicios implica que la responsabilidad de cumplimiento de la normativa antilavado de activo y contra la financiación del terrorismo, así como la supervisión sea poco clara.

Los registros de clientes y de transacciones pueden ser mantenidos por distintas entidades, a menudo en diferentes jurisdicciones, lo que hace más difícil que las fuerzas del orden y los reguladores puedan tener acceso a ellos. Este problema se ve agravado por la rápida evolución de la tecnología de las monedas virtuales descentralizadas y de los modelos de negocio, incluido el número cambiante y los tipos/roles de los participantes que prestan servicios en los sistemas de pagos en moneda virtual.

Es importante destacar que los componentes de un sistema de moneda virtual pueden estar ubicados en jurisdicciones que no cuenten con adecuados controles de antilavado de activos y contra la financiación al terrorismo (ALA/CFT). Los sistemas de monedas virtuales centralizados podrían ser cómplices de lavado de dinero y deliberadamente podrían buscar jurisdicciones con regímenes ALA/CFT débiles. Las monedas virtuales convertibles descentralizadas que permiten transacciones anónimas de persona a persona pueden parecer existir en un universo digital totalmente fuera del alcance de cualquier país en particular.

1.4 Prevención de lavado de dinero

El GAFI es un organismo intergubernamental establecido desde 1989 por el Grupo de los Siete (G7), con el mandato de fijar estándares y promover la implementación efectiva de medidas legales, regulatorias y operativas para combatir el lavado de activos, el financiamiento del terrorismo y el financiamiento de la proliferación de armas de destrucción masiva y otras amenazas, con el fin de proteger la integridad del sistema financiero internacional de los riesgos

derivados de dichos delitos; e identificar vulnerabilidades a nivel nacional para proteger el sistema financiero internacional de usos indebidos. (Unidad de Información y Análisis Financiero (UIAF)).

Este organismo está formado por los miembros de 37 países y dos organizaciones regionales: el Consejo de Cooperación del Golfo y la Comisión Europea (FATF). Para llevar a cabo sus funciones, contempla los siguientes grupos de trabajo, (Unidad de Inteligencia Financiera (UIF)):

- Grupo de Desarrollo de Políticas (PDG): coordina la elaboración de recomendaciones, metodologías de evaluación, guías, mejores prácticas y otros documentos sobre los estándares internacionales. Además, tiene la responsabilidad de desarrollar la estrategia de vinculación entre el GAFI y el sector privado.
- Grupo de Evaluaciones y Cumplimiento (ECG): coordina y determina lo relativo a la cuarta ronda de evaluaciones mutuas, para determinar el nivel de cumplimiento de los países con respecto a las nuevas 40 Recomendaciones del GAFI y monitorear a los países que no cumplan cabalmente con éstas.
- Grupo de Riesgo, Tendencias y Métodos (RTMG): desarrolla la documentación de tipologías y tendencias, así como la identificación de riesgos estratégicos relacionados con el Lavado de Dinero y Financiamiento al Terrorismo (LD/FT). Además, provee insumos al PDG.
- Grupo de Revisión de Cooperación Internacional (ICRG): identifica y revisa a las jurisdicciones que presentan fallas en la implementación efectiva en sus regímenes de prevención de LD/FT y recomienda medidas, en su caso.
- Grupo de Coordinación de la Red Global (GNCG): apoya el trabajo de la red global, la cual está conformada por el GAFI y los órganos regionales estilo GAFI, como GAFILAT y GAFIC, entre otros, mediante el desarrollo e intercambio de mejores prácticas para el trabajo conjunto de los miembros de la Red Global.

Por lo que respecta a México, es miembro del GAFI desde el año 2000, y a través de la UIF forma parte del Consejo Directivo de dicho organismo y funge como copresidente del GNCG y del Grupo Revisor de Cooperación Internacional para las Américas, el cual se encarga de evaluar los progresos de los países de la región en el cumplimiento de sus planes de acción para atender las deficiencias en sus regímenes de prevención y combate al Lavado de Dinero, Financiamiento al Terrorismo y Proliferación de Armas de Destrucción Masiva (LD/FT/PADM).

1.4.1 Estándares Internacionales sobre la lucha contra el Lavado de Activos, Financiamiento al Terrorismo y Financiamiento de la Proliferación de Armas de Destrucción Masiva.

Las 40 Recomendaciones del GAFI comprenden un esquema de medidas que los países deben implementar para combatir el lavado de activos y de los delitos relacionados. Las legislaciones de los países miembros del GAFI deben observar, desde su propia naturaleza legal, gubernamental, socioeconómica y de riesgos, estas Recomendaciones. Por ello, (GAFI, 2020)

fija un estándar internacional que los países deben implementar, adaptándolas a sus circunstancias particulares para (p.5):

- Identificar los riesgos, y desarrollar políticas y coordinación interna;
- Luchar contra el lavado de activos; financiamiento del terrorismo y financiamiento de la proliferación;
- Aplicar medidas preventivas para el sector financiero y otros sectores designados;
- Establecer poderes y responsabilidades (por ejemplo. Autoridades investigativas, de orden público y de supervisión) y otras medidas institucionales;
- Mejorar la transparencia y la disponibilidad de la información de sobre el beneficiario final de las personas y estructuras jurídicas; y
- Facilitar la cooperación internacional.

1.4.1.1 Recomendaciones de nuevas tecnologías.

En esta recomendación, el GAFI (2020) refiere que los países deben:

- Considerar los activos virtuales como bienes, productos, fondos, fondos y otros activos; u otros activos de valor equivalente; y,

- Aplicar las medidas pertinentes en virtud de las Recomendaciones del GAFI a los activos virtuales y a los proveedores de servicios de activos virtuales (PSAV).

- Identificar, evaluar y comprender los riesgos de lavado de activos y financiamiento del terrorismo que surgen de las actividades de activos virtuales y las actividades u operaciones de los PSAV.

- Aplicar un enfoque basado en el riesgo para garantizar que las medidas para prevenir o mitigar el lavado de activos y el financiamiento del terrorismo sean proporcionales a los riesgos identificados.

- Exigir que los PSAV tengan licencia o se registren en la(s) jurisdicción(es) donde se crean para estar autorizadas a realizar actividades de PSAV y que ya están sujetas a toda la gama de obligaciones aplicables en virtud de las Recomendaciones del GAFI.

- Garantizar que los PSAV estén sujetos a una reglamentación y supervisión o monitoreo adecuados de ALA/CFT y que estén aplicando eficazmente las recomendaciones pertinentes.

- Asegurar que exista sanciones efectivas, proporcionadas y disuasorias, penales, civiles o administrativas, disponibles para hacer frente a los PSAV que no cumplan los requisitos ALA/CFT, de conformidad con la Recomendación 35.

1.4.2 Disposiciones regulatorias mexicanas.

En México, se pensaba que el sector financiero era el más sensible para realizar actos de lavado de dinero; sin embargo, de acuerdo a un estudio realizado por el GAFI se identificó que hay diferentes actividades que por su naturaleza pueden considerarse como vulnerables. Por esto, es que se promulga la Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita (LFPIORPI) el 17 de octubre de 2012, Ley Para Regular las Instituciones de Tecnología Financiera llamada como "Ley *Fintech*" y se emiten Circulares de Banco de México, para proteger al sistema financiero y la economía nacional, estableciendo medidas y procedimientos para prevenir y detectar actos u operaciones que involucren recursos de procedencia ilícita.

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

El propósito de ésta ley, es prevenir, controlar, vigilar y sancionar el lavado de dinero u otros activos procedentes de la comisión de cualquier delito, además, establece las reglas que deben observar las personas obligadas que señala en su artículo 18.

La Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita (LFPIORPI), considera a varias actividades no financieras como vulnerables, ya que pueden servir como medio para la integración de recursos de dudosa procedencia a la economía formal del país; entre los cuales están los activos virtuales, el desarrollo inmobiliario, juegos y sorteos, tarjetas de servicio y crédito, de prepago y cupones, cheques de viajero, metales y joyas, blindaje, obras de arte, por mencionar algunas.

También se señalan las siguientes obligaciones para quienes realicen dichas actividades vulnerables, (artículo 18 de la LFPIORPI):

- Realizar el trámite de alta y registro ante el Servicio de Administración Tributaria (SAT) y deberán estar inscritos en el Registro Federal de Contribuyentes y contar con el certificado vigente de la Firma Electrónica Avanzada.
- Integración de expedientes por un plazo de 5 años contados a partir de la fecha de la realización de la Actividad.
- Identificar a los clientes y usuarios
- Presentar los avisos e informes a la Unidad de Inteligencia Financiera (UIF), por conducto del SAT
- Umbral de avisos: Avisos al SAT sobre las operaciones que sus clientes o usuarios lleven a cabo por un monto superior al establecido en la LFPIORPI a acuerdo al tipo de actividad.
- Resguardo y protección de información
- Brindar las facilidades necesarias para que el SAT lleve a cabo las visitas de verificación de cumplimiento de la LFPIORPI.

- Manual de Políticas Internas de identificación de clientes o usuarios, así como los criterios, medidas y procedimientos internos para dar cumplimiento a lo establecido en la LFPIORPI, su Reglamento, Reglas de carácter general y demás disposiciones que de ellas emanen.

El Sistema del Portal de PLD, menciona los siguientes beneficios que trae el cumplimiento de esta Ley para la sociedad mexicana y para quienes realicen las actividades vulnerables:

- Impacta al flujo de recursos de la delincuencia organizada, limitando así la reinversión de estos recursos en actividades delictivas.
- Previene que los sectores que realicen actividades vulnerables sean utilizados por la delincuencia organizada para reutilizar los recursos obtenidos en la comisión de actividades delictivas.
- Fomenta una sana competencia económica.
- Previene la imposición de posibles sanciones administrativas y penales para quienes incumplan con lo dispuesto por esta Ley.

1.4.2.2 Ley para Regular a las Instituciones de Tecnología Financiera.

Ante el crecimiento del sector Fintech que se ha registrado durante los últimos años en México, su regulación se convirtió en un asunto inminente. Por esta razón, con la participación de la Comisión Nacional Bancaria de Valores (CNBV); la Secretaría de Hacienda y Crédito Público (SHCP); y, el Banco de México (Banxico), el 8 de marzo del 2018 se logró promulgar la Ley para Regular a las Instituciones de Tecnología Financiera "Ley *Fintech*", con el objeto de regular los servicios financieros que prestan las ITF; así como su organización, operación y funcionamiento y los servicios financieros sujetos a alguna normatividad especial que sean ofrecidos o realizados por medios innovadores.

La "Ley *Fintech*" se estableció para regular las ITF, permitiendo a las autoridades mexicanas, vigilar el sano desarrollo del sector *Fintech* con el objetivo de promover mejores condiciones de competencia en la prestación de servicios financieros. La Ley se concentra principalmente en tres áreas: i. pagos electrónicos, ii. financiamiento colectivo y iii. activos virtuales -valores que actualmente, no están cubiertos por ninguna entidad financiera regulada, como el *bitcoin*-.

La Ley tiene por objeto regular los servicios financieros que prestan las instituciones de tecnología financiera, contemplando los siguientes principios (Art. 2 de la Ley):

- Inclusión e innovación financiera.
- Promoción de la competencia.
- Protección al consumidor.
- Preservación de la estabilidad financiera.
- Prevención de operaciones ilícitas y neutralidad tecnológica.

Así pues, esta Ley, regula a las *Fintech*, reconociendo como tales a las Instituciones de Financiamiento Colectivo, Instituciones de Fondo de Pago Electrónico y a las Sociedades

Autorizadas para operar con Modelos Novedosos. A fin de prevenir el lavado de dinero y evitar el financiamiento al terrorismo; así como incrementar la inclusión financiera.

La Ley contempla las siguientes áreas:

- Instituciones de tecnología financiera: pagos electrónicos, financiamiento colectivo (*crowdfunding*), activos virtuales.
- Figuras reguladas: sandboxes regulatorios (modelos novedosos), API y open banking.

Algunos de los beneficios que aportan la Ley son:

- Préstamos en línea de forma inmediata.
- Firma de documentos digitalmente.
- Mayor accesibilidad a servicios y bienes financieros.
- Incremento en el acceso al crédito.
- Prevención de fraude.
- Prevención en el mal uso de la información.
- Genera certeza a las empresas en el sector.
- Da garantías al usuario.
- Habilitar a los negocios para recibir pagos en línea sin necesidad de un intermediario financiero (bancos).
- Automatización y análisis profundo de procesos de crédito (Pymes).
- Permite la competencia de las Fintech en el sector financiero.

1.4.2.2 Circular de Banco de México.

El Banco de México publicó el 8 de marzo de 2019, las Disposiciones de Carácter General aplicables a las Instituciones de Crédito e Instituciones de Tecnología Financiera en las Operaciones que realicen con activos virtuales.

A pesar de que Banco de México considera apropiado mantener una “sana distancia” entre el sistema financiero y los activos virtuales debido a su volatilidad y a los riesgos que representan para sus tenedores por la complejidad de la tecnología que los soporta (procesos matemáticos y criptográficos); y de los factores que determinan su precio; además del riesgo que representan en materia de lavado de dinero y financiamiento al terrorismo; dicha institución, busca promover y aprovechar el uso de tecnologías que puedan dar un beneficio a la eficiencia o funcionalidad, de la operación interna de las *Fintechs* e instituciones de crédito, es decir, la utilización de tecnología como registros distribuidos, cadena de bloques o incluso los propios activos virtuales en sus procesos internos podría llegar a ser factible, siempre y cuando los riesgos de los activos virtuales no impacten al consumidor final.

El objeto de estas disposiciones es:

- Determinar los activos virtuales, así como definir sus características, con los que las Instituciones podrán operar de conformidad con lo previsto en la Ley;
- Establecer los términos, condiciones y restricciones de las Operaciones que las Instituciones podrán realizar con activos virtuales;
- Establecer plazos, términos y condiciones que deberán observar las Instituciones para los casos en que los activos virtuales con los que operen se transformen en otros tipos de activos virtuales o modifiquen sus características;
- Determinar la información relacionada con las Operaciones con Activos Virtuales que las Instituciones deberán presentar al Banco de México para obtener su autorización para operar con activos virtuales, y
- Establecer las características de las autorizaciones para realizar Operaciones con Activos Virtuales.

Capítulo 2.
Análisis del impacto del *bitcoin* en el ecosistema *blockchain*

2.1 Funcionamiento del *bitcoin*

El *bitcoin* (primera criptomoneda y moneda virtual), convertible descentralizada, es una unidad de cuenta compuesta por "cadenas únicas de números y letras" que integran unidades de la moneda y que solo tienen valor porque los usuarios individuales están dispuestos a pagar por ellas. (FATF, 2014).

El GAFI define el *bitcoin* como un medio de pago en línea conforme a lo establecido por Nakamoto o una representación digital[6] de valor que puede negociarse en línea (FATF, 2014). Sin embargo, no se considera dinero debido a su falta de estatus de curso legal como son los billetes o monedas emitidos por un banco central.

El *bitcoin* funciona como medio de cambio o intercambio debido a que puede intercambiarse por bienes y servicios en muchos comercios (Houben y Snyers, 2018) de forma digital entre usuarios con un alto grado de anonimato y se pueden cambiar en dólares estadounidenses, euros y otras monedas fiduciarias o virtuales. (FATF, 2014).

Como usuario, el *bitcoin* es una aplicación móvil o de escritorio *web* que provee un monedero electrónico (virtual) que permite a los usuarios enviar y recibir *bitcoins*, realizar transacciones de bienes y servicios. (Mora García, 2016). Cualquier persona puede descargar el software gratuito de código abierto desde un sitio *web* para enviar, recibir y almacenar *bitcoins* y monitorear las transacciones de *bitcoin*. (FATF, 2014).

Para (Cruz, 2018), *bitcoin* es una red con un nuevo sistema de pago "*peer to peer*" que se comercializa entre personas a través de internet con una moneda completamente digital sin el respaldo de ningún gobierno y descentralizada, (sin el control de ningún banco central), en sus transacciones no hay intermediarios ni costos en las mismas; y que opera bajo sus cuatro principios:

- Desregulación e independencia de cualquier institución Bancaria.
- Con soluciones tecnológicas (algoritmos) a los problemas de inflación.
- Exime la necesidad de confiar en políticos financieros, inversionistas, o economista.
- Es libre de deuda. (p.67)

[6] *Representación digital:* es una representación de algo en forma de datos computarizados que se representan usando valores discretos (discontinuos) para incorporar información, en contraste con señales continuas o analógicas que se comportan de manera continua o representan información usando una función continua. Un *bitcoin*, puede contener una representación digital de la moneda virtual, pero la moneda solo funciona como tal si está vinculada digitalmente, a través de Internet, al sistema de la moneda virtual. (FATF, 2014).

2.1.1 Red *Bitcoin*

La red *Bitcoin* es una fuente abierta descentralizada en un sistema de partes (P2P), que no requiere de una autoridad central como un gobierno, banco o cualquier intermediario permitiendo así a los usuarios intercambiar los *bitcoins* directamente entre ellos (Crypto, 2017).

El usuario es una persona o entidad que adquiere una moneda virtual y la usa para comprar bienes o servicios que pueden ser reales o virtuales, así como transferirlas a otra persona o entidad para uso personal o como inversión. También puede adquirir direcciones de *bitcoin*, que funcionan como cuentas, en un intercambiador de *bitcoin* o en un servicio de billetera en línea. Además, las transacciones se identifican por la dirección de *bitcoin*, que es una cadena de letras y números que no está vinculada sistemáticamente a un individuo. Por esto es que se dice que *bitcoin* es "pseudoanónimo". (FATF, 2014).

El *bitcoin* (moneda virtual) se pueden conseguir de diferentes maneras: la primera, es comprando una moneda virtual con dinero real (fiduciario) o con otra moneda virtual. Como moneda descentralizada, los usuarios pueden comprarlas por medio de un cambiador (*exchanger*) o directamente a otro usuario; la segunda, hay algunas actividades específicas como convertirse en un comerciante que acepta monedas virtuales por la compra de bienes y servicios virtuales o reales y la tercera, al extraerlas a través de un proceso de minería o como parte de una comisión de transacción, es decir, un minero puede generar nuevos *bitcoins* ejecutando un *software* especial para resolver un algoritmo sofisticado o muy complejo una competencia en la cual los mineros resuelven acertijos criptográficos y el minero que gana obtendrá una recompensa 12,5 *bitcoins* en 2019 y las comisiones de transacción que los usuarios pagan a los mineros por validar transacciones. (FATF, 2014). Es importante señalar que para febrero de 2021 la recompensa es de 6,25 *bitcoins*.

La principal característica de las criptomonedas (*bitcoin*), es la tecnología "*blockchain*" (cadena de bloques), conocida como contabilidad pública o libros contables, que registra y almacena cada una de las transacciones procesadas, dicha cadena está asegurada mediante un código criptográfico que se almacena de forma acumulativa y cronológica para evitar la doble contabilidad; el registro de las transacciones se hace en una base de datos que registra la temporalidad de cada transacción y se replica en los servidores de todo el mundo. (Cruz, 2018).

En palabras del propio Marc Andreessen, creador de Netscape "*una cadena de bloques es esencialmente solo un registro, un libro mayor de acontecimientos digitales que está distribuido o es compartido entre muchas partes diferentes. Solo puede ser actualizado a partir del consenso de la mayoría de participantes de sistema y, una vez introducida, la información nunca puede ser borrada. La cadena de bloques de Bitcoin contiene un registro certero y verificable de todas las transacciones que se han hecho en su historia*" (Mora, 2016, pág. 10).

El *blockchain* o cadena de bloques constituye la parte esencial del funcionamiento de las criptomonedas, el cual se basa en la creación de bloques de información pública que conforma

un sistema abierto semi-anónimo de la aprobación y comprobación de las transacciones realizadas. Los usuarios de este sistema se identifican mediante pseudónimos públicos que puede ser consultado por cualquier usuario de la red *peer to peer*. (Cruz, 2018).

La aprobación de las transacciones consiste en agregar bloques que forman una cadena y que deben ser aprobados por todos los usuarios involucrados en la encriptación del bloque, es decir, las transacciones incluidas a dicha cadena "se confirman", después de un cierto número de "confirmaciones" la transacción adquiere plena validez, cuando la posibilidad de doble pago es ya prácticamente nula. (Cruz, 2018).

Además, el uso de los libros contables (cadenas de bloques) elimina los intermediarios en las operaciones. Una operación con *blockchain* opera directamente de persona a persona a través de una clave pública (dirección de pago cifrada que pasa de un emisor a un receptor a través de una aplicación que informa a los mineros la presencia de una nueva transacción. (Cruz, 2018).

Cuando un usuario obtiene monedas virtuales, esta representación digital de valor debe conservarse y guardarse en una billetera (*wallet*), la cual, tiene como función controlar el acceso de los usuarios a las monedas virtuales. También, es importante saber que las monedas no se encuentran guardadas en la billetera, realmente se encuentran registradas en la cadena de bloques (*blockchain*) en la red de *Bitcoin.* (Antonopoulos, 2017, p. 93).

La billetera (*wallet*) administra direcciones, que son una combinación de llaves público-privadas; además muestra el saldo del usuario y también crea y firma transacciones (Antonopoulos, 2017). Por su parte, las billeteras se utilizan para almacenar las llaves y enviar y recibir criptomonedas. Hay dos tipos de billeteras: Hot Wallet y Cold Wallet. (Coty de Monteverde 2019).

Cuadro 2.1
Principales características de las billeteras wallet

Hot Wallet	Cold Wallet
→Siempre conectadas a internet	→No están conecados a internet
→Es como una cuenta corriente. Adecuada para movimientos frecuentes de cantidades pequeñas	→Es como una cuenta de ahorro. →Son adecuadas para cantidades grandes. No son prácticos para mandar cantidades en cualquier momento, pero si lo son para recibir.
→Son vulnerables a ser robadas	→Son más seguras
Ejemplos:	Ejemplos:
* Software PC o APP móvil	* Almacenados en PC, USB o CD
* Online web	* Impreso o escrito en un papel
	* Hardware wallets que pueden conectarse a una PC cuando se necesite.

Fuente: Creación propia de Coty de Monteverde. Institute for Advancer Management (CEU IAM). Blockchain y su aplicación en el ámbito financiero.

2.1.2 Direcciones.

Las direcciones de *bitcoin* son largas cadenas de números y letras aparentemente aleatorias, como “13mckXcnnEd4SEkC27PnFH8dsY2gdGhRvM” (Franco, 2015, p. 9) que se utilizan para identificar a los usuarios. En la red *Bitcoin* los usuarios no se identifican por sus nombres o ubicación física, sino por su dirección de *bitcoin* en el libro de contabilidad pública o cadena de bloques (*blockchain*). Por esto se dice que *bitcoin* brinda cierto nivel de anonimato. Un usuario puede generar tantas direcciones de *bitcoin* como quieran para enviar y recibir transacciones, de hecho, se recomienda usar una dirección nueva en cada transacción (Antonopoulos, 2017).

Al descargar una aplicación de *software* de una billetera en un teléfono inteligente, una PC, un computador portátil o al registrarse en un servidor de proveedor de billetera en línea es como si se abriera una cuenta bancaria en un banco comercial y éstos generan una combinación de llaves público-privadas que se derivan matemáticamente entre sí y están relacionadas con cada dirección de *bitcoin*.

La red de *Bitcoin* está diseñada para “garantizar que las transacciones se puedan crear, propagar en la red, validar y finalmente agregar al libro de contabilidad pública (*public ledger*) o cadena de bloques (*blockchain*)” (Antonopoulos, 2017, p. 117). Dicha transacción es recolectada por los mineros para ser validada y luego ser incluida en nuevos bloques los cuales serán adheridos de manera permanente en la cadena de bloques (*blockchain*).

2.1.3 Emisión del *bitcoin*.

Para la creación de cada *bitcoin* se utilizan algoritmos matemáticos muy grandes y complejos, por lo que es una moneda altamente segura y además por su fácil uso, ha creado una gran revolución en el sistema de pagos y ha causado un revuelo en la comunidad bancaria, empresarial, organismos e instituciones internacionales por el gran volumen de transacciones que se realizan al día. (Mora, 2016)

Mientras que los bancos centrales (gobiernos) imprimen dinero, en la tecnología *Bitcoin* (*Blockchain*) miles de computadoras de todo el mundo están minando la criptomoneda y compitiendo entre sí.

Cada bloque se genera a través del sistema *Proof of Work (PoW)* (Prueba de Trabajo) el cual consiste en llevar a todos los nodos de la red a participar en la búsqueda de una solución válida a un problema matemático complejo que permite la creación de un nuevo bloque. (Rodríguez, 2019).

De acuerdo a (Houben y Snyers, 2018), los mineros crean monedas y validan transacciones mediante el “Sistema distribuido de prueba de trabajo” (PoW) donde se deben resolver los “acertijos criptográficos” para que se puedan agregar nuevos *bloques* a la cadena de bloques (*blockchain*). Estos acertijos se forman de toda la información anteriormente registrada en la

cadena de bloques además de un nuevo conjunto de transacciones que serán incorporadas al siguiente bloque.

El *bitcoin* está diseñado y programado para producir una cantidad fija de monedas cada 10 minutos aproximadamente. El minero que encuentre primero el hash (acertijo criptográfico) será quien genere el nuevo bloque y recibirá la recompensa. Podrá incluir en su bloque todas las transacciones antes validadas. Además de una transacción *coinbase* (de creación de nuevas moneda), tendrá su recompensa en *bitcoins*. Estas nuevas monedas, son puestas en circulación luego de una determinada cantidad de confirmaciones.

El *bitcoin* puede funcionar como:

- Moneda o medio de pago: Las empresas y servicios que admiten el *bitcoin* este puede hacerse más popular entre la gran mayoría.
- Divisa: Podría intentarse un acuerdo global que permitiera la aceptación generalizada de la criptomoneda como una divisa de cambio más. Sin embargo, su naturaleza anónima que dificulta el rastreo de sus transacciones por parte de la policía o identidades financieras, hace que por el momento muchos gobiernos y la banca se muestren recelosos hacia ella.
- Inversión: Aquí están todos aquellos que adquieren la moneda con intención de pasar sus ahorros a un valor que pueda mantenerse estable frente a posibles cambios en el panorama económico. Y es también una forma de especulación a través de la cual se comienza a hablar de la “burbuja del *bitcoin*”.

2.2 Ecosistema *blockchain*

Dentro de la cuarta revolución industrial, se dice que la tecnología de *blockchain* es la que va a tener mayor poder de revolucionar todo, por ello la importancia de entenderla. Antes de ver su definición, características, clasificación y su ecosistema, primero demos una mirada a sus antecedentes.

La primera revolución industrial tuvo lugar en Gran Bretaña (1780 y 1850), la cual dio origen al “capitalismo industrial”, como lo indica Salort I Vives (2012), los avances tecnológicos de ésta época fueron esenciales para el cambio del feudalismo a capitalismo; de los cuales, algunos de éstos aún perduran en la actualidad.

La segunda revolución industrial (1870 – 1970), estuvo más orientada en aspectos económicos y sociales y como lo refiere el autor. La creciente demografía tanto en Europa como en Estados Unidos propició esta segunda revolución, principalmente en este último y gracias a su industrialización. Las fábricas se transformaron en empresas modernas y la división del trabajo y la mano de obra no calificada tuvieron auge.

La tercera revolución industrial o revolución digital que tuvo sus inicios en 1970, tuvo como principal eje la información, los medios electrónicos y las telecomunicaciones y se caracterizó

por la aplicación masiva de la tecnología en los procesos productivos. En 1991, sale la primera *web* de Internet y a partir de aquí, se dio una transformación económica, se modernizó la industria y también los modelos de negocio. El internet trajo muchos beneficios, como en el caso de la comunicación, hacerla más rápida y eficiente.

Por último, la cuarta revolución industrial, surge en 2011 y representa el conjunto de innovaciones tecno-científicas, cuya sinergia da la oportunidad de producir bienes y servicios en la actualidad (Álvarez Argüelles, 2018). Sin embargo, hasta 2013 se sugiere su implementación en la feria industrial[7].

Esta industria comprende técnicas avanzadas de producción en conjunto con tecnologías inteligentes que se incorporan en las organizaciones, así como las personas y los activos. Las tecnologías de innovación dentro de esta industria está Internet de las cosas, robótica, inteligencia artificial y desde luego *blockchain*.

2.2.1 Definición y características.

De una forma genérica, se define *blockchain* como una "tecnología basada en la teoría de juegos, criptografía e ingeniería de software para que una red de computadoras anónimas pueda llegar a un consenso sobre un registro compartido". Es una cadena de bloques de información que están unidos entre sí mismos por algoritmos criptográficos, de ahí el nombre de *blockchain*, que traducida literalmente quiere decir "cadena de bloques", (Ast Federico, 2020). Es una base de datos, donde se anotan las transacciones en criptomonedas que hacen usuarios anónimos.

La Consultora Tecnológica Vector ITC define *blockchain* como el "Libro de contabilidad digital incorruptible de transacciones económicas que se puede programar para registrar no solo transacciones financieras sino prácticamente todo lo que tenga valor", también dice que: es una de las tecnologías de libro distribuido donde cada nodo obtiene su propia copia del libro. Cada vez que alguien añade una nueva transacción, se actualizan todas las copias del libro. Se puede considerar que la Tecnología de Contabilidad Distribuida (DTL) es la tecnología madre de *blockchain.*

Así pues, la contabilidad distribuida se define como una base de datos descentralizada, distribuida en varios ordenadores o nodos, donde cada uno mantendrá el libro, si ocurre algún cambio en los datos, el libro se actualizará de forma independiente en cada nodo.

De una manera más sencilla, se puede decir que *blockchain* es una base de datos donde se escriben (registran) transacciones que hacen los usuarios en cualquier criptomonedas como *bitcoin* o *heterum*, entre otras. Son bloques que se encuentran encadenados.

[7] Feria Industrial: Es la Feria que se celebra anualmente en Hannover, Alemania, donde se reúne a toda la vanguardia de las innovaciones en el mundo de los procesos productivos.

Es una base de datos segura, compartida y distribuida que registra la propiedad de cualquier tipo de activo y cuenta con las siguientes características:

I. Descentralizada: No hay una autoridad central que valide las operaciones, por lo tanto, la confianza se construye con base en programas de software que validan, verifican y hacen un consenso de las operaciones. No hay intermediarios. Todos son dueños de la información, no tiene un operador central, además, los participantes llegan a un consenso y todos saben cuál es el estado de la base de datos en cada momento.

Figura 2.1
Esquema simple centralizado, descentralizado y distribuido.

Fuente: Buterin, 2017

Con este esquema se puede entender claramente que: "descentralizado significa que ninguna entidad tiene control sobre todo el procesamiento" y "distribuido significa que no todo el procesamiento de las transacciones se realiza en el mismo lugar". (Buterin, 2017).

De acuerdo con Buterin (2017), hay tres tipos de descentralización de software que los explica de la siguiente forma:

1. Descentralización arquitectónica: *¿de cuántas computadoras físicas se compone un sistema*? *¿Cuántas de esas computadoras puede tolerar averiarse en un solo momento*?
2. Descentralización política: *¿cuántas personas u organizaciones controlan en última instancia las computadoras que componen el sistema*?
3. Descentralización lógica: *¿la interfaz y las estructuras de datos que presenta y mantiene el sistema se parecen más a un solo objeto monolítico o a un enjambre amorfo*? Una simple forma de indagarlo es: si se corta el sistema a la mitad, *¿las dos partes continuarán trabajando como unidades independientes*?

Por lo tanto, *blockchain* está políticamente descentralizada, nadie las controla; arquitecturalmente descentralizada, no hay punto de falla central en la infraestructura; pero están lógicamente centralizadas, es decir, que hay un estado acordado entre todos y el sistema se comporta como una única computadora.

II. Inmutable: quiere decir que, una vez que se incluye algo en la cadena de bloques no se puede alterar, sólo se permite añadir transacciones. Esto se logra mediante una función hash criptográfica, la cual debe tener ciertas propiedades para ser considerada segura, una de esas es el efecto avalancha. El efecto avalancha quiere decir que, si se hace un pequeño cambio en la entrada, afectará el hash de salida.

III. Transparencia: esta característica brinda privacidad y transparencia a la vez. Esto se da porque la identidad del usuario está oculta a través de criptografía y se representa sólo por una dirección pública que mostrará el historial de transacciones, es decir, existe una trazabilidad de los datos lo que la hace transparente. Como ejemplo, en el caso de las investigaciones forenses -fraude y corrupción- que toman meses podrían acelerar sus tiempos. Así es como "*Si cada parte involucrada desconfía de las razones y las acciones de las demás, resulta difícil llegar a un acuerdo. Pero si los gobiernos y las nuevas empresas de tecnología utilizaran una cadena de bloques pública, ambas partes podrían conseguir lo que quisieran (...) el gobierno utilizaría una ligera regulación algorítmica para proteger la seguridad y los derechos de los ciudadanos*." (Forde, 2017).

Además, también es:

- Compartida: debido a que todos tienen la misa copia de la base de datos, se comparte a todos los participantes, y
- Segura: porque utiliza la criptografía para crear transacciones que son inmunes al fraude.

Por sus características, la tecnología *blockchain* proporciona los siguientes beneficios:

Figura 2.2

Beneficios de la tecnología *blockchain*

Fuente: Creación propia, de Coty de Monteverde, 2019. Institute for Advancer Managment (CEUIAM). Blockchain y su aplicación en el ámbito financiero.

- Seguridad: La criptografía garantiza la seguridad mediante el uso de dos llaves, una pública y una privada.
- Integridad: Dado que es inmutable y tienes la trazabilidad completa de todo lo que ha pasado, es decir, todas las transacciones realizadas, por lo que es bueno para los auditores y el regulador.
- Trazabilidad: Quiere decir que una vez que se registra una transacción, se guarda y ya no se puede borrar. Es fácil de auditar e imposible de falsear porque todo queda registrado. Trazabilidad completa de todas las transacciones.
- Rápida implementación: no representa macro proyectos que lleven meses o años.
- Escalable e interoperable porque es muy fácil de añadir un nuevo participante, un nuevo nodo a esta red.
- Garantiza la privacidad por la criptografía. En el caso de un *blockchain* privado, garantiza la privacidad de los participantes.

La tecnología *blockchain* es de interés para muchos, debido a que:

- Es altamente resistente a ataques externos.
- Elimina reconciliaciones y disputas.
- Simplifica mucho los procesos que involucra varios participantes en diferentes localizaciones que tienen diferentes intereses.
- Permite crear nuevos negocios y servicios que en la actualidad no son posibles.

Es de relevancia resaltar que esta tecnología originalmente fue creada con la base de la criptomoneda *bitcoin.* No obstante, por sí misma ha impactado en muchas otras áreas aparte de la financiera, como en la salud, gobierno y también en procesos de fabricación o distribución.

2.2.2 Clasificación.

De acuerdo a la Consultora Tecnológica Vector ITC, *blockchain* se clasifica de la siguiente manera:

- *Blockchain pública:* de código abierto y distribuida, es decir, permite a cualquier persona participar como usuario, minero, desarrollador o miembro de la comunidad de forma libre, las transacciones que se realizan son totalmente transparentes, esto hace que cualquiera pueda examinar los detalles de las transacciones. Es una red descentralizada sin ningún individuo o entidad que controle qué transacciones se registran o el orden en que se procesan, donde cualquiera está abierto a unirse, independientemente de su ubicación, nacionalidad, etc.; por lo que es difícil para las autoridades cerrarla; además, cuenta con una expansión de red lenta y difícil, la participación es pseudónima, por lo que sus nodos

son desconocidos y poco confiables y no es propia para servicios financieros que requieren control de información centralizada.

- *Blockchain privada*: Conocidas como *blockchain* autorizadas, es cuando un propietario genera y administra *blockchain*. Es un sistema cerrado, donde los participantes necesitan consentimiento para unirse a la red, las transacciones son privadas y sólo las pueden realizar los participantes que tienen permiso. Es una red centralizada y son valiosas para las empresas que desean colaborar y compartir datos, pero no quieren que sus datos comerciales confidenciales sean visibles en una cadena de bloques pública, por lo que sus nodos son confiables.

- *Blockchain híbrida*: Es una combinación de *blockchain* público y privado los miembros de la red o las entidades dominantes pueden decidir qué transacciones pueden seguir siendo públicas y cuáles estarán abiertas a un grupo más pequeño de miembros; además, garantiza que las transacciones sean privadas pero verificables utilizando un historial inmutable en la cadena de bloques pública. Así, cada transacción debe ser verificada por una red masiva y, generalmente es confiable y segura; por lo que no requiere de una entidad central de gobierno o intermediarios para controlar las cosas.

  En la combinación hibrida cualquier alteración de una transacción debe realizarse bajo un proceso de verificación innato, por lo que es difícil que una sola entidad manipule la transacción o las entradas. Un aspecto importante es que, aunque los participantes tienen los mismos derechos para ver, editar y agregar su permiso a una transacción, la identidad de las partes involucradas en la transacción nunca se revela a otras partes de la red, es decir, los nodos son invitados y las transacciones son públicas, por lo que fortalece la seguridad de los participantes, resuelve problemas de lenta velocidad de transacciones y problemas de escalabilidad a participantes de red pública, Es una red adecuada para sistemas semi-cerrados, compuesto para pocas empresas (consorcios), podría usarse en instituciones financieras.

  Puede ayudar a construir herramientas a nivel empresarial de la tecnología de código abierto. Además, su sólida seguridad permite su uso en pagos transfronterizos confiables para financiación y comercio. Las aplicaciones industriales son otro aspecto en el que la cadena de bloques híbrida puede desempeñar un papel crucial, como viajes, energía, aviación, etc.

2.3 Empresas mexicanas *blockchain*

Recién, se realizó el primer estudio sobre el ecosistema de *blockchain* en México, por la empresa Innoventia (de Teknei y Hill House Capital) en donde se enlistan las empresas relacionadas con *blockchain* en el país. En dicho estudio se mapeo a las 81 empresas identificadas que corresponden a diferentes sectores y que de alguna forma utilizan como herramienta esta tecnología, mismas que se muestran en la figura 2.3.

Figura 2.3

Ecosistema *Blockchain* México

Fuente: Primer Estudio del Ecosistema Blockchain México, elaborado por Innoventia, 2019. Empresa de Servicios Blockchain, formada por Teknei y Hill House Capital.

Sobre este esquema, es importante comentar que hoy en día, el marco legal ha contribuido en gran medida a que se incrementen los *exchanges* en México con la consecuente adopción de inversión en criptomonedas. En las consultoras se pueden ver a las grandes de siempre; además de empresas que han visto una oportunidad de negocio y están invirtiendo en este rubro.

Los fondos de inversión también tienen un gran interés, ya que ven al *blockchain* como un vehículo adicional para invertir. En cuanto a la formación, se espera que se puedan incrementar las empresas que provean cursos y certificaciones para tener un mayor número de recursos humanos cualificados en el país. Respecto a las soluciones, ya hay varios usos, como la venta de contenido personal, registro de la propiedad, sector salud, contratos de compra-venta, entre otros.

La tecnología *blockchain* tiene la capacidad para resolver problemas políticos, sociales, industriales y económicos. En México tiene un gran campo de acción, dado que figura como una solución a la corrupción y la falta de transparencia. Además, *blockchain* en la industria, agiliza los procedimientos y reduce el margen de error. Es un sistema de registro distribuido que facilita el procesamiento de datos y la transparencia. Un proyecto *blockchain* bien aplicado, agiliza los procesos, los vuelve más confiables y transparentes. (Innovenia, 2019*).*

Por esto, es que las empresas Bitso, GBM, Lvna Capital, ConsenSys, Volabit, Exponent Capital y BIVA se unieron para formar *Blockchain* México, la primera asociación mexicana de este

sistema en el país, con el propósito de promover y fomentar el uso de *blockchain* y su principal objetivo es difundir la tecnología, que la conozcan en las universidades y los reguladores, hacer alianzas y lanzar productos, toda esta gama de acciones que promuevan el ecosistema de *blockchain* en el país, es decir, educar, promover y crear comunidad, así como generar mejores prácticas, a través de foros, pláticas y difusión sobre el uso, beneficios e impacto de la tecnología y alianzas. (Pontaza, Expansión 2018).

En México, en temas de transparencia esta es la tecnología ideal para que cualquier mexicano pueda saber de dónde sale un peso y donde termina. Los casos de mayor uso están las remesas y la transparencia. Específicamente, los sectores en los que se ve mayores beneficios al implementar esta tecnología son el financiero, gobierno, aseguradoras, consumo, medios y telecomunicaciones, turismo, farmacéuticas y salud.

Los principales retos que presenta *Blockchain* en México son, por un lado, la regulación, ya que no hay una sola Ley *blockchain*, para comprender las reglas que están detrás de *blockchain*, es necesario analizar cuál es el giro de la empresa; por ejemplo, la "Ley *Fintech*" en México habla en términos generales sobre las bases para regular las empresas que operan con criptomonedas, como es el caso del *bitcoin*; sin embargo, *blockchain* no puede obedecer a una sola ley, su regulación depende del uso que se le dé a *blockchain*. En segundo lugar, está la falta de personal calificado, ya que, *blockchain* al ser una tecnología nueva, aún tiene un largo camino por delante y la mayoría de las empresas que demandan profesionales de *blockchain* se ven obligadas a recurrir a talentos fuera del país.

2.3.1 Empresas *Fintech*.

Fintech es un término compuesto por las palabras inglesas Finance y Technology, significa tecnologías aplicadas a las finanzas, productos, servicios y mercados financieros. Son empresas que lideran el sector tecnológico aplicado a las finanzas e invocan el uso y aplicación en las empresas financieras de nuevas modalidades de servicios de la sociedad de la información que van surgiendo en los mercados para aplicar tecnologías eficientes y sistemas innovadores que mejoran la comunicación (Cassinello, Cervera, Ibáñez, López, 2017).

Las empresas *Fintech* utilizan la tecnología en sus modelos de negocio como habilitador principal de su oferta de productos y servicios financieros. Esta industria se caracteriza por marcos colaborativos y ágiles de trabajo para el desarrollo de soluciones y productos financieros distintos a los tradicionales (Cassinello, Cervera, Ibáñez, López, 2017).

(Nieto, 2019) refiere que de acuerdo a (Núñez, 2016), las empresas *Fintech* se caracterizan por su gran componente tecnológico y sus servicios financieros facilitan la vida cotidiana gracias a la innovación tecnológica, y dentro de sus principales actividades está la banca digital, los préstamos y créditos *online*, el cambio de divisas por medio de la red o los pagos online.

2.3.1.1 Propósitos y alcances.

Las *Fintechs* son aquéllas *startups*[8] (empresas emergentes) o empresas que desarrollan productos financieros totalmente digitales, con menor burocracia, mayor transparencia y que desafían al mercado dominado por los grandes bancos, es por eso que muchos las llaman "disruptivas". Éstas incorporan el *Smart Data*[9], siendo los datos el componente principal para crecer y ofrecer mayor eficiencia operativa y productividad. A diferencia de las entidades financieras tradicionales, ya que cuentan con la suficiente capacidad para adaptarse rápidamente a los cambios gracias a la generación, incorporación y análisis de datos.

Las *Fintechs* ofrecen las más diversas soluciones, como tarjeta de crédito, cuenta digital, tarjeta de débito, préstamos, seguros, y más. La tecnología es la gran ventaja competitiva con relación a las empresas tradicionales del sector y permiten que la mayoría de sus clientes controlen los productos a través de sus smartphones, sin necesidad de ir físicamente a una sucursal bancaria o casa de bolsa, y con costos bajísimos y a veces sin costos (libres de comisiones) para los usuarios, logrando crecer rápidamente.

El número de empresas que crean soluciones innovadoras para el sector financiero está creciendo. Se trata de una tendencia mundial para transformar la relación de las personas con el dinero.

Como refieren (Cassinello, Cervera, Ibáñez, López, 2017)*, e*l objetivo de las Instituciones *Fintech* es facilitar a los clientes (usuarios financieros) productos, instrumentos, contratos y servicios, tradicionalmente ofrecidos por la banca de forma analógica, o digital, pero con automatización limitada de procesos, de modo completamente virtual con las siguientes características:

- Sin mediación humana, a través de aplicaciones, plataformas o sistemas digitalizados.
- Remplazo de la intervención de intermediarios personales en la relación de las entidades con clientes y entre empresas.
- Creación de nuevas relaciones directas entre clientes sin mediación bancaria.

[8] Startup es una gran empresa en su etapa temprana; a diferencia de una Pyme, la Startup se basa en un negocio que será escalable más rápida y fácilmente, haciendo uso de tecnologías digitales", explica Morelos, director de Startupbootcamp Fintech México. Como su nombre lo indica, el término solamente aplica cuando el proyecto está en el arranque. Una vez que haya escalado dejará de llamarse Startup. Temporalidad, escalabilidad y crecimiento exponencial definen, a grandes rasgos, este tipo de emprendimientos, los cuales ocupan hoy el mayor interés de los inversionistas.

[9] "Smart Data" (Natalia Nieto, 2017), es un sistema capaz de recopilar gran cantidad de datos, al igual que el Big Data, pero que tiene un valor añadido ya que además de recoger la información también es capaz de analizarla.

2.3.1.2 Segmentos de mercado.

Las *Fintechs*, se han orientado principalmente a los segmentos de mercado que mayor impacto han tenido la crisis financiera: las Pymes y los pequeños ahorradores. Al investigar sobre las *Fintechs* se observó que los expertos señalan que los servicios de tecnología financiera ofrecidos por las *Fintechs*, va dirigida a conquistar a la generación de jóvenes "millenials"[10], que en su vida cotidiana conviven con la tecnología. Como dice Banal-Estañol, "este modelo de negocio se ajusta mejor a los crecientes segmentos de mercado como la generación de los millenials, que conviven con el uso de la tecnología", (Banal, 2016).

Más allá de emplear tecnología en las finanzas, las *Fintechs* se caracterizan por un nuevo modo de relacionarse en la contratación de servicios financieros, más cooperativo, colaborativo, democrático, desintermediado (desbancarizado en algunos casos) y promotor de la inclusión social financiera.

2.3.1.3 Operaciones habilitadoras.

Los modelos de negocio de las *Fintech* se basan en la aplicación de las tecnologías habilitadoras de soluciones. Las tecnologías innovadoras son parte esencial de los servicios que ofrecen las *Fintech*. Las principales habilitadoras son las siguientes *(Cassinello, Cervera, Ibáñez, López, 2017)*:

- *Uso de dispositivos móviles/smartphones y apps*: Facilitan el acceso a servicios a los usuarios mediante productos *fintech* mediante canales digitales y procesos virtuales en tiempo real.
- *Seguridad y biométricos*: Medio de autenticación mediante el reconocimiento facial, de voz, dactilar entre otros, para brindar seguridad y confianza al usuario.
- *API*: Interfaces que habilitan la interconexión entre plataformas.
- *Cloud computing*: Dan acceso a un mayor espacio de almacenamiento de información y acceso vía remota.
- *Legacy systems:* Sistemas o aplicaciones ya rezagados pero que aún siguen siendo utilizados por las instituciones financieras ya que son críticos en sus procesos.
- *Quantum computing*: Permite la superposición y enlazamiento de la información, dando a los ordenadores un poder de procesamiento superior a cualquier computadora tradicional.
- *Realidad aumentada*: Permite a los dispositivos incluir capas de información visual sobre el mundo real intentando ser parte del mismo.

[10] "Millenials". O generación Y, se refiere a los nacidos entre 1982 y 1994. algunos consideran el comienzo de la generación de los millenials desde 1980 y su término puede extenderse hasta el año 2000. Se considera una generación que creció con la tecnología y la cultura popular desarrollada entre los años 80 y 2000, son personas familiarizadas con la tecnología. Los millenials crecieron con la aparición de las primeras tecnologías y las redes sociales, conviviendo con ellas por mucho más tiempo que la generación anterior.

- *Inteligencia artificial:* Es una tecnología que se basa en algoritmos para eliminar errores humanos, automatizar procesos y reducir costos.
- *Big data*: Consiste en la recopilación, almacenamiento y procesamiento de grandes cantidades de datos que faciliten la toma de decisiones.
- *Blockchain:* Es un registro de transacciones permanente dentro de una red descentralizada que contiene información cronológicamente ligada, utilizando un código encriptado.

2.3.1.4 *Principales servicios.*

- *Medios de pago y transferencias:* Se refiere a plataformas dedicadas a la provisión de servicios de pago y transacciones a través de internet, de forma independiente a los bancos. Ofrecen soluciones sobre medios de pago electrónicos y canales digitales que hagan posible la ejecución de transacciones entre agentes económicos, sin la necesidad de utilizar dinero físico o de asistir a una sucursal. En este grupo también se pueden incluir servicios transaccionales como los cambios de divisas. (Nieto 2019). Los pagos y remesas han tenido un crecimiento importante en los últimos años derivado principalmente de factores geopolíticos.

  En este modelo de negocio es donde se observa mayor madurez debido al alto impacto que ha tenido el comercio en línea. Actualmente se cuenta con una gran disponibilidad de mecanismos de pago y de transferencia de dinero a través de plataformas para pagos móviles y comercio electrónico. La industria de pagos presenta tres tendencias principales: Comercio sin interrupciones, pagos móviles y soluciones vía *blockchain* y criptomonedas. (BANCOMEXT y PROMÉXICO, 2018).

  Así mismo, permite al usuario realizar y recibir transferencias de dinero. A comparación de la banca tradicional, estas *Fintechs* ofrecen al usuario: mejores tipos de cambio para transferencias en otras divisas. comisiones o costos adicionales menores. transferencias más rápidas, Eliminación de intermediarios bancarios para el procesamiento de las operaciones. Ejemplos NetPay, Openpay, Clip, Pagamobil (BANCOMEXT y PROMÉXICO, 2018).

- *Infraestructura para servicios financieros:* Se refiere a la creación y mejora de la tecnología existente y de los procesos de gestión para la prestación de servicios financieros. También, estas empresas ponen a disposición de otras *Fintech* o entidades financieras sus productos o servicios, sin tener relación directa con los clientes finales. *(Nieto 2019).*

- *Originación digital de créditos:* Modelo de negocio que proporciona servicios de solución a las empresas financieras para agilizar y hacer más eficientes los procesos de originación de créditos a través de una página *web* o una App móvil, reduciendo costos y tiempos en la originación y aprobación de los créditos por medio de herramientas digitales, en las cuales, los clientes pueden subir todos los documentos necesarios, revisar simulaciones de créditos,

informarse sobre todos los términos y condiciones, entre otras cosas. Los clientes esperan un proceso de solicitud de préstamo rápido, intuitivo y transparente con decisiones en tiempo real para todo tipo de créditos. Adaptar la otorgación de créditos a la realidad actual se convierte en una gran ventaja competitiva.

Las principales ventajas que ofrecen son:

a. Incremento de la productividad de los promotores y analistas de crédito.
b. Automatización de los procesos de aprobación de crédito.
c. 100% de visibilidad en el proceso.
d. Proceso de *backoffice* o mesa de control, incluyendo digitalización de documentos.
e. Agiliza la toma de decisiones a través de indicadores de gestión dinámicos alineados a los objetivos de cada negocio.
f. Sistema de ejecución de pagos y cobros.

- *Soluciones financieras para empresas.* Permiten incrementar la productividad y la eficiencia de las empresas a través de la automatización de procesos, generación de reportes oportunos y funcionalidad de predicción de patrones e identificación de tendencias. (BANCOMEXT y PROMÉXICO, 2018). Entre los servicios que ofrecen estas soluciones se encuentran los siguientes:

  a. Análisis de información e inteligencia del negocio: Los servicios que se proporcionan van desde la organización y vinculación de todas las cuentas bancarias hasta la categorización de manera automática de las transacciones. Permite a las organizaciones centralizar y organizar la información para apoyar la toma de decisiones de la empresa. Como ejemplo se tiene Fenergo y Glass. *(*BANCOMEXT y PROMEXICO, 2018).
  b. Contabilidad digital y facturación electrónica: organiza y optimiza los procesos contables de la empresa; así como captura, valida, organiza las facturas y genera reportes de manera automática. Como ejemplo se tiene Quickbooks y Contalink. (BANCOMEXT y PROMEXICO, 2018).

- *Finanzas personales y asesoría financiera*. Proporciona a los usuarios herramientas digitales para evaluar servicios financieros, proveer reportes sobre su comportamiento con respecto a ahorro, gasto y deuda para su adecuada gestión. Asimismo, ofrece soluciones para la gestión integral de portafolios de inversión, contrastan los perfiles de los clientes con sus objetivos y el riesgo asociado a los instrumentos financieros adicional a automatizar instrucciones de inversión. (BANCOMEXT y PROMÉXICO, 2018).

  Entre los principales beneficios se observan: la emisión de balances financieros en tiempo real, automatización de conciliaciones, generación de alertas al exceder monto planeado de

gastos, análisis de patrón de gastos y recomendaciones para el ahorro, control de tarjetas bancarias y notificación de transacciones (BANCOMEXT y PROMÉXICO, 2018):

a. Eficiencia financiera. Herramientas que apoyan la gestión del ahorro y la organización de gastos, para mejorar el control de las finanzas. Ejemplos Claritymoney.

b. Comparación. Aplicaciones que contrastan las características de diferentes productos financieros y permiten adquirirlos en línea. Ejemplos Money Super Market.

c. Score de crédito. Soluciones para el monitoreo y análisis de la información crediticia. Ejemplos Credit karma.

d. Impuestos. Plataformas de soporte para las declaraciones de impuestos. Ejemplos Track.

- *Intermediación de instrumentos financieros.* Se refiere a plataformas dedicadas a la compraventa de acciones u otros activos financieros que cotizan en bolsa. Otra alternativa a la bolsa son las aplicaciones de mercados de divisas y de *commodities* donde se invierte en materias primas o bienes primarios (Nieto 2019).

  Otorgan diversos beneficios desde un teléfono celular, como: disminución de las barreras de acceso a información, reducción de costos de operación, ejecución de operación y monitoreo de riesgos en tiempo real e interacción entre actores para la transmisión de conocimiento. Esta modalidad representa el mayor número de actores entre los segmentos emergentes, como son la gestión patrimonial, insurtech y la banca digital. (BANCOMEXT y PROMÉXICO, 2018).

  Las soluciones digitales para la inversión de activos financieros se clasifican en (BANCOMEXT y PROMÉXICO, 2018):

  a. Inversión (fondos de inversión, proyectos de infraestructura).
  b. Mercados de divisas (Soluciones FX).
  c. Criptomonedas. Ejemplo: Coinbase.
  d. Intercambio en el mercado accionario (trading). Ejemplo: inversión en el mercado accionario Robinhood Ejemplo: trading Etoro.
  e. Análisis económico/mercado, administración de riesgos y estimaciones. Ejemplo: Estimize.

- *Financiación alternativa.* Oportunidades para la inclusión financiera desarrollando nuevos modelos para captar usuarios a través de canales digitales de venta y operación, así como métodos innovadores para identificar y mitigar el riesgo crediticio. Se basa en el uso de plataformas de préstamos persona a persona (P2P lending) sin la presencia de una institución financiera, en donde el inversionista asume el riesgo del préstamo.

  Las *Fintechs* no fondean los préstamos que se otorgan, sus ingresos provienen de las comisiones por el uso de la plataforma. Las plataformas realizan estudios de viabilidad sobre los proyectos con la finalidad de calificar el riesgo de los mismos antes de ofrecerlos para capitalización. (BANCOMEXT y PROMÉXICO, 2018).

Las soluciones digitales de préstamos se clasifican en *(BANCOMEXT y PROMÉXICO, 2018)*:

a. Crowdlending Permite a las empresas obtener préstamos de inversores individuales o múltiples, tanto privados como institucionales, a través de una plataforma de intermediación en línea. Ejemplos Funding Circle, Peerform.

b. Marketplace lending (P2P lending) Ofrece a los usuarios la opción de realizar solicitudes de préstamos en un mercado en línea para encontrar actores que inviertan buscando mejores condiciones de rendimiento que las disponibles en la oferta tradicional. Estas plataformas utilizan algoritmos para identificar el riesgo crediticio de los prestatarios y optimizar las tasas de crédito y rendimiento. Ejemplos Upstart, Prosper.

- *Insurtech*. La tecnología de seguros busca eficientar la industria de seguros ofreciendo soluciones para la contratación y operación de productos que ofrecen las compañías aseguradoras; tales como pólizas ultra personalizadas, prestaciones y seguros sociales y el uso de los datos provenientes de dispositivos móviles para fijar precios de forma dinámica en las primas de acuerdo con el comportamiento observado. Por mencionar algunas de las insurtechs en México están WeeCompany, MangoLife, Truvius y Salud Cercana. *(BANCOMEXT y PROMÉXICO, 2018).*

- *Criptomonedas y blockchain*

a) Los *bitcoins* son monedas virtuales que tienen el mismo valor que el dinero que solo funcionan en internet. Se considera un sistema de pago seguro y con la característica de ser una moneda descentralizada. A diferencia de las otras plataformas *fintech* es que el *bitcoin* no tiene propietario y los usuarios de esta moneda quienes controlan su valor y uso. Opera mediante la tecnología *blockchain*, diseñada para ser la base común y descentralizada para que empresas o agentes de un sector puedan compartir información, servicios o procesos.

b) Los ICO *(Initial Coin Offering),* es decir, oferta inicial de moneda, es un modelo similar al IPO (*Initial Public Offering)*, término que se utiliza cuando una empresa sale a bolsa y quiere ofrecer las acciones a los posibles inversores a cambio de dinero. (Nieto 2018).

ICO de capital, recauda mediante financiamiento colectivo (crowdfunding) para su posterior bursatilización en cripto-bolsas, ICO de deuda. Sirve para recaudar fondos para sus operaciones emitiendo bonos o préstamos sindicados sobre una plataforma *blockchain*, sin necesidad de intermediarios o cumplimientos regulatorios. En el caso de las criptomonedas, se otorgan *tokens* virtuales en lugar de acciones a los inversionistas. (Nieto 2018, *BANCOMEXT y PROMÉXICO, 2018)*).

Cuando se decide utilizar la tecnología de *blockchain* para un uso especial tiene que existir una moneda asociada generalmente llamada "*token*" para evitar que se confunda el proyecto

con una nueva moneda. Cambiando estos *tokens* pre-minados por dinero, pueden usarse en un proyecto para realizar pagos por servicios específicos.

ICO de capital, recauda mediante financiamiento colectivo (crowdfunding) para su posterior bursatilización en cripto-bolsas, ICO de deuda. Sirve para recaudar fondos para sus operaciones emitiendo bonos o préstamos sindicados sobre una plataforma *blockchain*. Se automatiza la originación, distribución, asignación y ejecución de un contrato a través de una red *blockchain* (smart contracts).

Por último, el Agrocoin es el primer token en México, cuyo valor está vinculado directamente a un commodity del mundo real, la cual invierte en la industria agraria enfocada en la cosecha de habanero. Con unos meses de operar en el país, la criptomoneda Agrocoin ha recabado poco más de 21 millones de pesos por parte de 475 inversionistas y ya comenzó a dar rendimientos. (BANCOMEXT y PROMÉXICO, 2018).

- *Entidades financieras disruptivas*. El negocio bancario está en constante transformación obligando a la banca tradicional a competir y a la vez colaborar con empresas enfocadas en la provisión alternativa de productos y servicios financieros a través de canales digitales, lo que permite ofrecer una mejor experiencia al cliente y ofertas altamente personalizadas.

  Entre los principales servicios que ofrecen este tipo de bancos se encuentran:

  a. Sistemas de pagos. Los clientes pueden enviar o recibir dinero a través de aplicaciones móviles.
  b. Préstamos. Los bancos ofrecen préstamos a través de aplicaciones móviles o sus páginas de Internet.
  c. Robo-advisors. Ofrecen asesoría financiera a través de inteligencia artificial en lugar de un asesor financiero tradicional. BANCOS DIGITALES.
  d. Administración del dinero. A través de una plataforma móvil, ofrecen al usuario apoyo y asesoría financiera a partir del análisis de sus hábitos de consumo y ahorro.

  Algunos ejemplos de este tipo de soluciones son: Standard, Chartered, Bank Mobile, Digibank y Hello bank.

- *Soluciones tecnológicas:* buscan proveer requerimientos operativos y de información para dar cumplimiento a requisitos regulatorios y de gobierno corporativo. Modelo de servicio que utilizan tecnología de computación en la nube y esquemas de software como servicio (SaaS) para ayudar a las empresas a cumplir con las regulaciones de forma más eficiente y menos costosa.
  Las regtech, utilizan como principales herramientas habilitadoras:

  a. *Cloud computing:* Permite guardar la información de una Institución en una sola.
  b. *Big data*: Son utilizadas para el procesamiento de información de forma eficiente.

c. Inteligencia Artificial: Es utilizada para capturar y aplicar el conocimiento y el comportamiento humano.
d. Biométricos*:* Permite identificar al cliente por medio de identificación física y características conductuales (KYC- Know Your Customer).
e. *Blockchain* Permite el desarrollo de plataformas para el intercambio de información con las Instituciones y Reguladores.
f. *API:* Ayuda a tener conexiones entre los diferentes softwares de una Institución permitiendo comunicarse entre sí.
g. *RPA:* Permite la automatización de procesos de la Institución.

2.3.1.5 Segmentos *Fintech*.

Las *Fintechs* mexicanas lideran el mercado latinoamericano en cuanto a la cantidad que están operando. En México y América Latina tienen un gran potencial debido a la gran cantidad de población que no está bancarizada y América Latina hay más teléfonos celulares que en todo Estados Unidos y Canadá[11]

Al cierre de agosto de 2018, *Fintech* México es el segundo mayor ecosistema de Latinoamérica por número de empresas, las cuales han crecido a 40. Es importante señalar que los segmentos de "pagos y remesas" así como "préstamos" son los que más startup *Fintech* concentran. (BANCOMEXT y PROMÉXICO, 2018).

Cuadro 2.2
Segmentos *Fintech* en México

Fintech	Segmento	Participación
334 Startups	Pagos y remesas	22%
	Préstamos	22%
	Gestión de finanzas empresariales	13%
	Gestión de finanzas personales	11%
	Otros	10%
	Crowdfunding	9%
	Tecnologías empresariales para instituciones financieras	7%
	Seguros	6%

Fuente: (BANCOMEXT y PROMÉXICO, 2018)

[11] Recuperado en https://www.responsabilidadsocial.net/las-empresas-fintech-definicion-tipos-objetivos-ejemplos).

Los principales convenios entre Instituciones Financieras y *Fintechs* son (BANCOMEX Y PROMÉXICO, 2018):

a) BBVA Bancomer. - Openpay derivado del programa Open Talent:
   - Busca en mejorar la experiencia del cliente.
   - Ofrece soluciones de pagos avanzadas y funcionalidades para comercios.
   - Esta alianza surgió de su programa BBVA Open Talent 2015.

b) Santander – Endeavor México:
   - Radar Santander. Busca identificar Fintech de alto impacto en la categoría de pagos digitales.
   - Las cuatro Fintech seleccionadas serán parte de un programa de aceleración de cinco meses. Scotiabank – Kabbage Alianza enfocada en el segmento de préstamos para PyME.

c) AcertumBank:
   - La marca pertenece a Banco Azteca.
   - Ofrece servicios de débito, de inversiones, tarjeta de crédito, así como pagos y transferencias.

d) Banorte IXE, Santander, Bancomer, Banamex y HSBC – *PayPal*:
   - Enfocada en mejorar la experiencia del cliente para compras en línea por lo que permite vincular una tarjeta de débito o crédito con la plataforma de pagos de *PayPal*.
   - Permite el uso de SPEI para realizar transferencias entre la cuenta del Banco y la de *PayPal*.
   - Ofrece una experiencia bancaria 100% móvil.

e) HeyBanco:
   - Ofrece la experiencia bancaria tradicional a través de una App.
   - Ofrece servicios como cuentas bancarias, así como transferencias de dinero y pagos.
   - La cuenta es respaldada por BanRegio.

2.3.1.6 Regulación y Supervisión.

Debido al crecimiento del sector *Fintech* y la falta de regulación, limitaba a la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (Condusef) en la defensa de los inversionistas, y después del fraude de la *startup Foodies,* es que las autoridades financieras mexicanas deciden regular estas instituciones con el objeto de brindar seguridad y condiciones jurídicas necesarias a todos los participantes del sector financiero.

Así es como el 9 de marzo de 2018, se promulgó la Ley para Regular las Instituciones de Tecnología Financiera “Ley *Fintech*”. A fin de ajustar la legislación mexicana, también se modificaron las siguientes leyes, entre otras, la Ley del Mercado de Valores, se reformó para excluir de su ámbito de regulación la oferta e intermediación de valores y la negociación con valores a través de Instituciones de Tecnología Financiera y se facultó a la CNBV para emitir disposiciones que regulen el ofrecimiento de servicios automatizados de asesoría y gestión de inversión (Lloreda Camacho & Co., 2019)

Por su parte, la Ley de Instituciones de Crédito se reformó para regular con mayor precisión el uso de tecnología en los bancos para el desarrollo de sus actividades y que las actividades realizadas por las *Fintechs*, no sean consideradas captación de recursos. Posteriormente, el 11 de septiembre de 2018, se emitió la regulación secundaria aplicable a Fintech, que comprenden las Disposiciones de carácter general aplicables a las Instituciones de Tecnología Financiera emitidas por la CNBV en su Circular 12/2018 dirigida a las Instituciones de Fondos de Pago.

Electrónico emitida por el Banco de México y las Disposiciones de carácter general a que se refiere el Artículo 58 de la Ley para Regular las Instituciones de Tecnología Financiera emitidas por la Secretaría de Hacienda y Crédito Público.

Por lo que respecta a la supervisión, la “Ley *Fintech*”, señala que la supervisión del cumplimiento de las ITF a la regulación de ésta Ley y las disposiciones que provengan de ella, estará a cargo de la CNBV apegándose a su Ley y reglamentos respectivos y demás disposiciones aplicables. Así pues, la CNBV puede efectuar visitas de inspección a las ITF con el objeto de revisar, verificar, comprobar y evaluar las actividades que realicen. Asimismo, puede investigar hechos, actos u omisiones de los que se pueda presumir una violación a esta Ley y otras disposiciones que se deriven de ésta.

Así mismo, dichas visitas de inspección pueden ser i. ordinarias: conforme a un programa anual establecido por la CNBV, ii. especiales: sin estar en el programa anual, se realizan para examinar y/o corregir situaciones especiales operativas, seguimiento a resultados obtenidos en una visita de inspección, o por presentarse cambios en la situación contable, jurídica o económica financiera o administrativa en una ITF y iii. de investigación: cuando la CNBV tenga indicios que puedan desprender la realización de una conducta que contravenga lo previsto en esta Ley y demás disposiciones que se deriven de esta.

También Banco de México, está facultado para supervisar el cumplimiento de las ITF respecto de las disposiciones que este emita, en términos de esta Ley; por lo que podrá ejercer las atribuciones que en materia de supervisión le confiere la Ley de Banco de México. Para estos efectos, las ITF, quedan comprendidas entre los intermediarios financieros a que se refiere la Ley de Banco de México.

Por otro lado, cabe destacar que actualmente, la CNBV supervisa a 5,069 entidades, dentro de los cuales se encuentra el sector de ITF. Dicha comisión, señala que la supervisión en materia

de PLD/FT se encuentra a la vanguardia de las normas internacionales y las tendencias mundiales, donde, en su regulación y supervisión, intervienen varias autoridades multidisciplinarias y técnicas. Y se emitieron lineamientos en materia de PLD/FT como herramienta para llevar a cabo las funciones de inspección donde se incluyen los procedimientos, principios y una guía para el establecimiento de un régimen preventivo que facilite el cumplimiento de las obligaciones y normativa de PLD/FT, así como de una gestión de riesgos, por parte de los sujetos supervisados. Considerando que un régimen preventivo efectivo requiere de una gestión de riesgos, es que estos lineamientos también ofrecen una guía para identificar y controlar los riesgos asociados con el LD/FT.

También la LFPIORPI, menciona que la SHCP puede realizar visitas de verificación a quien realice Actividades Vulnerables (Activos Virtuales, entre otras), para comprobar el cumplimiento de las obligaciones previstas en dicha Ley, considerando que la verificación solo podrá abarcar actos u operaciones consideradas como Actividades Vulnerables en los términos de la Ley antes mencionada.

Por lo tanto, las ITF son autorizadas, reguladas y supervisadas por la SHCP, la CNBV y el Banco de México.

Capítulo 3.
Efecto del anonimato de la tecnología *blockchain*

3.1 Tecnología *blockchain*

Actualmente, para muchos, la tecnología *blockchain* aún es un tema desconocido o incluso temeroso. De hecho, todavía hay quienes se muestran escépticos de que se use esta tecnología en el futuro, porque todavía estamos muy temprano en el desarrollo y la adopción generalizada de esta tecnología, e inclusive desconocida para muchas personas. Se puede decir que para 2022 *blockchain* es lo que fue para finales de la década de 1990 el Internet. Al parecer, está aquí para quedarse, por ello su importancia de entender cómo funciona.

La tecnología *blockchain* hace posible que las criptomonedas, como es el caso de *bitcoin*, funcionen de la misma manera que el Internet hace posible el correo electrónico. Y para entender de una forma sencilla cómo funciona esta tecnología, se hablará de la cadena de bloques, la minería y seguridad, partiendo de que en las transacciones con criptomonedas participan los usuarios y mineros.

Las criptomonedas basadas en *blockchain* cuentan con dos tipos de participantes: I. Usuarios que desean realizar transacciones con criptomoneda; y, II. Mineros: que actúan como creadores y validadores de las transacciones.

3.1.1 Cadena de bloques.

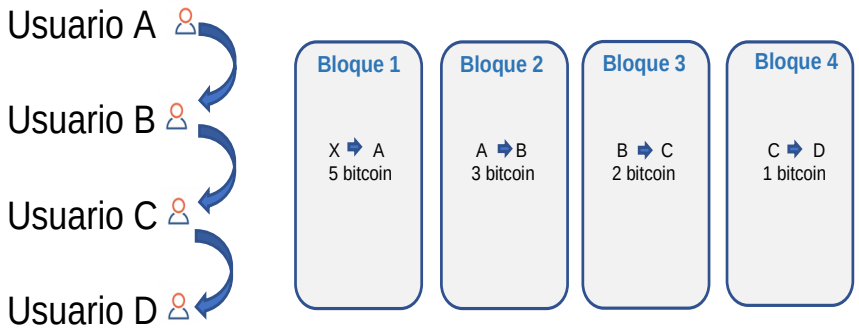
Al estar la tecnología *blockchain* detrás de la cadena de bloques, ésta no puede ser propiedad, es como Internet. Cualquiera puede usar la tecnología para ejecutar y poseer sus propias cadenas de bloques.

Recordemos que la cadena de bloques es un libro de contabilidad digital distribuido, inmutable con diferentes usos, además de las criptomonedas (Darlington, 2021). Como libro de contabilidad, se registran todas las transacciones realizadas por los usuarios, y cada transacción o registro en el libro mayor, se almacena en un "bloque". Por ejemplo, en el bloque 1 el usuario X le manda al usuario A 5 *bitcoins*, en el bloque 2 el usuario A le manda al usuario B 3 *bitcoins* y así sucesivamente; además se determina el saldo de cada usuario como se muestra a continuación:

Usuario A: Recibe 5 y manda 3 (5 – 3 +1) = 3
Usuario B: Recibe 3 y manda 2 (3-2) =1
Usuario C: Recibe 2 y manda 1 (2-1) = 1

A continuación, se presenta un esquema que muestra el registro de las transacciones con *bitcoin* en una cadena de bloques.

Figura 3.1
Funcionamiento de la cadena de bloques

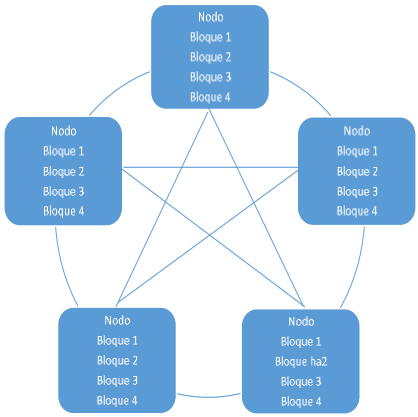


Fuente: elaboración propia, de Ávila, 2018. ¿Cómo se debe plantear un curso introductorio a la tecnología Blockchain, que haga uso de la información y los trabajos disponibles, y que también permita aplicar tal tecnología al contexto colombiano?

Ahora bien, en el caso de registrar el bloque 5, no se puede recibir transacciones con un monto mayor al saldo que tenga cada usuario; por ejemplo, del usuario A no se puede recibir más de 2 *bitcoins*.

Los bloques son registrados por los mineros en cada uno de los nodos de la red, es decir, las transacciones quedan registradas en todos los nodos de la red y cualquier usuario de la red puede tener acceso a ellas en cualquier momento y verificarlas.

Figura 3.2
Estructura bloques en la tecnología *blockchain*



Fuente: elaboración propia, de acuerdo a Soto, 2021. ¿Qué es la tecnología blockchain y cómo funciona?

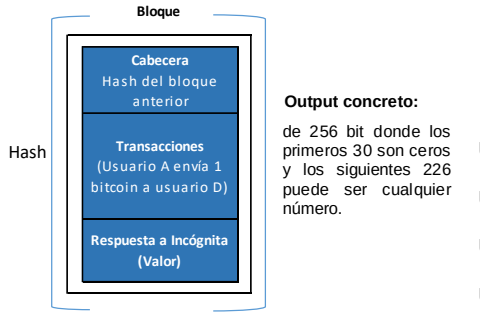
El orden de los bloques es importante, para poder determinar el saldo de los usuarios, ya que se tienen que construir todas sus transacciones de inicio a fin. Aproximadamente se registran como 2,300 transacciones por bloque. Ahora, con un ejemplo, se muestra cómo funciona *blockchain* a través de una transacción con *bitcoin*. Supongamos que se va a construir el bloque (5) con una nueva transacción, de acuerdo a la figura 3.2.

En la red están todos los mineros escuchando a todos los usuarios, esperando a que salga una transacción. La transacción se da, donde el usuario A le envía 1 *bitcoins* al usuario D, los cinco mineros van a hacer lo mismo, en el bloque nuevo van a construir una cabecera para lo cual, escogen el bloque anterior (bloque 4) hacen su hash (firma digital/ huella dactilar de un input) y la escriben en la cabecera del bloque (5).

Así es como se respeta el orden de los bloques y también se protege la integridad de la cadena, ya que si se quisiera cambiar un bits del bloque 3, cambiaría la huella del bloque (3) y entonces se presentaría una discontinuidad del hash de este bloque y del siguiente (4) y se rompería la cadena, entonces, si se quisiera transcribir una transacción del bloque anterior (3), se tendría que cambiar en todos los bloques subsecuentes, porque al cambiar una transacción en un bloque, se modifica su hash, y habría que cambiar el *hash* de entradas y salidas de todos los bloques subsecuentes. Por eso, todos los bloques futuros dependen de la información de los bloques anteriores, y esta dependencia de un bloque al siguiente, forma una cadena segura: la cadena de bloques.

Después de escribir el *hash*, los mineros toman la transacción del usuario A que le envía 1 *bitcoins* al usuario D y la colocan en bloque (5) y, por último, se dan a la tarea de dar respuesta a la incógnita que es aquél valor que hace que cuando pones todo junto (cabecera, transacción y valor de la incógnita) en la función de *hash* hace que el valor del output, sea un valor compuesto de 256 bits que empiece primero con 30 ceros y después 226 dígitos.

Figura 3.3
Ejemplo de la estructura de un output



Fuente: elaboración propia, de Ávila, 2018. ¿Cómo se debe plantear un curso introductorio a la tecnología Blockchain, que haga uso de la información y los trabajos disponibles, y que también permita aplicar tal tecnología al contexto colombiano?

Para encontrar ese valor, no existe fórmula alguna, más que ir haciendo pruebas; y así es como inicia una competencia entre todos los mineros para realizar el máximo de cálculos por segundo poniendo valores aleatorios y ver quién es el primero en encontrar el valor que den con la condición para generar un output de 256 bits donde los primeros 30 números sean cero y los 226 restantes dígitos diferentes y así se evita un choque de nodos, ya que es muy difícil de encontrar dicho valor.

La longitud de los ceros en el caso de *bitcoin* se definió de 30 ceros para hacer que la escritura de cada bloque tarde un tiempo de 10 minutos, sin embargo, cada criptomoneda define su propio nivel de dificultad para separar el tiempo.

Una cadena de bloques pública es un modelo de contabilidad de triple entrada donde las transacciones en una cadena de bloques se sellan criptográficamente mediante una tercera entrada, creando un registro a prueba de manipulaciones de transacciones almacenadas en bloques y que éstas sean verificadas por un mecanismo de consenso distribuido. Este mecanismo de consenso también asegura que se incorporen nuevos bloques a cualquier *blockchain*. Un ejemplo de esto es lo que se llama la prueba de trabajo (PoW). (Darlington, 2021)

3.1.2 Minería.

Las personas detrás de la red y los sistemas de cómputo contratados para la validación de las transacciones es lo que se conoce como “mineros” y su actividad como “minería”, cuyo trabajo es retribuido con nuevas unidades de *bitcoin*.

(Bit2me Academy, 2021) señala que la misión de la minería es básicamente certificar que nadie usa las monedas dos veces la nueva creación del registro contable y que nadie pueda introducir en el mercado *bitcoin*s falsos.

En lugar de que un banco centralmente registre las transacciones, el libro mayor es actualizado por un minero y todos los usuarios y mineros almacenan la actualización de las transacciones.

La minería no es universal para todas las cadenas de bloques; es un mecanismo de consenso utilizado actualmente por *bitcoin* y ethereum, sin embargo, ethereum pretende pasar a otro, en 2022. (Darlington, 2021).

La minería (PoW, término técnico), es el mecanismo de consenso original que se basa en la criptografía, la cual usa ecuaciones matemáticas que solo las computadoras pueden resolver. (Darlington, 2021).

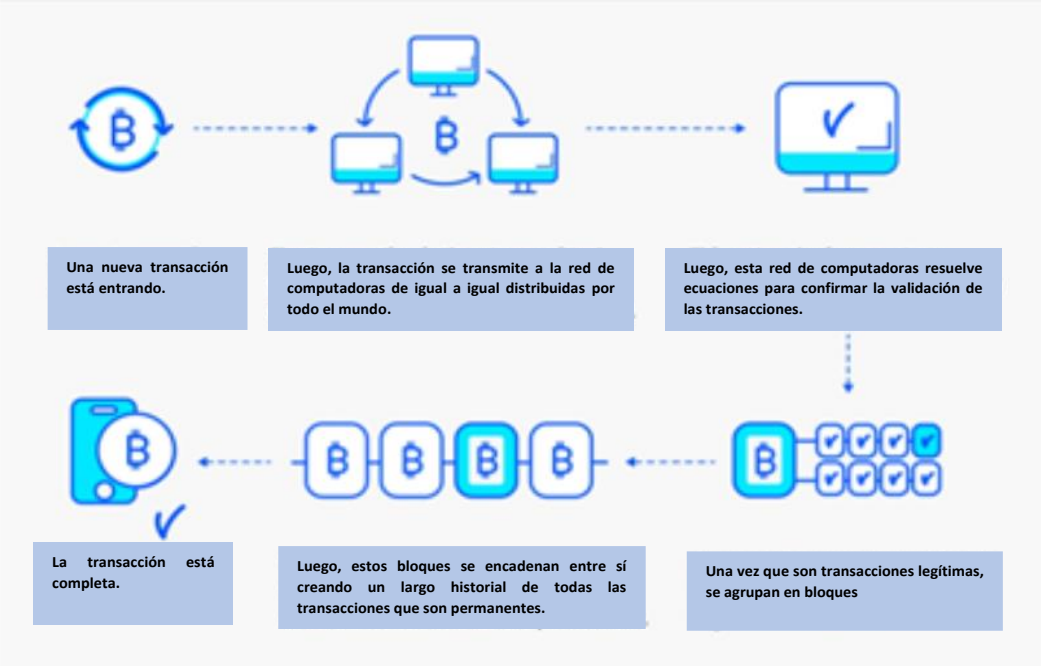
¿Cómo funciona el proceso de *bitcoin* en *blockchain*? (Darlington, 2021) explica que: “Al enviar *bitcoin*, paga una pequeña tarifa (en *bitcoin*) por una red de computadoras para confirmar que su

transacción es válida. Luego, su transacción se agrupa con otras transacciones pendientes en una cola para agregarse a un nuevo bloque.

Las computadoras (nodos) luego trabajan para validar esta lista de transacciones en el bloque resolviendo un problema matemático complejo para generar un hash, que es un número hexadecimal de 64 dígitos. Una vez resuelto, el bloque se agrega a la red y su tarifa, combinada con todas las demás tarifas de transacción en ese bloque, es la recompensa del minero."

Figura 3.4

Funcionamiento de *bitcoin* en *blockchain*.



Fuente: Darlington, 2021. ¿Qué es la tecnología Blockchain?

Cada vez que se agrega un bloque nuevo a la red, se le asigna una clave única. Para obtener una clave, se toma la clave e información del bloque anterior y se ingresan en una fórmula. Conforme se van agregando nuevos bloques, se vuelven cada vez más seguros y más difíciles de manipular.

Cabe agregar, que la minería (PoW) presenta dos grandes desventajas, por un lado, usa mucha electricidad y por otra, sólo puede procesar un número limitado de transacciones simultáneamente (siete para *Bitcoin*), por ello es que las transacciones tardar por lo menos diez minutos.

Hay otro mecanismo de consenso y éste es (PoS), que aún utiliza algoritmos criptográficos para la validación, aquí las transacciones son validadas por un validador elegido en función de del número de monedas que tienen, también conocido como su participación. Aquí, técnicamente no

se está minando y, por lo tanto, no hay recompensa en bloque. Los bloques están 'forjados'. Los que participan en este proceso bloquean una cantidad específica de monedas en la red. Entre más participe una persona, tendrá más poder de extracción y posibilidades de ser seleccionada como validador para el siguiente bloque. (Darlington, 2021).

Además, para asegurar que los de mayor cantidad de monedas no siempre sean seleccionados, se utilizan otros métodos de selección, como la selección aleatoria de bloques (se escogen los falsificadores con la apuesta más alta y el valor de *hash* más bajo) y la selección de la edad de las monedas (los falsificadores se seleccionan en función del tiempo que han retenido sus monedas). En este mecanismo, los tiempos de transacción son más rápidos y menos costos. Las criptomonedas Neo y *Dash*, por ejemplo, pueden enviar y recibir transacciones en segundos.

Por último, explicado de forma más sencilla, los mineros revisan las transacciones y reúnen las últimas transacciones creadas en un grupo llamado bloque. El conjunto de los bloques se puede comparar con el conjunto de páginas de un libro mayor (libro de contabilidad), el cual certifica todos los movimientos y el saldo de los usuarios.

Los mineros, son los participantes de la red que juegan un papel fundamental, ya que son los responsables de validar y agrupar las transacciones en bloques, retransmitirlas y registrarlas, además, emplean un alto poder computacional para resolver un *puzzle* criptográfico[12] para validar cada bloque. Los mineros se localizan principalmente en China, América del Norte, Europa del Norte y del Este, es donde hay más granjas de minería y se consume más energía, ya que se requiere de lugares fríos (con bajas temperaturas), donde la energía sea barata, la conexión de internet sea rápida. (Coty de Monteverde, 2019).

3.1.3 Seguridad.

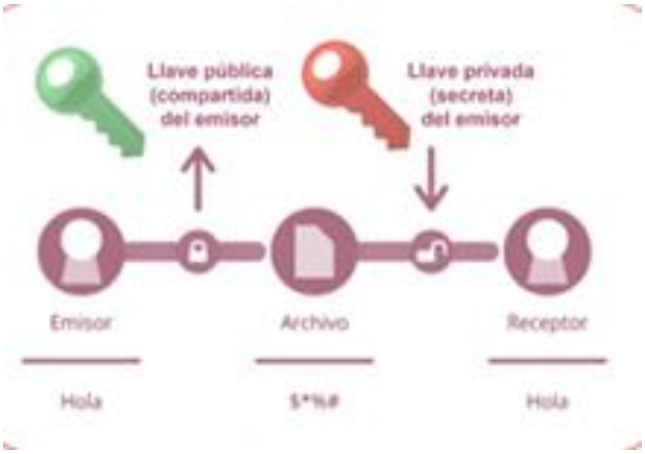
IBM, señala que la tecnología *blockchain* crea una estructura de datos con cualidades de seguridad inherentes basada en la criptografía, descentralización y el consenso, que garantizan la confianza en las transacciones. Cuando aparece un nuevo bloque, éste se conecta a todos los bloques anteriores en una cadena criptográfica, por lo que es casi imposible manipularlo. Además, las transacciones, en los bloques se validan y acuerdan mediante un consenso, garantizando que éstas sean verdaderas y correctas.

Ahora, se hablará un poco de la criptografía, ya que ésta le da confianza y seguridad a la red *blockchain*. La criptografía asimétrica, conocida como criptografía de llave pública (compartida) se utiliza para que el emisor pueda encriptar y cifrar un mensaje y una privada (secreta que uno se la queda) para que el receptor pueda desencriptar y descifrar el mensaje para poder leerlo. Para poder descifrar un mensaje es indispensable contar con la llave privada. Para entenderse

[12] *Puzzle criptográfico*: se refiere a un reto que crea un elemento interviniente en una comunicación -la etiqueta RFID- para que otro elemento que hace una petición sobre el primero -el lector- lo resuelva invirtiendo así tiempo y recursos computacionales con el propósito de evitar la participación de participantes deshonestos en la comunicación. (Monasterio, 2012).

mejor, se puede decir que las claves son como la contraseña o firma digital de una cuenta bancaria que van ligada a la dirección de uno. Las claves pueden ser invertibles. Estas claves, sirven para firmar y comprobar la autentificación, es decir, comprobar firma. (Coty de Monteverde, 2019).

Figura 3.5
Claves Pública y Privada sobre la que se basa la criptografía



Fuente: Coty de Monteverde, 2019. Institute for Advancer Management (CEU IAM). Blockchain y su aplicación en el ámbito financiero.

(Houben y Snyers, 2018, p. 20), la combinación de llaves público-privadas basada en la criptografía, "*es la técnica de proteger información transformándola (encriptándola) en un formato ilegible que solo puede ser descifrado (o desencriptado) por alguien que posee una llave secreta*".

Para tener acceso a los *bitcoins* que se encuentran almacenados en la cadena de bloques (*blockchain*), un usuario debe registrar en la billetera, una contraseña para descifrar temporalmente la llave privada (Franco, 2015).

Se puede decir que las llaves públicas: son como un número de cuenta bancaria en el que el usuario recibe fondos y las llaves privadas: son el número de identificación personal secreto, clave o PIN de dicha cuenta bancaria que permite usar los *bitcoins*. También, "crean las firmas requeridas para gastar los *bitcoins* al demostrar la propiedad de los fondos utilizados en una transacción". (Antonopoulos, 2017, p. 58).

En otras palabras, para transferir *bitcoins* de una dirección a otra, la transacción debe firmarse con la llave privada.

Las redes *blockchain* pueden variar sobre quién puede participar y quién tiene acceso a los datos:

- Redes públicas: generalmente permiten que cualquiera se una y que los participantes se mantengan en el anonimato. Utilizan computadoras conectadas a Internet para validar

transacciones y lograr consenso. Como ejemplo se tiene *bitcoin*, donde las computadoras de la red (mineros) tratan de resolver un problema criptográfico para crear una prueba de trabajo y validar la transacción. Aparte de las claves públicas, hay pocos controles de identidad y acceso.

- Redes privadas: usan la identidad para confirmar la membresía y los privilegios de acceso y normalmente, sólo permiten que se unan organizaciones conocidas. Se unen las organizaciones para forman una "red comercial" privada, exclusiva para miembros. Es una red autorizada que logra el consenso a través de un "respaldo selectivo", donde los usuarios conocidos verifican las transacciones. Solo los miembros con acceso y permisos especiales pueden mantener el libro de transacciones. Requiere más controles de identidad y acceso.

Además, señala que, si bien es cierto que la tecnología *blockchain* opera a prueba de manipulaciones, las redes *blockchain* no son inmunes a los ataques cibernéticos y al fraude. Se pueden manipular vulnerabilidades conocidas en la infraestructura de *blockchain* en ataques y fraudes, como lo han sido la explotación de códigos, llave robadas, computadoras pirateadas.

Aunque la tecnología *blockchain* tiene mecanismos de seguridad por diseño, en algunas funcionalidades es insegura, principalmente cuando los usuarios no están conscientes, de los riesgos de ciberseguridad. (López, 2021).

Uno de los aspectos más críticos en *blockchain* es la protección de la clave privada o el mecanismo de intercambio de claves (Pública-Privada), ya que son más primitivos que una “firma electrónica cualificada” depurada y consolidada. (López, 2021).

Por otro lado, también es importante comentar sobre el trilema de *blockchain* o escalabilidad. Normalmente, los proyectos de *blockchain* se basan en sus principales propiedades: descentralización, escalabilidad y seguridad, y los desarrolladores normalmente tratan de equilibrarlos. Sin embargo, frecuentemente tienen que sacrificar uno por los otros.

El término “trilema *blockchain*” conocido como “trilema de escalabilidad” (Buterin), se refiere a que:

- En la descentralización, las decisiones se toman por consenso sobre una red distribuida de computadoras; por lo que el envío de transacciones lleva más tiempo al requerir varias confirmaciones para validar una transacción. Por eso, *Bitcoin* es lento.

- La escalabilidad, es la capacidad del sistema para hacer frente a un número creciente de transacciones y es esencial, debido a que cualquier sistema debe ser eficiente a medida que más personas lo utilicen. Para lograr la escalabilidad, a menudo se hace a costa de la descentralización.

Como ejemplo de ello, es que mientras *Bitcoin* puede procesar siete transacciones por segundo, Ethereum treinta y las compañías de tarjetas de crédito 5,000, con la capacidad de procesar mucho más si es necesario. En el caso de Visa puede procesar hasta 24,000 por segundo.

- Para (López, 2021), la seguridad es la capacidad que tiene una cadena de bloques para protegerse de los ataques. Sin embargo, los intercambios y el código fuente han sido pirateados en muchas ocasiones, no obstante, muchos desarrolladores se enfocan en la escalabilidad y descentralización a expensas de la seguridad.

Para IBM, la seguridad de la cadena de bloques es un sistema integral de gestión de riesgos para una red de cadena de bloques, que utiliza marcos de ciberseguridad, servicios de garantía y mejores prácticas para reducir los riesgos contra ataques y fraude.

Por otro lado (López, 2021), afirma que la tecnología *blockchain* no es 100% segura. Señala que, en el ámbito de las criptomonedas, se han experimentado explotaciones de vulnerabilidades que han tenido repercusión y han demostrado debilidades inherentes en la seguridad de la *Blockchain* y, la "Inyección de código externo", es una de las vulnerabilidades más graves "que hace referencia a un posible código malicioso externo no controlado" que surgen cuando hay la necesidad de corregir un error o añadir una funcionalidad a través de esa "referencia" entonces se abren vectores de ataque que pueden afectar a la integridad de la cadena de bloques, intencionadamente o por un error humano.

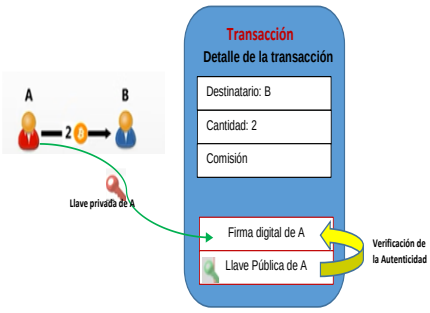
Después de abordar los participantes en la red de *Bitcoin y blockchain*, como usuarios, mineros, billeteras, etc., y la seguridad, se muestra cómo son las transacciones de *bitcoin*, ya que éstas son la parte más importante de todo el sistema.

3.1.4 Transaccionalidad.

Después de entender la cadena de bloques, la minería y la seguridad de *blockchain*, ahora se explicará cómo es una transacción, que es una de las partes centrales del sistema *Bitcoin*, ya que, mediante ésta, se transfiere el dinero entre las cuentas de los usuarios.

Figura 3.6

Ilustración de una transacción de *bitcoin*



Fuente: Coty de Monteverde, 2019. *Institute for Advancer Management (CEU IAM). Blockchain* y su aplicación en el ámbito financiero.

Una transacción comprende: el destinatario; la cantidad de *bitcoins* que va a transferir; la comisión; la firma digital del transmisor (usuario A), que es su llave privada y es la que no comparte la transacción; y los validadores (nodos) que van a verificar que la transacción sea auténtica, es decir que realmente es el usuario A quien está realizando la transacción, porque al aplicar la llave pública se desencripta, y si fuera una llave privada inventada o diferente, con la llave pública no se podría desencriptar debido a que no corresponde la llave pública a esa llave privada. Esta es la forma en que se garantiza la autenticidad de las personas y de las transacciones. (Serrano, 2020).

De manera simple, una transacción de *bitcoin,* es una transferencia de la representación digital de valor de una dirección de *bitcoin* a otra dirección en la red de *Bitcoin.* Los mineros toman la transacción para validarla y luego la incluyen en nuevo bloque que será incorporado de manera inalterable en la cadena de bloques (*blockchain*).

Una transacción se compone de una o más entradas (*inputs*) y una o más salidas (*outputs*), donde:

- La(s) entrada(s) (*inputs*) de una transacción proviene de la(s) salida(s) (*outputs*) de una o varias transacciones anteriores, por lo que muestran de dónde proviene esa representación digital de valor en una transacción específica “creando así una cadena de propietarios en la medida en que el valor se mueve de propietario a propietario” (Antonopoulos, 2017, p. 21), y cuenta con una firma que se crea con la llave privada que se asocia con la llave pública de la dirección de *bitcoin* del remitente, que “demuestra la verdadera propiedad de los fondos que se están gastando” (p. 55).

- Las salidas (*outputs*) de transacción tienen la cantidad de la representación digital de valor a transferir y la dirección de *bitcoin* del receptor o destinatario.

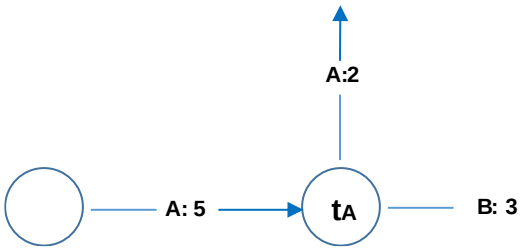
Ahora bien, las entradas (*inputs*) son débitos que “reducen el saldo de la(s) cuenta(s) del remitente” y una o más salidas (*outputs*) son créditos que “aumentan el saldo de la(s) cuenta(s) del receptor” (Möser, Böhme y Breuker, 2013, p. 2).

(Möser, Böhme y Breuker, 2013) explican que el protocolo de *Bitcoin* establece que cualquier salida referenciada por una entrada se agota y no se puede volver a hacer referencia a ella, impidiendo así, que los usuarios gasten el doble de su dinero haciendo referencia a una salida en dos transacciones diferentes. Sin embargo, al ser *Bitcoin* un sistema distribuido es posible que el destinatario de una transacción no pueda saber que el remitente ha hecho referencia a dicha salida en particular, en otra transacción anterior. Por eso es que *Bitcoin* conserva el registro de todas las transacciones llamado cadena de bloques, donde los bloques representan estructuras de datos que encapsulan transacciones, y una referencia del bloque anterior, formando así una cadena.

Como ejemplo, en el caso de una persona (usuario A) que quiere enviar *bitcoins* a otra persona (usuario B) mediante una transacción, para poder hacerlo, hace una referencia a una salida con el valor de una transacción anterior (cinco *bitcoins*) y crea dos salidas, en una envía el valor de *bitcoins* (3 *bitcoins*) que quiere transferirle a la otra persona (usuario) y en la otra salida, devolviéndose 2 *bitcoins* a sí misma.

Figura 3.7

Ejemplo de un gráfico de transacciones parciales



Fuente: Creación propia. Möser, Böhme y Breuker, 2013, Una investigación sobre las herramientas de blanqueo de capitales en el ecosistema de Bitcoin.

Se dice que devolver *bitcoins* a uno mismo es una práctica común y generalmente, la cantidad de *bitcoins* a la que hacen referencia todas las entradas no siempre será igual a la cantidad que uno realmente quiere enviar. Esto se debe a que, como se mencionó anteriormente, las entradas solo se pueden usar una vez, por lo tanto, se debe crear una nueva salida para devolver el cambio.

Finalmente, para garantizar que el titular sea quien pueda retirar de una cuenta, las transacciones se combinan con firmas digitales que están relacionadas con las claves públicas referenciadas en las entradas. (Möser, Böhme y Breuker, 2013, p. 2).

3.2 Impacto en el Sistema Financiero Mexicano

En México se han identificado alrededor de 50 criptomonedas distintas en operación, destacando "*bitcoin*" y "*ethereum"*, de acuerdo con datos de la Unidad de Investigaciones Cibernéticas y Operaciones Tecnológicas. (Ángel, 2019, Animal Político).

Aun y cuando la criptomoneda *bitcoin* no se considera una moneda legal, tampoco es ilegal realizar operaciones con *bitcoins*, después de establecerse como un activo virtual hoy en día, es la moneda más usada y cada vez es mayor la participación del *bitcoin* en el mercado mexicano. Su sistema de pagos ha revolucionado y facilitado la fluidez del dinero a través de Internet. (Equipo Editorial, Mi Punto de Vista, 2019).

Debido a su creciente popularidad en todo el mundo, en México, son cada vez más las personas que se animan a invertir y realizar transacciones con *bitcoin* a pesar de su no muy buena reputación en sus inicios. Hoy en día, está creciendo cada vez más la popularidad de esta criptomoneda entre los mexicanos. (Equipo Editorial, Mi Punto de Vista, 2019).

En la actualidad, en México es posible realizar diversas operaciones con *bitcoin*. La mayoría de los mexicanos invierten con intenciones de ahorro y muchos otros realizan compras electrónicas o pagos de renta utilizando esta criptomoneda.

Esta criptomoneda ya es aceptada en muchos comercios y franquicias como *Starbucks*, cadenas de supermercado, librerías y restaurantes y principalmente servicios ofrecidos en la página *web*, esto está motivando que cada vez más mexicanos se sumen a este método de pago y vean con optimismo el futuro de las criptomonedas. México, además de Brasil, es de los países donde más se utiliza estos activos y donde las *Fintechs* están identificando grandes oportunidades de negocio.

Mensualmente se comercializan más de 1,000 millones de pesos en *bitcoins* y cada año aumenta el uso de *bitcoins* en México. Con una fuerte presencia, el *bitcoin* parece ser una de los métodos de pago más confiables para los mexicanos. Por lo que cada vez más mexicanos deciden ahorrar o invertir en criptomonedas.

Para Alberto Djemal, director de Bitrus, las criptomonedas están ganando terreno principalmente en el área de las finanzas personales. (Guzmán, 2020).

Las criptomonedas le están haciendo competencia a los servicios bancarios, pues cubren más o menos las mismas necesidades; facilitan el envío de dinero y el almacén de valor. Con *bitcoin*, la gente tiene una nueva alternativa financiera, tiene más opciones para guardar y enviar dinero. Además, cada vez es más utilizado para envío de remesas, ya que es muy fácil enviar dinero de otros países a México con *bitcoin*.

Esto ha llevado a los bancos a innovar, pues compiten con una tecnología descentralizada, ágil y que se desarrolla a gran velocidad. Así, en marzo 2019, se comunicó que los bancos mexicanos habían creado una asociación para habilitar pagos digitales y momentáneos.

Aún y cuando *bitcoin* representa un reto para el gobierno e instituciones financieras. Cada vez más personas usan *bitcoin* en México, más empresas llegan a invertir en el campo de las criptomonedas y se inventan nuevos casos de uso de *Blockchain* con *tokens*. Mientras los bancos están desarrollando nuevas tecnologías y el gobierno está implementando prohibiciones en torno a criptomonedas, el desarrollo del ecosistema de *Bitcoin* en México no se detiene. (*Bitcoin* México, 2020).

Bitcoin México (2020), señala que el 5.9% de usuarios de internet poseen criptomonedas en México, lo que representa el lugar número 16 del mundo y es mayor al porcentaje de usuarios que poseen cripto en Estados Unidos, Japón e incluso China. Esto de acuerdo con el estudio de *Hootsuite*.

México es territorio fértil para el desarrollo de plataformas exitosas que le han dado solidez a la aceptación del *bitcoin* y en un estudio de este año sobre el ecosistema de *Blockchain* en México, se identificaron 81 empresas de diversas áreas que trabajan con *Blockchain*, tecnología que da soporte a la existencia de *bitcoin*.

Se están desarrollando muchos proyectos en México, tal es el caso de las tiendas Oxxo, que a través de ellas se puede comprar *bitcoin*, permite depósitos para fondear una *digital wallet* (billetera digital en inglés). Está creciendo la cantidad de cajeros automáticos de *bitcoin* en México, principalmente gracias al trabajo de *Cryptobuyer*. Gracias a la estabilidad que tiene el ecosistema de *Bitcoin* en México, en comparación con otros países latinoamericanos, muchos proyectos han elegido a este país para expandirse.

Aún y cuando en México las criptomonedas no están bajo regulación, varios países han permitido la implementación de *exchanges*. “El mercado mexicano es uno de los más importantes y crecientes de Latinoamérica respecto a la compra de criptomonedas”, dijo Alberto Djemal, director de Bitrus, comenta (Guzmán, 2020).

Las transacciones realizadas por los usuarios de *bitcoin*, se realizan a través de *exchanges* de criptomonedas que son empresas que funcionan como casas de cambio y normalmente ofrecen sus servicios a través de plataformas (páginas *web* o aplicaciones). En estas plataformas se pueden comprar y vender monedas digitales, usando *bitcoins* como moneda de cambio o haciendo las compras con pesos.

Muchos de los *exchanges* permiten hacer transferencias bancarias para depositar dinero en su plataforma y después comprar criptomonedas, pero también hay algunas *exchanges* que dan la opción de adquirirlas mediante tarjeta de crédito/débito, *Paypal* e incluso tratar directamente la compra con otros usuarios interesados en vender (*Localbitcoins*). (BTC, México).

Además de las comisiones que cobran las *exchange* al cambiar las monedas también se debe de fijar uno en el *rate* o tasa de cambio, que es el precio que uno va a pagar cuando compra en la plataforma y también al que ofrecerán cuando vendas, ya que cada *exchange* pone su propio precio y este puede variar mucho de una plataforma a otra.

Entre las mejores *exchange* en México se encuentran Bitso, Cex.io, *Localbitcois*, Volabit,

- *Bitso:* Es una *exchange* que permite cambiar pesos mexicanos por *bitcoins* y viceversa. Se pueden añadir fondos a la cuenta de uno mediante transferencia bancaria y del mismo modo retirar el dinero cuando se haya vendido las monedas. El registro en la plataforma es muy sencillo y rápido, tan solo verificando la cuenta con el celular uno ya puede empezar a operar.

- *Cex.io: Exchange* fiable, con un sistema de comisiones bastante bajo y que además ofrece soporte a la mayoría de países al rededor del mundo. En la sección de compras o ventas. Con una cuenta básica se puede comprar 300 USD diarios, con un límite de hasta $1000 mensuales. Hay hasta 4 niveles de verificación con lo que los límites de compra, venta y retiro serán superiores. Se pueden comprar *bitcoins* con tarjeta de crédito y débito (Comisión 3.5% + $ 0.25). Las transferencias bancarias no tienen comisiones, como tampoco las tiene hacer transferencias dentro de la misma plataforma.

- *Localbitcoins:* Es uno de los *exchange* que más se utiliza en todo el mundo, por la seguridad que ofrece al actuar como intermediario en las transacciones y por la gran variedad de métodos de pagos que aceptan sus usuarios. Compras los *bitcoins* directamente a otras personas físicamente, incluso puedes llegar a quedar con ellas y comprárselos por dinero en efectivo o también aceptan transferencias bancarias y muchas otras modalidades de pago online. No cobran comisiones por comprar *bitcoins*, pero sí por vender a una tasa del 1% del total de la transacción. Hay que estar atentos a la tasa de cambio.

- *Volabit:* Plataforma muy sencilla de manejar. Una vez registrado, puedes ver el balance de tu cuenta y la opción de depositar pesos en tu cartera *Volabit* o depositar *bitcoins*. Para hacer tu primer depósito en pesos o *bitcoins*, es necesario que aumente tu nivel inicial de membresía. El nivel básico se obtiene con solo ligar tu número de teléfono y puedes depositar y retirar hasta $7.000 pesos por día, para el nivel Pro se requiere subir una identificación y un estado de cuenta bancario y se puede depositar y retirar hasta $500.000. Cobra una comisión del 0.8% (más IVA) en la compra y venta de *bitcoins*. No cobran comisiones por retirar o depositar *bitcoins*, sólo se cobra la comisión de red que corresponde a los mineros (0.0005 BT).

- *Bitrus:* Fintech que apostó por crear una casa de cambio de criptodivisas y una billetera electrónica (*wallet*) que operan a la par. Con *Bitrus Wallet* se puede abrir una cuenta de

> forma fácil y rápida, obtener una tarjeta y hacer compras en internet o en establecimientos, con la seguridad de que las criptomonedas están a salvo. Mientras que la plataforma permite comprar, almacenar y vender divisas digitales de forma simple. Las *wallet* están en espera de la Ley para Regular las Instituciones de Tecnología Financiera, mejor conocida como "Ley *Fintech*". La *exchange* de *Bitrus* comenzó a operar en octubre 2019 y mantiene más de 23 usuarios registrados en la plataforma, con movimientos de alrededor de 80 millones de pesos.

Djemal consideró que la *Fintech* se caracteriza por ofrecer servicios de banca tradicional, ya que puede servir para realizar pagos por internet a diversos comercios y servicios, así como para la recepción de remesas desde el extranjero con bajas tarifas y rapidez. Con estos productos, dijo, la empresa contribuye a incrementar la *inclusión financiera*[13] del país.

En nuestro país existen administradores transparentes de carteras de *bitcoins* como Bitso, que han colaborado con las autoridades. De hecho, hace un año aproximadamente, se publicó en México la denominada "Ley *Fintech*" que busca establecer cierta regulación en el manejo de esta divisa, sobre todo para que haya entidades responsables y que, en caso de ser necesario, colaboren con las autoridades.

Uno de los principales usuarios potenciales de esta y otras plataformas similares, son todas aquellas personas que no se encuentran bancarizadas, es decir, que no tienen una cuenta bancaria en alguna institución como Banxico, Banorte, entre otros.

En México, el ecosistema de *Bitcoin* tiene un desarrollo muy activo a pesar de que las instituciones financieras y el gobierno mantienen una posición escéptica frente a las criptomonedas. La adopción de *bitcoin* sigue su curso, la comunidad de cripto en México es cada vez más activa y más grande.

3.2.1 *Bitcoin* en el lavado de dinero.

Primero recordemos brevemente cómo funciona el lavado de dinero.

Cuando el dinero proveniente de un delito no se puede declarar como tal ante la SHCP porque significaría la confesión del delito, por lo que se miente y se mezcla. Generalmente los criminales operan con nombres falsos, en anonimato o por medio de cómplices, así rompen el vínculo entre ellos y el dinero. Después, se compra o vende otros activos para despistar. Esto se puede realizar de muchas formas. Se puede comprar un bien para después venderlo. O se pueden colocar bienes en un lugar donde no se hagan muchas preguntas.

[13] Inclusión Financiera: en México, la inclusión financiera se define como el acceso y uso de servicios financieros formales bajo una regulación que garantice la protección al consumidor y promueva la educación financiera para mejorar las capacidades financieras de todos los segmentos de la población.

No olvidemos que las personas lavan dinero usando oro, diamantes, bienes raíces, arte, dinero en efectivo, tarjetas de regalo y muchas cosas más, entre ellas, actualmente las criptomonedas. Sin embargo, el blanqueo a gran escala ocurre en los bancos, principalmente en los que están ubicados en territorios con jurisdicciones especiales, como es el caso de: Suiza, Hong Kong, Singapur, Estados Unidos, Isla de Man y del Canal, Emiratos Árabes Unidos, Luxemburgo, el Reino Unido, Mónaco y Bahréin. Lituania, Panamá, Estonia e Irlanda también están en esta lista que cada vez es más grande. Las grandes fortunas se refugian en estos lugares para lavar dinero y para también evadir impuestos. Los bancos en estos lugares garantizan confidencialidad. Para estos países es un negocio redondo y significa ingresos muy importantes.

En muchas ocasiones, *bitcoin* ha sido censurado como facilitador de lavado de dinero y la evasión de impuestos e indudablemente esta actividad ocurre, pero es ilógico pretender que sólo sucede exclusivamente con *bitcoin*. Esta vieja actividad sucede con todo lo que tenga valor. Lavar dinero con *bitcoin* funciona del mismo modo que funciona con las otras maneras que existen.

Las criptomonedas son sólo una nueva alternativa. Desde que fueron creadas, han resultado bastante factibles para los delincuentes ya que, el pago con criptomonedas permite traficar todo tipo de bienes sin riesgo de ser rastreados por alguna autoridad. Su fama de ser utilizadas en actividades ilícitas, probablemente sea una consecuencia del malentendido de una de sus características que es el “anonimato” (Cadenas, 2018).

Hay reportes de la DEA, donde señalan que organizaciones delictivas como los Zetas y Jalisco Nueva Generación, han iniciado el uso de monedas virtuales (*bitcoin*), para lavar dinero, e incluso, la *dark web* es utilizada para el contrabando de drogas con transacciones virtuales, por lo que han surgido servicios de intercambio para convertir la moneda fiduciaria en virtual y viceversa.

En México, se han estado investigando casos de posible lavado de dinero donde grupos delictivos podrían estar convirtiendo fuerte sumas de dinero, en criptomonedas que pueden ser transferidas casi de forma anónima al sistema financiero internacional. La sospecha surgió cuando algunas entidades financieras que operan en plataformas tecnológicas detectaron en México la compra masiva de *bitcoins*. Este sistema está siendo utilizado debido a la naturaleza del mismo y a los escasos controles que existen. (Angel, 2019. Animal Político).

Hoy en día, los casos de lavado de dinero a través de criptomonedas son un reto prioritario para la Unidad de Delitos Cibernéticos, de la Fiscalía General de la República (FGR) y ya han realizado distintas investigaciones relacionadas con monedas digitales y su uso en actividades ilícitas.

Al respeto, cabe mencionar que la FGR ha reportado que hay una comunidad importante entre el *bitcoin* y la *dark web*. Tienen algunas investigaciones por compra y venta de drogas y armas, a través de la *dark web* y los *bitcoins* como mecanismo de transferencia.

En los medios se habla mucho sobre la *deep web* o *dark web* para relacionarla con actividades criminales, por lo que es importante entender cómo operan estas secciones de la *web*. La *deep web* es el contenido de la red (90%) que no es accesible a través buscadores como Google, *Bing, Explorer* etc., comprende toda la información a la que no se puede acceder públicamente, es decir, no puedes acceder si no pagas una determinada cuota o una mensualidad. Pueden ser páginas usuales protegidas por un *paywall*[14], archivos guardados en *Dropbox*[15], correos guardados en los servidores algún proveedor, y otros.

La *dark web* o internet oscura (0.1% del internet), parte de la *deep wep*, es la forma como se conoce a ciertas plataformas y contenidos en línea donde solo se puede acceder con programas específicos que, en la mayoría de los casos, permiten la "navegación anónima" y ocultan la identificación de los equipos que se utilizan. Es una porción de Internet intencionalmente oculta a los motores de búsqueda, con direcciones IP enmascaradas y accesibles sólo con un navegador web especial. El más popular es *TOR*, pero también tienes a Freenet, I2P o ZeroNet. Cada una de estas es una *Darknet*, pero cuando se refieren a todas en general se utiliza el término *Dark Web*.

(Cadenas, 2018), señala que, en un informe de la Europol en 2015, se reportó que el *bitcoin* representó el 40% de todos los pagos asociados con la delincuencia en crímenes cibernéticos, donde se identificó principalmente dos tipos de actividades donde se encuentra relacionadas las criptomonedas:

Una es el *crimen cibernético habilitado*, en donde el delito se comete dentro del entorno virtual, por ejemplo: los *malwares*[16] *o ransomwares*[17]. Uno de los casos más recordados es el *Wanna Cry*, un *ransomware* que bloqueó la información de instituciones y negocios en 150 países de todo el mundo, incluyendo empresas como Telefónica (MX:TEFN) y FedEx (NYSE:FDX), y exigió el pago para la recuperación en *bitcoins*.

Y la otra, es el *delito cibernético*, que son conductas delictivas que permiten que se realicen crímenes apoyados por el uso de computadoras o internet, asociando el uso de las criptomonedas para cometer actos ilícitos.

Los primeros casos se vieron en el sitio ubicado en la *deep web*, *Silk Road*, por 2013, cuando se empezaron a utilizar las criptomonedas para la adquisición de artículos ilegales. Los delincuentes

[14] *Paywall*: Es un sistema que restringe el acceso a contenido a usuarios que no cuentan con una suscripción pagada.
[15] *Dropbox:* servicio de alojamiento de archivos multiplataforma en la nube. Permite a los usuarios almacenar y sincronizar archivos en línea y entre ordenadores y compartir archivos y carpetas con otros usuarios y con tabletas y móviles
[16] *Malwares*: Abreviatura de *Malicious* software, término que abarca todo tipo de programa o código informático malicioso cuya función es dañar un sistema o causar un mal funcionamiento. Dentro de este grupo se encuentran algunos términos cómo Virus, Troyanos (*Trojans*), Gusanos (Worm), *Ransomwares*, etc.
[17] *Ransomwares*: programa de software que infecta tu computadora y muestra mensajes que exigen el pago de dinero para restablecer el funcionamiento del sistema. Sistema criminal para ganar dinero que se puede instalar a través de enlaces engañosos, mensaje de correo electrónico, mensaje instantáneo o sitio *web*. Tiene la capacidad de bloquear la pantalla de una computadora o cifrar archivos importantes predeterminados con una contraseña.

recibían *bitcoin* por la comercialización de estos productos preservando su anonimato; sin embargo, el problema se presentaba en el momento de cambiar esos *bitcoins* por dinero fiduciario al haber pocas casas de intercambio (*exchange*). El anonimato se da debido a que las direcciones de *bitcoin* no están registradas para particulares, a diferencia de las cuentas bancarias, estas direcciones funcionan como un identificador único.

3.2.2 Factores de riesgo por activos virtuales.

El principal riesgo de lavado de activos con monedas virtuales deriva del "anonimato", que se origina por lo complicado que es poder rastrear las transacciones. Para poder mitigar este riesgo, las entidades obligadas y las autoridades requieren poder dar un seguimiento a las transacciones en moneda virtual.

El usuario de *bitcoin* puede ocultar su identidad detrás de una dirección de *bitcoin*, considerando que las direcciones de *bitcoin* son una combinación de números y letras que no tienen ninguna relación con la identidad o ubicación física del usuario en el mundo real. Sin embargo, las direcciones de *bitcoin* no brindan un total anonimato, debido a que *bitcoin* es seudónimo puesto que las direcciones forman parte del libro de contabilidad pública (*blockchain*) donde la información financiera de todas las transacciones se encuentra disponible en la red. Es decir, el resumen de cada usuario de *bitcoin* es público, pero la identidad detrás de esos resúmenes está oculta. Y al no contar con ninguna verificación de identificación de identidad de los usuarios al realizar las transacciones en monedas virtuales, el seudónimo o las monedas virtuales convertibles descentralizadas completamente anónimas, como es el caso de *bitcoin*, representan un alto riesgo de lavado de activos.

Por su parte, (Möser, Böhme y Breuker, 2013), afirman que: "*aunque la relación entre las cuentas de bitcoin y las identidades civiles de sus propietarios es a priori desconocida, las transacciones de bitcoin no son anónimas..… pensar en él como un libro mayor público distribuido que registra todas las transacciones entre cuentas válidas de bitcoin. Esta información se almacena de forma segura en una estructura de datos en constante crecimiento llamada cadena de bloques y permanece visible para todos, para siempre*." (p.1).

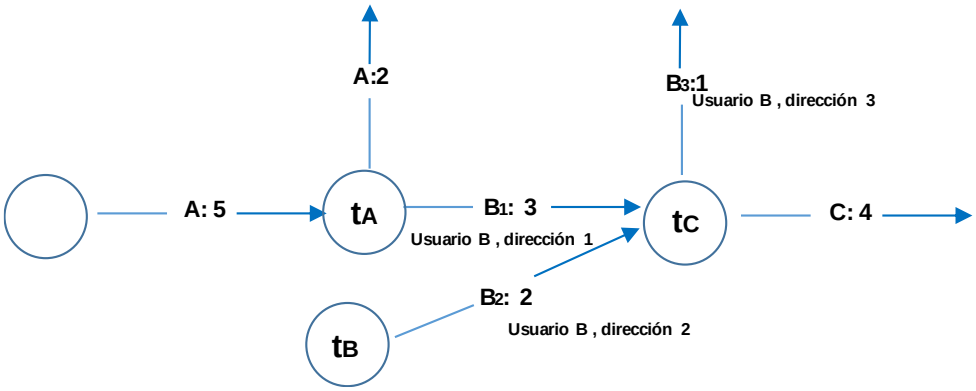
(Möser, Böhme y Breuker, 2013), También señalan que las direcciones de *bitcoin* se pueden identificar con personas reales, aunque esto no sea tan fácil. Cualquier usuario puede crear tantas direcciones como quiera. Aunque a primera vista, se pudiera pensar que las direcciones creadas por una persona pueden pertenecer a muchas personas, en lugar de a una sola, es posible que se pueda identificar a las personas detrás de las direcciones.

Por otro lado, refieren que considerando las direcciones y referencias de las salidas y entradas en una transacción; el hecho de que las salidas de dos direcciones que se mencionan como entradas en una misma transacción, se podría interpretar como evidencia de que ambas direcciones pertenecen a la misma persona. Además, sabiendo que una transacción generalmente tiene dos salidas, donde una es el envío de la cantidad de *bitcoins* que realmente

quiere enviar el usuario y la otra, la devolución de su cambio; y al haber tres salidas en una misma transacción es muy probable que pertenezcan a la misma persona propietaria debido a que los *bitcoins* de dos direcciones se han combinado para financiar una producción mayor es decir, se juntan las cantidades de *bitcoins* de ambas direcciones para sumar la cantidad de *bitcoins* que se requieren enviar a otra persona, y probablemente la producción pequeña sea el cambio. Por ellos, es que la información del entorno puede ser útil para razonar sobre las identidades detrás de las direcciones de *bitcoin*. A continuación, se muestra un gráfico para su mejor entendimiento con un gráfico de una transacción que suma los *bitcoins* (3+2) de dos direcciones distintas (B1 y B2) de una misma persona (usuario B), que requiere para enviar a otra persona (usuario C) y una salida por la devolución de su cambio (B3).

Figura 3.8

Ejemplo gráfico de una transacción que suma los *bitcoins*



Fuente: Creación propia. Möser, Böhme y Breuker, 2013, Una investigación sobre las herramientas de blanqueo de capitales en el ecosistema de *Bitcoin*.

También*, bitcoin* como cualquier otra moneda virtual convertible, puede ser intercambiada por moneda fiduciaria o por cualquier otra moneda virtual lo que pueden aumentar el riesgo de lavado de activos por los siguientes motivos.

- Las monedas virtuales convertibles se comercializan en Internet, por lo que no hay una verificación e identificación de identidad cara a cara de los usuarios, lo que permite posibles inversiones y transferencias anónimas porque la identidad del inversionista, remitente o destinatario no está identificada en relación con una ubicación física y real.

  “El protocolo de *Bitcoin* no requiere ni proporciona ninguna identificación y verificación de los participantes ni genera registros históricos de transacciones que están necesariamente asociadas con la identidad del mundo real” (FATF, 2014, p. 9).

El GAFI ha identificado tres factores de riesgos de lavado de dinero a través de monedas virtuales:

a) La relación no cara a cara: La ausencia de contacto cara a cara entre el comerciante y el cliente “puede indicar una situación de mayor riesgo de LA/FT” (GAFI, 2013, p. 14), considerando que el riesgo de fraude de identidad aumenta al permitirle a los clientes la posibilidad de proporcionar información inexacta, errónea o falsa con el propósito de ocultar la relación entre los fondos y una actividad ilícita.

   Al respecto, para ayudar a mitigar el seudónimo o anonimato de las monedas virtuales, el GAFI ha reconocido algunas buenas prácticas que las entidades obligadas deberían implementar para realizar una debida diligencia del cliente, dichas prácticas consideran ratificar la información de identidad que se reciba por el cliente como en bases de datos, quizá rastreando la dirección IP del cliente, así como buscar en Internet información que confirme la relación entre la actividad y el perfil de transacción del cliente. (FATF, 2019).

b) Segmentación de servicios y el alcance geográfico: Las transacciones de monedas virtuales pueden involucrar diferentes tipos de participantes, como son los usuarios, mineros, proveedores de servicios de billeteras, mezcladores, cambiadores, etc., sin embargo, es probable que no todos ellos se consideren como entidades obligadas en algunas jurisdicciones. Además, las transacciones realizadas por Internet no tienen límites geográficos alguno, así que, aquellos modelos de negocio de monedas virtuales (*Fintech*) que se encuentren en un país que no tenga controles o cuente con controles débiles contra el lavado de activos, pueden prestar servicios a clientes ubicados en otra jurisdicción, incluso que sí los tenga.

   El modo de mitigar estos riesgos, según el GAFI, es por medio de algunos procedimientos de licencia o registro para todos aquellos VASP, para poder reducir la naturaleza transfronteriza de las transacciones a través de activos virtuales y así, los modelos de negocios en este sector estén debidamente autorizados o registrados en cada jurisdicción donde prestan sus servicios, permitiendo a las autoridades implementar una supervisión efectiva; imponer sanciones efectivas y, recopilar información o evidencia.

c) Métodos de financiamiento anónimos y dinero en efectivo: éstos, representan un alto riesgo de lavado de activos al adquirir monedas virtuales ya que no se tiene un registro adecuado de la transacción.

   GAFI señala que, para mitigar este riesgo, los modelos de negocios que tengan alguna relación con activos virtuales podrían considerar *“limitar la fuente de financiamiento a una cuenta bancaria, tarjeta de crédito o débito, o al menos aplicar tales limitaciones a la compra inicial, o por un período determinado hasta que se pueda establecer un patrón de transacción, o para comprar por encima de un umbral determinado”* (FATF, 2015, p. 13).

También *(Möser, Böhme y Breuker, 2013, p. 2),* señala que, si fuera posible garantizar el cumplimiento de, conoce a tu cliente en los límites del sistema *Bitcoin*, que es el punto preciso donde se intercambian las criptomonedas *bitcoin* por productos y servicios o monedas normales,

se podría identificar actividades sospechosas dentro del libro de contabilidad de las transacciones públicas y responsabilizar a los delincuentes en el momento y lugar en que interactúan con el mundo real; pero lamentablemente, esto se vería frustrado por intermediarios (prestadores de servicio) que ofrecen servicios para anonimizar la relación entre remitentes y destinatarios de transacciones dentro del sistema *Bitcoin*. Estos servicios también se conocen como mezclas de *bitcoin*.

La criptomoneda convertible permite a las partes de una transacción un grado de anonimato mayor que los medios de pago tradicionales. (Puvogel, 2018). Habitualmente, las transacciones entre sus usuarios son no presenciales y –a priori– anónimas. Un SMV descentralizado puede ser utilizado sin necesidad de proporcionar dato de identificación alguno del usuario. Sin embargo, dicho anonimato no puede estar garantizado, derivado del surgimiento de técnicas para descubrir las identidades de los usuarios en una determinada transacción.

Aunque también, hay programas de anonimato, que son herramientas y servicios como redes oscuras y mezcladores, diseñados para ocultar el origen de una transacción *bitcoin* y facilitar el anonimato. (Ejemplos: *Tor* (red oscura), Monedero Oscuro (red oscura), Lavandería *Bitcoin* (mezclador).

3.3 Uso del anonimato del *bitcoin*

En este apartado, se abordará los riesgos y amenazas de *bitcoin* y otras monedas virtuales convertibles descentralizadas en el lavado de dinero, para ello, primero se hablará un poco sobre el anonimato.

3.3.1 Técnicas y herramientas para conservar el anonimato del *bitcoin.*

Antes de iniciar esta sección, primero se explica qué se debe de entender por técnicas/herramientas de anonimización (anonimizador[18]). Se entienden como las innovaciones tecnológicas que los usuarios utilizan para poder ocultar el origen de una transacción en moneda virtual, buscando un alto nivel de anonimato, y que, por cierto, debido a la rápida y constante evolución que está teniendo el desarrollo tecnológico en esta área, continuamente se están desarrollando nuevas técnicas y que las técnicas de las que se hablen en este trabajo de investigación, a su término, ya hayan cambiado.

Una pieza importante en el uso de técnicas y herramientas para conservar el anonimato en las transacciones con *bitcoin* son los proveedores de servicio. El GAFI ha identificado la existencia de intermediarios, especialistas, y profesionales (proveedores de servicio) que se dedican al lavado de activos. Son personas naturales o jurídicas que no participan en la comisión del delito fuente o subyacente de lavado de activos, pero brindan servicios para disfrazar u ocultar los

[18] Anonimizador: “se refiere a herramientas y servicios, como redes oscuras y mezcladores, diseñados para ocultar la fuente de una transacción de *Bitcoin* y facilitar el anonimato. (Ejemplos: Tor (*darknet*); Dark Wallet (*darknet*); *Bitcoin* Laundry (mezclador))”. (FATF, 2014).

recursos provenientes de una actividad ilícita (FATF, 2018). En el ámbito de las monedas virtuales, los mezcladores y los cambiadores son identificados como terceros o entidades que pueden proporcionar dicho servicio para anonimizar la relación entre remitentes y destinatarios de transacciones dentro del sistema *Bitcoin*. A continuación, se explicará cómo funcionan:

- Los cambiadores (*exchangers*) de monedas virtuales: Los cambiadores son potencialmente utilizados, principalmente aquellos que no tienen licencia o no están registrados. (Serrano, 2020), refiere que Fanusie & Robinson, identificaron en su estudio, que entre los años de 2013 a 2016, los cambiadores "representaron la mayor parte (45%) del volumen total de *bitcoins* lavados".

  Los cambiadores son personas o entidades que prestan servicios de intercambio de monedas virtuales a moneda fiduciaria u otra moneda virtual a cambio de una tarifa o comisión (Böhme, et al., 2015, p. 220). La plataforma de intercambio puede estar en línea o tener una ubicación física en la que cualquier usuario puede comprar y vender monedas virtuales.

  "Los cambiadores generalmente aceptan una amplia gama de pagos, incluidos efectivo, transferencias electrónicas, tarjetas de crédito y otras monedas virtuales, y pueden ser proveedores afiliados al administrador, no afiliados o un proveedor externo" (FATF, 2015, p. 29). En algunas jurisdicciones los cambiadores no están obligados a cumplir con la regulación sobre el Conocimiento del Cliente, el monitoreo y mantenimiento del registro de transacciones, la identificación y reporte de transacciones sospechosas a las autoridades UIF del país donde se localizan. Por lo tanto, éstos se podrían aprovechar para el lavado de activos en sus fases de colocación e integración, ya que el dinero con el que se compra monedas virtuales puede provenir de una actividad ilícita.

- Mezcladores o servicios de lavandería, también conocidos como *mixers* o *tumblers*: (Serrano, 2020), señala que los delincuentes usan estos servicios para romper la cadena de propietarios en las transacciones en monedas virtuales convertibles descentralizadas con el propósito de evitar cualquier vinculación de los *bitcoins* que han sido mezclados con el delito fuente o subyacente logrando así un completo anonimato por parte del usuario y no ser "rastreados hasta su origen" (Rolf van Wegberg, Jan-Jaap Oerlemans, & Oskar van Deventer, 2018, p. 425).

  Los mezcladores ofrecen servicios para anonimizar transacciones, al disfrazar "la cadena de transacciones en la cadena de bloques (*blockchain*) mediante la vinculación de todas las transacciones en la misma dirección de *bitcoin* y enviarlas juntas de tal manera que aparezcan enviadas desde otra dirección" (FATF, 2014, p. 6). Los servicios de mezcla se realizan a través de una plataforma en línea donde los usuarios solicitan sus servicios enviando sus "fondos a un servidor central y luego son recuperados en una dirección de *bitcoin* diferente" (Franco, 2015, p. 213). A continuación, se dará una breve descripción de cómo se lleva a cabo este tipo de servicios.

Como primer paso, los usuarios envían sus fondos a una dirección propiedad del mezclador. Después, dichos "fondos en esta dirección pasan a través de una capa de transacciones internas (...) con el propósito de confundir a aquellos que intentan hacer la trazabilidad de los mismos" (Franco, 2015, p. 213). Recordemos que cada transacción cuenta con entradas (*inputs*) y salidas (*outputs*), donde las entradas (*inputs*) muestran las salidas (*outputs*) de anteriores transacciones. Pues bien, a través del servicio de mezcla, las entradas (*inputs*) no se pueden vincular con las salidas (*outputs*) de las transacciones anteriores debido a las transacciones internas que realizó el servicio de mezcla con sus propias monedas o con las monedas de otros usuarios. Así, se logra ocultar la cadena de propiedad y el destinatario final al cual el usuario quería que le fueran enviados los fondos (GAFI, 2014). Y, por último, los fondos son devueltos al usuario a través de direcciones de *bitcoin* diferentes. (Ejemplos; *Blockchain*.info; *Bitcoin* Laundry; OnionBC; *Bitcoin* niebla; por mencionar algunos).

Aún y cuando el historial de éstas transacciones se destruye, en la cadena de bloques (*blockchain*) se puede identificar que los *bitcoins* de una determinada dirección han sido mezclados (AMLC, 2017).

Después de lo anterior, en caso de que aquella plataforma que preste servicios de mezcla sea considerada como entidad obligada; al tener que contar con un programa antilavado de activos, la información correspondiente a la relación entre las entradas (*inputs*) y salidas (*outputs*) quedaría disponible para las autoridades. Por ello, las transacciones que se realizan a través de un servicio de mezcla se pudieran consideran como sospechosas por la capa adicional de anonimato que se le proporciona y, en consecuencia, debería reportarse a la UIF del país correspondiente. Pero, si dichos intermediarios no son entidades obligadas en su jurisdicción, no están obligados a implementar un programa antilavado y reportar dichas transacciones a la UIF.

Lo anterior, muestra la gran importancia y necesidad de una regulación efectiva de las actividades y profesiones no financieras designadas, y la necesidad de una mayor conciencia entre los sectores de servicios profesionales.

Por su lado, (Cadenas, 2018), señala que una de las formas para blanquear dinero con criptomonedas, es a partir de una dirección de *bitcoin* creada por un "*Mixer*"(o *tumblers*) que mezcla los capitales para que se pierda el rastro. Es una herramienta que hace que sea virtualmente imposible conocer la dirección que represente fondos provenientes de actividades "ilícitas". En caso de tener *bitcoins* legalmente obtenidos, se puede incorporar *bitcoins* obtenidos de manera ilegal y mezclarlos. El *Mixer* combina los fondos, elimina la dirección de la cuenta ilícita y crea una nueva dirección o identificador. Incluso, algunas empresas ofrecen "seccionar" los montos y garantizar que, aquellos *bitcoins* ilegales, no regresen al cliente. Es decir, el mezclador conoce las direcciones de *bitcoins* que se depositaron antes y evitará que regresen al mismo cliente. Este modelo de servicio es el ideal para lavadores frecuentes.

En la literatura especializada en informática se identifican dos técnicas de anonimización *CoinJoin y CoinSwap.*

CoinJoin: técnica especial de mezcla de fondos que no requiere la presencia de un intermediario. (Franco, 2015) “En *CoinJoin*, varios usuarios acuerdan que se mezcle una suma determinada de fondos y luego crean una transacción con múltiples entradas y salidas del tamaño elegido, una para cada participante. Esta transacción es realizada por fuera de la cadena (*off-chain*) para poder ser firmada por todos los participantes. Una vez firmada por todos, se publica en la cadena de bloques (*blockchain*)” (p. 214). Esta técnica permite a los usuarios mezclar sus fondos con una sola transacción, la transacción acordada se publica en la cadena de bloques (*blockchain*). Dicho de otra forma, más sencilla, un grupo de personas une sus fondos fuera de línea y luego realiza la transacción en línea.

CoinSwap: técnica en la que un tercero entra en la transacción para que las direcciones del remitente y del receptor no pueden ser identificadas. Para explicarlo mejor, supongamos que Alicia quiere enviar fondos a Beto a través de *bitcoin* y no quieren ser identificados en transacción en la cadena de bloques. Entonces, Alicia le envía los fondos a Carlos, y al mismo tiempo Carlos le paga a Beto, pero con fondos diferentes, los cuales no se relacionan con los que recibió de Alicia (Franco, 2015).

Es de gran importancia tener presente estas técnicas de anonimización porque los usuarios pueden llegar a ser catalogados como entidades obligadas cuando realizan transacciones de monedas virtuales convertibles utilizando tales técnicas.

La Universidad Delft, en Países Bajos, después de un estudio, reporta que, en efecto, las criptomonedas son útiles para blanquear dinero y son muchos los servicios ofrecidos en la *Deep Web* que facilitan esta actividad.

(Möser, Böhme y Breuker, 2013), en su estudio sobre las herramientas de blanqueo de capitales en el ecosistema de *Bitcoin*, mencionan algunos servicios de mezcla que se pueden realizar por medio de Internet o de una conexión a través de *Tor network*, sistema muy conocido de comunicación anónimo que se apoya en una red mixta peer-to-peer y que para obtener los servicios, los usuarios tienen que crear una cuenta o interactuar con el servicio a través de una interfaz *web*, según el servicio ofrecido, en los cuales se proporciona toda la información necesaria requerida y reciben una dirección que en ocasiones puede ser de un solo uso, para enviar *bitcoins*. También señalan que los sitios *web* que se basan en una cuenta, permiten depositar y retirar *bitcoins*. Estos servicios que se mencionan como ejemplo son:

- *Bitcoin Fog*: servicio al que se accede únicamente a través de *Tor,* y permite generar hasta 5 direcciones para depositar *bitcoins*. Los *bitcoins* se pueden retirar hasta un máximo de 20 direcciones, repartidas en un período de tiempo de 6 a 96 horas con un total mínimo de 0,2 *BTC*. Cobra una cuota que puede estar entre el 1 y el 3% del valor de la transacción.

(Möser, Böhme y Breuker, 2013) observaron que este servicio agrupa una cantidad grande de transacciones pequeñas en una cantidad chica de transacciones grandes, que después se usan para hacer todas las transacciones salientes, en tanto, las transacciones de entrada permanecen intactas durante mucho tiempo, y así evitar que se detecten conexiones directas entre la transacción de entrada y salida; aunque la estructura del servicio podría dejar la posibilidad de disminuir el anonimato de las transacciones utilizando información de contexto adicional.

- *OnionBC5*: billetera *bitcoin* a la cual se accede a través de *Tor*. Ofrece el envío de transacciones de manera anónima, ofrece un servicio de depósito en garantía que se puede utilizar para retrasar los pagos de *bitcoin* por bienes comprados en línea hasta que se hayan entregado los bienes. Cobra una cuota del 3% con un tamaño de transacción mínimo de 0.5 *BTC*.

- *BitLaundry*: Este servicio no permite depositar *bitcoins* en una billetera virtual. Aquí, se deben especificar las direcciones de destino, el número de transacciones salientes y un período de tiempo. Se genera una dirección de un solo uso a la que el usuario debe enviar al menos 0,25 BTC. La cuota de servicio, se divide en dos partes. La primera es el 2,49% del total, y la segunda es 0,00249 BTC por transacción saliente.

  (Möser, Böhme y Breuker, 2013) realizaron tres ensayos con este servicio de mezcla, observando en el primero, una conexión entre una transacción de salida y su transacción de entrada, donde el enlace directo constituye solo una pequeña parte del tamaño de la transacción, lo que evidencia un anonimato imperfecto. En su segunda prueba, no se mostró ninguna conexión. Sin embargo, en el tercero, el servicio usó directamente la mitad de la transacción de entrada para crear una transacción de salida, por lo que sugieren que este servicio no proporciona un muy buen anonimato. Esto podría ser por un bajo uso del servicio, y/o falta de medidas técnicas para garantizar que los usuarios no reciban sus monedas de entrada.

- *Blockchain.info*: ofrece un servicio de envíos compartido que usa una billetera compartida para intercambiar *bitcoins* entre diferentes usuarios. Su tamaño mínimo de transacción es 0.2 BTC. Su tarifa de mezcla es de 0,5%.

  Aunque el servicio ha utilizado nuestra entrada, no es posible encontrar conexiones directas entre las transacciones de entrada y salida. El servicio agrupa una gran cantidad de transacciones pequeñas en otras más grandes, que luego se dividen nuevamente, lo que dificulta inferir el origen de los *bitcoins*.

A continuación, se mencionan los escenarios de ataque a los servicios de anonimización de transacciones para el sistema *Bitcoin*:

- Confiar en un solo servicio.

- Un número pequeño de usuarios independientes. Si este conjunto es pequeño, el grado de anonimato también será pequeño.

- Envío de todos los mensajes por parte del servidor de mezcla a sus destinatarios, en el mismo orden en que los remitentes los han proporcionado a la mezcla, las relaciones entre remitentes y destinatarios serían obvias. Una forma de evitarlo es retrasar el reenvío de mensajes por períodos de tiempo aleatorios.

- El valor de transacción en un sistema de transacción como *Bitcoin* podría servir como huella digital, revelando el origen de una transacción. Por ejemplo, si un atacante monitorea las direcciones de un usuario y sabe cuántos *bitcoins* transfirió al servicio, podría intentar buscar una transacción de salida del mismo tamaño (menos la tarifa predecible) en los bloques siguientes. Por esto, los servicios aconsejan a sus usuarios que no paguen la cantidad total de *bitcoins* que pagaron anteriormente [17]. También se anima a los usuarios a dividir la transacción saliente en varias transacciones más pequeñas y distribuirlas durante un período de tiempo, lo que dificulta que un atacante las vincule.

  La comunicación entre los usuarios y el servicio. Un usuario debe proporcionar al servicio toda la información relativa a los *bitcoins* que quiere pagar dentro y fuera del servicio. Esta información incluye las direcciones. Por lo tanto, si el tráfico puede ser interceptado, un atacante obtendría toda la información que necesita. En este documento, nos enfocamos solo en los ataques que se pueden realizar de forma expuesta, es decir, ataques basados solo en información disponible públicamente de la cadena de bloques de *Bitcoin*. Eso significa que no consideramos ningún tipo de ataque que implique hacerse cargo de los servicios de mezcla, monitorear su infraestructura de comunicación, etc.

3.3.2 Señales de alerta sobre el anonimato.

El GAFI preparó un listado de señales de alerta (indicadores) de LD/FT asociados con los activos virtuales para coadyuvar a los sujetos obligados relacionados con activos virtuales, así como las IF, las Actividades y Profesiones no Financieras Designadas (APNFD)[19] y VASP, facilitando a los sujetos obligados aplicar un enfoque basado en riesgos para los requisitos de debida diligencia del cliente para conocer a sus clientes, entender la naturaleza e intención de la relación comercial y comprender la fuente de los recursos y que pueda servir como referencia para el análisis de los Reportes de Operaciones Sospechosas (ROS) o aumentar la efectividad en la detección, investigación y aseguramiento de los activos virtuales que estén involucrados en actos delictivos.

[19] APNFD: Según GAFI son: i. Casinos; ii. Agentes inmobiliarios; iii. Comerciantes de metales preciosos; iv. Comerciantes de piedras preciosas; v. Abogados, notarios, otros profesionales jurídicos independientes y contadores (profesionales que trabajan solos, en sociedad o empleados de firmas profesionales); vi. Proveedores de Servicios Fiduciarios y Societarios se refiere a todas las personas o actividades que no se cubren en las recomendaciones, y que, como actividad comercial, prestan determinados servicios a terceros.

También puede ser útiles para los sujetos obligados, APNFD y VASP al preparar ROS y en el caso de los reguladores financieros, monitorear el cumplimiento de las entidades con los controles de Prevención de Lavado de Dinero y Combate al Financiamiento al Terrorismo (PLD/CFT).

Estas señales de alerta, se fundamentan en más de cien estudios de casos proporcionados por las jurisdicciones en el periodo de 2017 a 2020, en los hallazgos reportados en el Informe Confidencial de Investigaciones Financieras que involucran Activos Virtuales (junio de 2019) y el Informe de GAFI publicado sobre Monedas Virtuales: Definiciones Clave y Posibles Riesgos PLD/CFT (junio de 2014), e información pública sobre el uso indebido de activos virtuales; así como en las características inherentes y las vulnerabilidades de la tecnología subyacente de los activos virtuales.

A continuación, se muestra algunas de señales de alerta:

- Operaciones de un cliente que involucran más de un tipo de activo virtual, sobre todo con aquellos activos que brindan mayor anonimato, como criptomonedas.
- Mover un activo virtual que opera en una cadena de bloques pública y transparente, como *Bitcoin*, a un intercambio centralizado y luego intercambiarlo inmediatamente por una criptomoneda de anonimato o moneda privada.
- Clientes con actividad de VASP que no están registrados o no cuentan con licencia en sitios *web* de intercambio *peer-to-peer* (P2P), sobre todo, cuando los clientes manejen una gran cantidad de transferencias de activos virtuales en nombre de su cliente. Uso de cuentas bancarias para facilitar estas operaciones P2P.
- Actividades transaccionales anormales, por el nivel y volumen de activos virtuales cobrados en intercambios de carteras asociadas a la plataforma P2P sin una explicación comercial lógica.
- Activos virtuales transferidos a o desde carteras que muestran indicios de alguna actividad previa relacionada con el uso de VASP que operan servicios de mezcla o caída o plataformas P2P.
- Operaciones que hacen uso de servicios de mezcla y rotación, lo que apunta a la intención de ocultar el flujo de recursos ilícitos entre direcciones de carteras conocidas y mercados de redes oscuras.
- Recursos depositados o retirados de una dirección o cartera de activos virtuales vinculadas a fuentes sospechosas conocidas, incluyendo mercados negros, servicios de mezcla, sitios de apuestas cuestionables, actividades ilegales (por ejemplo, *ransomware*).
- El uso de carteras de papel o *hardware* descentralizadas / no alojadas para transportar activos a través de las fronteras.

- Usuarios que ingresan a la plataforma VASP habiendo registrado sus nombres de dominio de Internet a través de *proxies*[20] o usando registradores de nombres de dominio que suprimen o censuran a los propietarios de los nombres de dominio.
- Usuarios que ingresan a la plataforma VASP usando una dirección IP asociada con una red oscura u otro software similar que permite la comunicación anónima, incluidos correos electrónicos cifrados y VPN.
- Una gran cantidad de carteras de Activos Virtuales (AV) aparentemente no relacionadas controladas desde la misma dirección IP (o dirección MAC), lo que puede implicar el uso de carteras *shell*[21] registradas para diferentes usuarios para ocultar su relación entre ellos.
- Recibir o enviar recursos a los VASP cuyos procesos de DDC o conocimiento de su cliente son débiles o inexistentes.

3.4 Análisis de la Normativa en Prevención del Lavado de Activos

3.4.1 A quién regular en las transacciones con bitcoin.

Ya que se tiene una mejor comprensión sobre las características de las criptomonedas, en particular del *bitcoin* su operación, funcionamiento, los participantes de la red *Bitcoin*, el sistema *blockchain* donde opera así como las técnicas y herramientas que utilizan los delincuentes para ocultar su identidad en las transacciones con esta criptomoneda para lavar dinero, se hace un breve análisis sobre la "Ley *Fintech*" a fin de identificar si esta regulación considera disposiciones que permitan identificar las operaciones de mezcla, transaccionalidad e intercambio en el sistema *blockchain* para conservar el anonimato, en prevención y combate al lavado de dinero.

En esta sección, primero se hablará sobre la relación que hay entre la ausencia de información de la identidad personal de los usuarios en las transacciones con *bitcoin*, el anonimato y su efecto en la regulación ALD/FCT de las criptomonedas, así como de la incógnita respecto de a cuál de todos los participantes en una transacción con *bitcoin* se debería regular para lograr una regulación más eficiente: a la red *bitcoin*, al remitente, al lavador, y después se hablará sobre el breve análisis a la "Ley *Fintech*" en México, considerando la regulación en Estados Unidos y la Unión Europea.

---

[20] *Proxy*: Servidor que actúa como intermediario en una red. Estas aplicaciones funcionan como intermediario entre la comunicación de un navegador con Internet. Así, la información de un ordenador va, primero, al ordenador intermedio (proxy), y éste se lo envía al ordenador de destino, de manera que no existe conexión directa entre el primero y el último. Es una herramienta conocida por proporcionar anonimato en Internet al ocultar la dirección IP pública del usuario. En lugar de hacer una solicitud de forma directa para, con un proxy la solicitud se envía a un servidor proxy que luego enviará la solicitud para acceder al sitio desde una IP diferente. Funcionan como control de acceso y filtrado de contenido. (Cunha, D. 2020).

[21] *Secure Shell*: es un protocolo que garantiza que tanto el cliente como el servidor remoto intercambien informaciones de manera segura. Su principal función es el acceso remoto a un servidor por medio de un canal seguro en el que toda la información está cifrada. Encripta la sesión de conexión, haciendo imposible que alguien pueda obtener contraseñas no encriptadas. Además, usa técnicas de cifrado que hacen que la información que viaja por el medio de comunicación vaya de manera no legible, evitando que terceras personas puedan descubrir el usuario y contraseña de la conexión ni lo que se escribe durante toda la sesión.

Antes que nada, recordemos que anteriormente se comentó que la tecnología sigue avanzando y los delincuentes utilizan estos avances para tomar distancia de sus actividades y ganancias ilegales mediante la banca virtual y transferencias electrónicas de dinero, donde pueden comprar, vender e intercambiar bienes sin ningún tipo de interacción física y aún y cuando este tipo de servicios mantiene registros digitales para identificar a un remitente y un receptor, los delincuentes cuentan con los medios para confundir su identidad digital, falsificando su dirección de protocolo de internet o utilizando la cuenta de otro individuo, y así, sus actividades no se puedan rastrear.

Así pues, cabe señalar que (Bryan, 2014), refiere que las monedas virtuales, como el *bitcoin*, agregan otra capa de anonimato al permitir a los usuarios transferir valores sin la recopilación de ningún tipo de información sobre la identificación personal. Lo que genera que continuamente, las regulaciones no afectan a las monedas virtuales por la falta de previsión de los profesionales que redactan el reglamento, creando así una zona gris jurídica, lo que hace que los delincuentes sigan capitalizando la innovación tecnológica para potenciar sus actividades ilícitas. De hecho, señala que: "*El blanqueo de capitales es un arte delictivo particular que puede beneficiarse del adelanto tecnológico*".

.

Por lo tanto, el anonimato y la resilencia de su protocolo, son unas de las principales características de *Bitcoin* que resultan desfavorables para una regulación Anti Lavado de Dinero y Combate al Financiamiento del Terrorismo (ALD/CFT) efectiva, esto, al no poder vincular a un usuario identificable a una sola dirección de *bitcoin*, por lo que, al tratar de rastrear la entrada, la superposición y el reingreso de fondos lavados, sería demasiado difícil para las entidades ejecutoras.

Además, como cada nodo minero de la red *Bitcoin* recibe y procesa todas las transacciones y la red *Bitcoin* escala automáticamente la dificultad para completar bloques de acuerdo al poder total de procesamiento de todos los mineros, impedir el funcionamiento de la red *Bitcoin* implica deshabilitar a todos los mineros en la red. Por tal motivo, los esfuerzos antilavado de dinero, enfrentan un objetivo difícil de identificar y, al mismo tiempo, la red es impermeable a la intercepción, es decir, que no puede ser penetrado por la humanidad para detenerlo o frenarlo. (Bryan, 2014).

También, recordemos que en cualquier transacción de *bitcoin*, aún en aquellas que implican actividades ilícitas de lavado de dinero, involucra como cinco participantes: (I) el remitente de *bitcoin* que inicia la transacción en la red, en nuestro caso con dinero sucio; (II) el receptor de *bitcoin* quien acepta los *bitcoins* el lavador que ayuda al remitente ofuscar la fuente del dinero sucio); (III) los mineros de *bitcoin* que verifican las transacción y las procesan completando bloques por una tarifa; (IV) el equipo central de desarrollo de *Bitcoin*, que actualiza el código base de *Bitcoin* según sea necesario; y (V) los cambios de moneda *bitcoin*, que facilitan la conversión de *bitcoins* para obtener monedas y viceversa. Ahora, la pregunta es *¿A quién se debe regular?* Ante esta pregunta, Bryan (2014) y, comenta lo siguiente:

- Regular la red *Bitcoin* será difícil, ya que, por su complejidad y naturaleza descentralizada, la hace impermeable a un solo punto de falla. En vez de tratar de vigilar todos los aspectos de la red *Bitcoin*, es más eficaz analizar cada entidad de transacción de *bitcoin* individualmente y determinar en un análisis de coste-beneficio, cuáles podrían ser los mejores aspectos a regular. La regulación de la transacción de *bitcoin* depende en gran medida de la entidad reguladora específica, reforzando aún más este análisis entidad por entidad.

- Regular al remitente inicial de *bitcoin*, no sería factible por la naturaleza seudónima y dispersa de las identidades de los remitentes. Cuando un usuario remitente envía *bitcoins* a otro usuario de *bitcoin* o a un servicio de lavado de dinero, no se proporciona información de identificación personal (PII), así que, la posibilidad de identificar al propietario de una dirección de *bitcoin* de un solo uso es extremadamente bajo. Por otro lado, atacar la base de usuarios de una comunidad quizá implicaría una mayor desconfianza y desaprobación hacia el gobierno, lo que pudiera llevar a un aumento de anonimización. Así qué, la inversión de recursos para intentar rastrear a los usuarios que no han proporcionado ningún PII supera el beneficio que se alcanzara a obtener de regular lo que pudiera ser transacciones menores.

- Regular a los receptores o quizá los lavadores de *bitcoin*, al parecer, tampoco es muy viable. Si bien es cierto que se podría permitir la aplicación y regulación específicas de quienes actúan con una intención delictiva y evitar la reacción negativa de la comunidad por el intento de regular a todos los remitentes de *Bitcoin*. La regulación de los lavadores también se enfrenta a los mismos problemas de anonimato, así que, si no hay salida física o PII para rastrear, las fuerzas del orden, se destinarán recursos importantes para que al final, se obtengan recompensas relativamente pequeñas. Además, muchos infractores se pueden esconder bajo las leyes internacionales menos rígidas y evitar las leyes más estrictas mientras impulsan actividades ilícitas. Así que, ir tras los receptores de *Bitcoin* y el dinero de los lavadores en particular, resulta ineficiente.

- Regular a los mineros no resultaría muy eficiente, al tomar los mineros, el lugar de un procesador de pagos, que presentan una cierta falta de culpabilidad de la minería al procesar las transacciones, siendo que el software de minería es el que procesa transacciones para bloquear sin que intervenga el usuario. Así como hay usuarios de *bitcoin* que entienden cómo opera la red *Bitcoin* y su actividad minera, la gran parte de ellos, solo pueden estar incentivados por la posibilidad de recompensas. Por lo tanto, si hubiera la posibilidad de probar una ceguera intencional, quizá no sería prudente perseguir a los mineros de *bitcoin* de forma individual, aún y cuando cada bloque recompensa dado al minero exitoso, y la dirección de *bitcoin* de ese minero queda registrado en el registro público de *Bitcoin*, además recordemos que un minero sigue siendo seudónimo. También, finalmente, como se dijo con anterioridad, la posibilidad de quebrar y confundir más la red *Bitcoin*, representa que perseguir a los mineros es ineficiente y quizás perjudicial.

- Regular el equipo de desarrollo de *Bitcoin* puede parecer como si se quisiera atacar a una figura de autoridad central lo que evitaría que la red *Bitcoin* actuara uniformemente a los desafíos que enfrenta *bitcoin*, no hay que olvidar que el código de *Bitcoin* es de código abierto y se distribuye a todos aquellos que deseen inspeccionarlo, así que, detener al equipo de desarrollo, realmente no contendría la distribución del código. Cuando mucho, retrasaría temporalmente las actualizaciones de código hasta que otro grupo de personas se hiciera cargo de las actualizaciones de código, probablemente de una manera más secreta, en lugar del grupo conocido públicamente que opera hoy.

  Por otro lado, es complicado afirmar que el equipo de desarrollo de *Bitcoin* tiene alguna información real sobre las transacciones individuales que pueden ocurrir en la red. Este equipo actúa más como una agencia de estándares que como una autoridad central para controlar el funcionamiento de la red. Por lo tanto, aunque el equipo de desarrollo de *Bitcoin* sería un objetivo conocido y quizás más fácil de enjuiciar, es controvertible si eliminar su influencia en la red serviría para disminuir la actividad ilegal que podría ocurrir a través de *bitcoin*.

- Por lo que se refiere a los cambiadores (intercambios) de *Bitcoin*, generalmente tratan con monedas fiduciarias, lo que permitirá que puedan caer con mayor facilidad bajo las leyes de cambio de moneda que definen al dinero como una moneda que se encuentra respaldada por un gobierno. Y como los cambiadores de divisa pueden retener los valores de los compradores y vendedores por transacciones, se pueden clasificar como transmisores de dinero, osea, intermediarios entre un comprador y un vendedor; así pues, de acuerdo a las leyes de transmisión de dinero y al estar probablemente menos descentralizados, será más fácil apuntar a la regulación.

  Un cambiador (intercambio) que facilita cientos o miles de transacciones, posiblemente recibiendo tarifas por procesar transacciones, como dice Bryan: “no podrá probar una falta legítima de conocimiento, ya que no es razonable que su actividad no estuviera regulada mientras que los intercambios de pago similares están sujetos a las leyes de transmisión y cambio de moneda estatales, federales e internacionales”. (Bryan, 2014, p.441). Por lo tanto, es probable que la regulación de *bitcoin* en los intercambios de divisas, tengan el mayor efecto con la menor inversión de recursos.

Después de haber hecho un análisis sobre la interrogante de ¿A quién se debe regular?, vale la pena retomar nuevamente las Recomendaciones del GAFI (estándar internacional contra el (LA/FT) y la guía para un enfoque basado en el riesgo de monedas virtuales *“Guidance for a Risk-Based Approach: Virtual Currencies”* publicada en 2015, donde el GAFI reconoce que las monedas virtuales que pueden ser cambiadas de ida y vuelta por una moneda fiduciaria o dinero real, presentan un alto riesgo de lavado de activos, puesto que los delincuentes generalmente buscan retirar el dinero en moneda virtuales o fiduciarias, por eso es que los puntos de intercambio entre monedas virtuales y fiduciarias requieren de una mayor transparencia y supervisión entre los participantes en el ecosistema de monedas virtuales. Pero Serrano (2020),

señala que esto fue un error, ya que el riesgo de lavado de activo también se presenta al intercambiar una moneda virtual (*bitcoin*) por otra moneda virtual (Monero), siendo esta última, una moneda virtual descentralizada y totalmente anónima.

En 2019 se actualiza la guía, donde ya se consideran los intercambios entre activos virtuales. Así pues, de acuerdo a lo señalado por el GAFI, cualquier persona natural o jurídica que tenga como objeto de su negocio una o más de las siguientes actividades u operaciones, se debe considerar como un VASP, es decir, "entidad obligada":

- Intercambios entre activos virtuales y moneda fiduciaria.
- Intercambios entre una o más formas de activos virtuales.
- Transferencias entre activos virtuales.
- Custodia o administración de activos o instrumentos virtuales teniendo el control sobre estos.
- Participar en la provisión de servicios financieros relacionados con la oferta inicial y/o venta de activos virtuales.

Por lo tanto, cuando cualquier persona natural o jurídica que realice cualquier actividad comercial que encaje en cualquiera de los cinco modelos de negocio antes mencionados se considera una entidad obligada y debe cumplir con un programa antilavado de activos sustentado en un enfoque basado en riesgos, de acuerdo a las características y el contexto de cada entidad obligada y, considerando por lo menos las reglas relacionadas con: I. Conocimiento del Cliente (KYC), II. la Debida Diligencia del Cliente (CDD), III. el registro de transacciones y IV. La obligación de monitorear, identificar y reportar transacciones sospechosas (FATF, 2019).

3.4.2 Análisis comparativo de la normativa aplicable en Estados Unidos, Europa y México.

El propósito de las medidas reglamentarias en la prevención del lavado de activos, es impedir que el flujo de dinero proveniente de la economía sumergida, es decir, de delitos o de actividades ilícitas, ingresen al sistema financiero de una economía legítima sin ser detectados. Como se vio anteriormente, Recomendaciones del GAFI determinan el estándar internacional, y cada país decidirá cómo abordar la prevención del lavado de activos conforme a la naturaleza de su jurisdicción. En esta sección se examinará las diferentes estrategias utilizadas en los Estados Unidos, la Unión Europea y México, para evitar que el "dinero sucio" representado en monedas virtuales ingrese a sus economías.

Debido al gran auge que han generado las criptomonedas en el mercado financiero mundial, principalmente en Estados Unidos, Alemania, Reino Unido y Japón, llevó a los gobiernos de estos países a regular las operaciones con esas monedas virtuales, desde su administración hasta su funcionamiento. Mientras que, en México, se han empezado a realizar este tipo de transacciones de manera paulatina con cautela y reserva, manteniendo fuera del sistema financieros los activos virtuales al no autorizar a las IC o ITF, ofrecer operaciones con activos virtuales al público en general. Según Banco de México, la volatilidad, el costo, el nivel de riesgo y la asimetría de la

información, son algunos de los factores por los que ha mantenido una sana distancia entre el sistema financiero y sus usuarios al realizar operaciones con activos virtuales.

Al respecto, cabe mencionar que la normativa de Estados Unidos y las directivas de la Unión Europea se consideran unas de las regulaciones que siempre han llevado la delantera en la prevención de lavado de dinero y financiamiento al terrorismo, y por su parte, México, se considera como el ecosistema *Fintech* más grande de Latinoamérica y su regulación del sector *Fintech*, abre el camino para América Latina y lo pone a la vanguardia.

Por lo anterior, es importante mostrar el enfoque de cada una de las normativas para la prevención del lavado de activos a través de medidas reglamentarias, mismas que se presentan en el siguiente cuadro:

Cuadro 3.1

Comparativo de normativa aplicable a Estados Unidos, Unión Europea y México

Estados Unidos		Unión Europea		México	
Año	**Norma**	**Año**	**Norma**	**Año**	**Norma**
1970	Mediante la Ley de Secreto Bancario (Bank Secrecy Act (BSA)), "codificaeda en el Título 31 del Código de los Estados Unidos" (Madginger, 2012, p.24), Estados Unidos inicia el combate contra el lavado de activos y otros delitos financieros, estableciendo los requisitos de mantenimiento de registros y la obligación de reportar por parte de las instituciones, al poder ser utilizadas como vehículos de lavado de activos (Bryans, 2014, p.456). Por lo que es pieza clave en la lucha contra el lavado de activos.	**1991**	Primera Directiva para la Prevención del Blanqueo de Capitales (1AMLD). Con el propóstio de "coordinar las medidas en los diferentes Estados miembros y salvaguardar la estabilidad del sistema Financiero en su Conjunto" (Houben & Snyers, 2018, p.58).	**2004**	La Unidad de Inteligencia Finaniera (UIF) se crea para colaborar en la prevención y combate a los delitos con recursos de procedencia ilícita (lavado de dinero) y financiamiento al terrorismo. Su tarea principal es implementar y dar seguimiento a mecanismos de prevención y detección de actos, omisiones u operaciones que favorezcan los delitos previstos en el Código Penal: i. Operaciones con Recursos de Procedencia Ilícita (art. 400 bis.) y ii. Financiamiento al Terrorismo (art. 139 quáter).
1990	La red contra los Delitos Financieros (Financial Crimes Enforcement Network (FinCEN)) del Departamento del Tesoro de los estados Unidos, se crea para regular y administrar la BSA, que funciona como la Unidad de Inteligencia Financiera (UIF).	**2001**	Segunda Directiva para la Prevenión del Blanqueo de Capitales (2AMLD).	**2012**	Mediante decreto del presidente Felipe Calderón Hinojosa, se expide la Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita (LFPIORPI), conocida como "Ley antilavado", se emite para proteger el sistema financiero y la economía nacional, estableciendo medidas y procedimientos para prevenir y detectar actos u operaciones que involucren recursos de procedencia ilícita. En su art. 17 enlista actividades vulnerables al lavado de dinero, quedando sujetas a las obligaciones previstas en esta ley. (Ley que entra en vigor en 2013).
2013	FinCen emite una sere de pautas de interpretación (interpretative Guidelines) y resoluciones administrativas (administrative rulings) para los modelos de negoio que involucren monedas virtuales. Define las monedas virtuales.	**2006**	Tercera Directiva para la Prevención del Blanqueo de Capitales (3AMLD). Después de la revición del GAFI a las 40 Recomendaciones de 2003).		
2019	En la normativa de FinCEN, cualquier transacción entre moneda virtual y moneda fiduciaria o entre moneda virtual y moneda virtual estará sujeta a la regulación. Sobre las Empresas de Servicios Monetrios (MSB), la aplicación de la regulación de FinCEN también se aplica para ciertos modelos de negocio que involucre la transmisión de recursos denominados	**2015**	Cuarta Directiva para la Prevención del Blanqueo de Capitales (4AMLD). Después de la revición del GAFI a las 40 Recomendaciones en 2012. Establece un enfoque basado en riesgos y la implementación de un programa contra el lavado de activos por parte de las entidades obligadas. Aún y con una falta de referencia explícita a las monedas virtuales en la aplicación de la 4AMLD, se sostenía que las monedas estaban dentro de este ámbito, además, tampoco hay referncia sobre entidades obligadas relacionadas con el manejo de monedas virtuales como cambiadores o proveedores de servivio de billetera en línea.	**2018**	Por decreto se adiciona a la LFPIORPI, en su artículo 17 de las actividades vulnerables, la fracción XVI relativa a las realizadas con activos virtuales, quedando todas, sujetas a las obligaciones previstas en esta ley y define lo que se debe entender por activo virtual.
	en valor sustituible por moneda de curso legal, específicamente monedas virtuales convertibles (CVC). Bajo la normativa de FinCEN, las instituciones financieras y las MSB deben estar registradas ante el Departamento del Tesoro de EU y desarrollar, implementar y mantener un programa escrito contra el lavado de activos para prevenir que las MSB se utilicen para lavar activos y el financiamiento de actividades terroristas.	**2018**	Quinta Directiva para la Prevención del Blanqueo de Capitales (5AMLD). Define a las monedas virtuales e introduce a los proveedores de servicio de cambio de monedas virtuales por moneda fiduciaria (cambiadores) y a los proveedores de servicio de custodia de monederos electrónicos (proveedores de servicio de billetera en línea) en la lista de entidades obligadas. Los estados miembros debieron transponer este cuerpo normativo antes del 10 de enero de 2020, con la finalidad de lograr una armonización para la prevención del lavado de activos en relación con las monedas virtuales convetibles a nivel de la Unión Europea. Sexta Directiva para la Prevención del Blanqueo de Capitales (6AMLD). Tiene por objeto que la definición de actividades delictivas que constituyan delitos antecedentes a efectos del blanqueo de capitales, sea uniforme en todos los Estados miembros. También se hace mención al uso de monedas virtuales; el cual presenta nuevos riesgos y desafíos desde la perspectiva de la lucha contra el blanqueo de capitales. Describe los procedimientos para la cooperación entre estados para la detección de delitos financieros y agresiones transfronterizas. Del mismo modo, se establece vigilancia internacional para las empresas que no cumplen con la directiva. Define sanciones para no dar lugar a dudas en la jurisprudencia relacionada y añade controles más exhaustivos para los procesos de verificación de identidad online. Recoge todas las prácticas en materia de prevención del blanqueo de capitales y la financiación del terrorismo de las compañías de todos los sectores, principalmente del financiero y los relacionados que deben aplicar y avanza en las sanciones impuestas si no se cumplen.		Dentro de sus obligaciones está: - Su registro ante e SAT (a partir del 3 de febrero 2020). - Identificación de sus clientes y usuarios. - Integración de expedientes (a partir de septiembrre 2019). - Presentar avisos de las operaciones realizadas ante la UIF, a través del SAT (a partir del 20 de abril de 2020). Se emite la "Ley *Fintech*" por la SHCP, CNBV y Banco de México, para regular los servicios financieros que prestan las Instituciones de Tecnología Financiera (ITF) y reconoce como *Fintech* a las Instituciones de Financiamiento Colectivo, de Fondo de Pago Electrónico y Sociedades Autorizadas para Operar con Modelos Novedosos. Se enfoca en las áreas de pagos electrónicos, financiamiento colectivo y activos virtuales -valores no cubiertos por ninguna entidad financiera regulada-. Mediante disposiciones de carácter General emitidas por la SHCP, se obliga a las ITF a establecer medidas y procedimientos para prevenir y detectar actos y omisiones u operaciones ubicados en los supuestos del art. 139 quarter o 400 bis del Código Penal, e implementar una metodología para evaluar los riesgos.
				2019	La Circular 4/2019 que emite Banco de México, para las IC e ITF, les permite a dichas instituciones a usar activos virtuales únicamente en sus procesos u operaciones internas, previa autorización de Banxico. El propósito de esta disposición es determinar los activos virtuales y definir sus características, con los que se podrán operara, establecer términos, condiciones y restricciones para el uso de dichos activos, sobre la contratación de terceros para la prestación de servicios con activos virtuales, así como la información a presentar.
				2021	La UIF emite un Criterio General aplicable a los proveedores de servicios de activos virtuales conforme al art. 17 fracc. XVI de la LFPIORPI, quedando sujetos a las obligaciones previstas en dicha Ley, aún cuando la infraestructura tecnológica se encuentre en a jurisdicción de otro país.

Fuente: elaboración propia, de Criptomonedas y lavado de activos: un análisis comparativo. Revista Nº 71 Abr.-Jun. 2020, (Serrano U., 2020), UIF México, recuperado de https://uif.gob.mx/es/uif ., LFPIORPI y LRITF, Circular 4/2019 de Banco de México y Criterio General para la aplicación de la fracción XVI del artículo 17 de la LFPIORPI, recuperado de https://www.gob.mx/uif/prensa/comunicado-040-la-uif-emite-criterio-general-para-la-aplicacion-de-fraccion-xvi-del-articulo-17-d0e-la-lfpiorpi?idiom=es.

Como se puede ver en el cuadro anterior, Estados Unidos ha sido el pionero en la prevención y combate en contra del lavado de activo y otros delitos financieros, al ser el primero en crear regulaciones (Ley del Secreto Bancario, 1970) e instituciones (FinCEN ,1990) para el combate contra lavado de activos y otros delitos financieros. Por su parte, el Parlamento de la Unión Europea adopta directivas para la prevención de blanqueo de capitales, siendo la primera en 1991, para coordinar las medidas de los países miembros, sus directivas, se han caracterizado por innovar los estándares internacionales y aplicar medidas que blinden el sistema financiero europeo. Mientras que México, no fue sino hasta 2004 (casi 30 años después) que crea la UIF para la prevención y el combate contra el lavado de dinero, para implementar y dar seguimiento a mecanismos de prevención y detección de operaciones con recursos de procedencia ilícita y financiamiento al terrorismo.

En el año de 2013, mientras Estados Unidos emite a través de FinCEN pautas de interpretación y resoluciones para modelos de negocio que involucren monedas virtuales, en México entra en vigor la LFPIORPI “Ley antilavado” para proteger al sistema financiero y la economía nacional, estableciendo medidas y procedimientos para prevenir y detectar actos u operaciones que involucren recursos de procedencia ilícita y relaciona las actividades vulnerables al lavado de dinero.

Por su parte, en 2015, en la Unión Europea, entra en vigor la Cuarta Directiva, siguiendo las Recomendaciones del GAFI, que establece un enfoque basado en riesgos, así como la implementación de un programa contra el lavado de activos por parte de las entidades obligadas.

En tanto, no es sino hasta 2018, que México, emite la “Ley *Fintech*” para regular los servicios financieros ofrecidos por las ITF, así como su organización, operación, funcionamiento, y la autorización para poder operar, contemplando las áreas de pagos electrónicos, financiamiento colectivo y el funcionamiento de los activos virtuales ofrecidos por medios innovadores, delimitando que las ITF sólo podrán operar con activos virtuales en su operación interna y no de cara al cliente, los cuales serán determinados por Banxico, de conformidad con lo estipulado por la SHCP, también se define a los activos virtuales, así como las disposiciones que obligan a las ITF a establecer medidas y procedimientos para prevenir y detectar actos y omisiones u operaciones relacionadas con el Financiamiento al Terrorismo u Operaciones con Recursos de Procedencia Ilícita, e implementar una metodología basada en riesgos para evaluar los riesgos. De acuerdo a esta Ley, los activos virtuales, no pertenecen al sistema financiero mexicano al no ser respaldados por el gobierno y el Banco de México, sin embargo, las reconoce como operaciones Financieras.

Por otro lado, mediante decreto, adiciona a la LPRIOPI en su art. 17 de las actividades vulnerables, adiciona la fracción XVI relativa a los activos virtuales, donde señala como actividad vulnerable “al intercambio de activos virtuales por sujetos distintos a entidades financieras en plataformas electrónicas, digitales o similares, administrar u operar la compra venta de éstos activos, proveer medios para custodiar, almacenar o transferir activos virtuales distintos a los reconocidos por Banxico”, quedando todas, sujetas a las obligaciones previstas en dicha Ley y

también, define como activo virtual “toda representación de valor registrada electrónicamente y utilizada entre el público como medio de pago y cuya transferencia sólo puede realizarse a través de medios electrónicos” y será objeto de aviso ante la Secretaría cuando el monto de la operación de compra o venta de un cliente sea por una cantidad igual o superior al equivalente a seiscientas cuarenta y cinco Unidades de Medida y Actualización.

Mientras tanto, La Unión Europea, en su Quinta Directiva, da una definición sobre las monedas virtuales e introduce a los proveedores de servicio (cambiadores, custodia de monederos electrónicos, etc.) dentro de las entidades obligadas incluyendo las realizadas con activos virtuales, haciendo así, sujetos obligados a esta Ley a todo aquél que las realice.

Para 2019, Estados Unidos, aplica la regulación FinCEN a las empresas de servicio monetario (MSB) que involucran transmisión de monedas virtuales convertibles y bajo esta normativa, las instituciones financieras y las Empresas de Servicios Monetarios (MSB, siglas en inglés) se deben registrar ante el Departamento del Tesoro e implementar un programa contra el lavado de activos. A la par, en México, Banxico emite la Circular 4/2019 para las IC e ITF, donde, por el riesgo que conllevan los activos virtuales, considera mantener sana distancia entre los activos virtuales y el sistema financiero, por lo que sólo se les permite operar con activos virtuales para su operación interna y previa autorización por dicha autoridad, así como los términos, y condiciones para sus usos, contratación de terceros para servicios con dichos activos y reportes a presentar.

En 2021, La UIF de México, a fin de mantenerse a la vanguardia sobre el monitoreo de proveedores de servicios de activos virtuales, emite un Criterio General aplicable a todos los proveedores que ofrezcan servicios de activos virtuales referidos en el Art. 17 fracción XVI de la LFPIORPI, quedando sujetos a cumplir con las obligaciones previstas en dicha Ley, aunque la infraestructura tecnológica se encuentre en la jurisdicción de otro país.

Es de relevancia hacer un análisis sobre la definición de moneda digital y/o activo virtual, lo que puede impactar en el alcance de las regulaciones.

De acuerdo con (GAFI,2014), se darán las siguientes definiciones:

Moneda virtual: a la representación digital de valor que puede ser comerciada digitalmente y funciona como un medio de cambio; y/o una unidad de cuenta; y/o un depósito de valor, pero no tiene curso legal en ninguna jurisdicción, que cumple con las funciones antes citadas por común acuerdo de la comunidad de sus usuarios. Divide las monedas virtuales en moneda virtual convertible y no convertible.

- La moneda virtual convertible (o abierta), tiene valor equivalente en moneda real y se puede intercambiar una y otra vez por dinero real. como *bitcoin*.

- Moneda virtual no convertible (o cerrada), específica de un mundo virtual particular, como los videojuegos o Amazon.com, y de acuerdo a las normas que regulan su uso, no se puede cambiar por dinero real.

En Estados Unidos, (FinCEN, 2013) define a la moneda virtual como "un medio de intercambio que funciona como una moneda en algunos entornos, pero no tiene todos los atributos de la moneda real…. no tienen un estado de curso legal en ninguna jurisdicción" y (FinCEN, 2019) define a las monedas virtuales convertibles (CVC) como “un tipo de moneda virtual que tiene un valor equivalente como moneda, o actúa como un sustituto de la moneda, y es por lo tanto, un tipo de “valor que sustituye a la moneda”, señalando que cualquier transacción que se realice en moneda virtual convertible estará sujeta a la regulación FinCEN, sin importar que ésta esté representada en un token físico o digital o si el tipo de libro de contabilidad utilizado para registrar las transacciones está centralizado o distribuido, o el tipo de tecnología utilizada para la transferencia del valor”. Es decir, cualquier transacción entre moneda virtual y moneda fiduciaria o entre moneda virtual y moneda virtual estará cubierta por FinCEN.

En la Unión Europea, el artículo 3(18) de la 4AMLD, modificado por la 5AMLD, define las monedas virtuales como la “representación digital de valor no emitida ni garantizada por un banco central ni por una autoridad pública, no necesariamente asociada a una moneda establecida legalmente, que no posee el estatuto jurídico de moneda o dinero, pero aceptada por personas físicas o jurídicas como un medio de cambio y que puede transferirse, almacenarse y negociarse por medios electrónicos”. Y el artículo 2(1)(3)(c)(g) y (h) de la 4AMLD, modificado por la 5AMLD, considera como entidades obligadas sólo a los “proveedores de servicios de cambio de monedas virtuales por monedas fiduciarias” y a los “promovedores de servicios de custodia de monederos electrónicos”. Por lo que, de acuerdo a la interpretación literal de la Directiva, el intercambio de una CVC a otra CVC (como es el caso de *bitcoin* a ethereum) o en el caso que se utilizara un servicio de mezcla, no estaría sujeto a la regulación de la Directiva.

En México, el Banco de México, refiere que, “en los medios, los activos virtuales tienden a asociarse con el concepto de moneda e incluso con servicios o productos financieros, sin embargo, estos no cumplen con los requisitos para ser considerados como moneda, pues incumplen con las funciones de la definición clásica del dinero: a) depósito de valor: el valor de los activos virtuales ha sido muy volátil. Los cambios bruscos en el precio muestran que su función como depósito de valor es ineficiente, b) sobre el medio de cambio, a pesar de que ya se pueden comprar bienes y servicio, aún son pocos los comercios que los aceptan y c) en cuanto a la unidad de cuenta, por la volatilidad en valor, los precios referidos a éstos se deben ajustar continuamente, por lo que limita su función como unidad de cuenta; por lo tanto, considera que los activos virtuales no representan algún tipo de moneda, servicio o producto financiero.

Define a los activos virtuales como “una unidad de información que no representa la tenencia de algún activo subyacente a la par, y que es unívocamente identificable, incluso de manera fraccional, almacenada electrónicamente ….”

Por su parte, La LFPIORPI y la “Ley *Fintech*”, definen a los activos virtuales como toda representación de valor registrada electrónicamente y utilizada entre el público como medio de pago y cuya transferencia sólo puede realizarse a través de medios electrónicos y para efectos de la “Ley *Fintech*”, se considerará como activo virtual sólo aquéllos que determine Banxico.

Las instituciones del sistema financiero no están autorizadas a celebrar ni a ofrecer al público operaciones con activos virtuales como es el caso de *bitcoin*, ether, xrp o cualquier otro que pudiera incluir servicios de depósitos, o cualquier otra forma de custodia, el intercambio o transmisión. No están permitido por la autoridad financiera.

No obstante lo anterior, Banco de México, en su página *web*, como parte de la explicación del proceso de compra-venta de activos virtuales, muestra un esquema de la compra y transacción de dichos activos, donde menciona que: “Además de poder obtener nuevos activos virtuales mediante la resolución de problemas matemáticos de alta complejidad, o según sea el caso de emisión para cada activo virtual, es posible adquirir activos virtuales ya existentes por medio de "exchanges", instituciones donde se intercambian activos virtuales por dinero de curso legal u otros activos virtuales. Aunque la transmisión de activos virtuales se da en la cadena de bloques, las operaciones de este tipo de empresas pueden ser independientes del sistema que sustenta dichos activos.” A continuación, se presenta el esquema de compra y transacción de activos virtuales.

Figura 3.9
Compra y transacción de activos virtuales

Fuente: Banco de México. Recuperado en https://www.banxico.org.mx/sistemas-de-pago/3---como-funciona-un-activo.html, diciembre 2021.

Después de este breve análisis, se puede concluir que a pesar de que las regulación de Estados Unidos y la Unión Europea definen a las monedas virtuales como una representación digital de valor que es aceptado como medio de cambio, sin el respaldo de un banco central o autoridad gubernamental y sin un estado de curso legal, la regulación de México no solo no reconoce a los activos virtuales como una moneda, por no cumplir con las funciones de la definición clásica del dinero, requisito para poder ser considerados como monedas; definiendo entonces a los activos virtuales como una representación de valor registrada electrónicamente que se utiliza como

medio de pago y sólo se puede transferir a través de medios electrónicos. Además, no autoriza a las entidades financieras a ofrecer al público en general, operaciones con activos virtuales. Sin embargo, la LFPIORPI considera como actividad vulnerable y sujeta a esta Ley el intercambio de activos virtuales por sujetos distintos a las Entidades Financieras mediante plataformas electrónicas, digitales o similares, así como que administren u operen, operaciones de compra, custodia, almacenamiento, o transferencia de activos virtuales.

El alcance del marco legal es diferente. Mientras que, para Estados Unidos, todas las transacciones con monedas virtuales están sujetas a su regulación. Para la Unión Europea, sólo el intercambio entre la moneda virtual convertible y moneda fiduciaria está bajo el alcance de la 5AMLD, presentándose una laguna en el marco legal de la Unión Europea en la prevención del lavado de activos cuando se utilizan monedas virtuales. Tal vez sea porque tomó de forma literal lo señalado por la Guía del GAFI de 2015, que el intercambio entre monedas virtuales convertibles y monedas fiduciarias, tiene un alto riesgo de lavado de activos, al ser el punto de intersección con el sistema financiero regulado de monedas fiat o uso legal, por lo que se enfocó en la regulación de plataformas que ofrecen servicios de intercambio de monedas virtuales convertibles y monedas fiat. (GAFI, 2015). Para México, la regulación no autoriza al sistema financiero ofrecer al público operaciones con activos virtuales, sólo para sus operaciones internas con aquellos que determine Banco de México, dejando sujetas a la LFPIORPI a todas las entidades no financieras que realicen el intercambio de activos virtuales mediante plataformas electrónicas, digitales o similares, así como que administren u operen, operaciones de compra, custodia, almacenamiento, o transferencia de activos virtuales.

Es de hacer notar, que Estados Unidos y México, dieron un paso adicional al cubrir todos los intercambios entre monedas virtuales previamente a la actualización de la Guía del GAFI publicada en junio de 2019, en donde se introducen a los Proveedores de Servicios de Activos Virtuales (VASP) que realicen intercambios entre monedas virtuales a otras monedas virtuales como entidades obligadas. Además, a pesar de la participación tardía del gobierno de México en las acciones para la prevención y combate del lavado de dinero y financiamiento al terrorismo, se ha posicionado muy rápido en un país a la vanguardia en América Latina en materia de regulación para la prevención combate de lavado de dinero y financiamiento al terrorismo, sin embargo, la corrupción y opacidad de los dirigentes del gobierno no ha permitido su implementación y aplicación eficiente a todos los sujetos obligados, no así incrementando desde luego, los delitos de cuello blanco.

3.4.3 Análisis del alcance de la regulación de la "Ley *Fintech"*.

El Banco de México, como parte de sus atribuciones para Regular las ITF y el Sistema de Pagos Electrónicos Interbancarios (SPEI), ha emitido la "Ley *Fintech"* para prevenir el uso de activos virtuales en el lavado de dinero, combatir el financiamiento al terrorismo y proteger a los consumidores. México, ocupa el séptimo lugar a nivel mundial en la regulación del sector *Fintech* (CNBV, 2019b, párr. 1).

Cómo se ha señalado en capítulos anteriores, aún y cuando el Banco Central ha mantenido una sana distancia con los activos virtuales por el riesgo que representan en materia de PLD/FT, no ha tenido la intención de restringir el uso de tecnologías que brinden un beneficio en pro de la eficiencia o funcionalidad de la operación interna de las ITF e IC, mientras no se incrementen de manera significativa, los riesgos operativos o financieros de las mismas. Como ejemplo del uso de éstas tecnologías están los registros distribuidos, la cadena de bloques, y hasta los propios activos virtuales que podrían llegar a ser factibles, con una previa autorización por parte de Banco de México, si y sólo si, los riesgos de los activos virtuales no impacten al consumidor final.

Por ello es que el Banco Central, con la "Ley *Fintech*", expuso una regulación en la que se define un mecanismo de solicitudes de autorización, a través del cual, se les requiere a las instituciones interesadas en realizar operaciones con activos virtuales, informar la manera en que atenderán los riesgos asociados a las operaciones que realicen con activos virtuales. Así pues, las solicitudes de autorización, no involucran autorización alguna para operar con activos virtuales de cara al cliente, puesto que Banco de México considera que no es conveniente que las instituciones financieras ofrezcan servicios con activos virtuales al público en general y que los riesgos asociados a los activos virtuales no deben impactar al usuario final.

Después de realizar una introspección a la "Ley *Fintech*", se observa que esta ley cuenta con disposiciones para regular la organización, la operación el funcionamiento y los servicios financieros que prestan las ITF, además de los requisitos para su autorización y/o revocación para operar como tal, y la supervisión. Esta regulación está dirigida para las Instituciones de Financiamiento Colectivo (IFC), a las de Fondos de pago Electrónico (FPE), las Operaciones con Activos Virtuales (OAV) y Modelos de Negocio (MN).

En su apartado de operaciones con activos virtuales, define el término "activo virtual" y señala que las ITF (IFC, IFPE y MN), sólo podrán operar con activos virtuales determinados por Banco de México, con apego a las disposiciones de carácter general emitidas por Banxico, donde establece el plazo, los términos y condiciones que se deberán observar; y, contar con una autorización previa antes de realizar operaciones con dichos activos. También, especifica algunas condiciones para la compra venta de activos virtuales con sus clientes y refiere que Banco de México es quien definirá las características de los activos virtuales, así como las condiciones y restricciones de las operaciones y demás actos que puedan realizarse con activos virtuales, la custodia y el control que se ejerza al realizar tales operaciones u actos. Señala que deberán divulgar a sus clientes los riesgos que existen al celebrar operaciones con este tipo de activos, incluyendo que el activo virtual no es moneda de curso legal y no está respaldada por el gobierno, la imposibilidad de revertir las operaciones una vez ejecutadas, la volatilidad del valor del activo y los riesgos tecnológicos cibernéticos y de fraude inherente a los activos.

Por otro lado, conforme a las recomendaciones del GAFI, de implementar un programa antilavado de activos para mitigar los riesgos de lavado de activos asociados con monedas virtuales convertibles, en su artículo 58, la "Ley *Fintech*" obliga a las ITF, a establecer e implementar medidas y procedimientos para prevenir y detectar actos, omisiones u operaciones

que puedan ubicarse en los art. 139 Quárter o 400 Bis del Código Penal Federal, además, una metodología para la evaluación de riesgos a los que estén expuestos y la presentación de reportes, los cuales deben estar contenidas y desarrolladas en un documento que se debe presentar ante la CNBV, mismo que se complementa con las disposiciones de carácter generar a que se refiere el artículo 58, done se encuentran descritos los lineamientos sobre el criterio, los procedimientos, casos, la forma, términos y plazos en que las ITF deben observar respecto a:

a. la debida diligencia del cliente (su identificación, clasificación del grado de riesgo y su conocimiento),
b. la creación, funciones y obligaciones de un comité de control interno y un oficial de cumplimiento,
c. la capacitación a sus miembros del consejo, directivos, funcionarios y empleados,
d. los sistemas automatizados para su operación,
e. la confidencialidad por parte del consejo de administración, comités, funcionarios y empleados de las IFT sobre la información relacionada con los reportes previstos en esta Ley,
f. las listas de personas bloqueadas,
g. los reportes de: operaciones relevantes, operaciones en efectivo en moneda extranjera, de transferencias internacionales que realicen las ITF, operaciones inusuales, operaciones con activos virtuales y de operaciones internas preocupantes,
h. el intercambio de información entre ITF, con otras entidades financieras, centros cambiarios, transmisores de dinero y asesores de inversión autorizados, así como con entidades financieras extranjeras, sobre las operaciones, actividades y servicios que realicen con sus clientes o de éstos entre sí. Entre otros.

Considerando el riesgo que representan los activos virtuales por el anonimato que provee en las transacciones, su facilidad para realizar transferencias transfronterisas, y la falta de controles y medidas homogéneas a nivel global, nos enfocaremos a la regulación que involucre a estos aspectos.

Conforme a la Recomendación 10 del GAFI, los lineamientos para el Conocimiento del Cliente y una Debida Diligencia del Cliente son “una medida esencial para mitigar los riesgos de LA/FT asociados con monedas virtuales convertibles” (GAFI, 2015, p. 12). La identificación del Cliente tiene como propósito realizar una verificación de los datos y documentos que muestren evidencia de la identidad del cliente en el mundo real al establecer una relación comercial e identificar a los beneficiarios reales en todas las transacciones e integrar un expediente con dicha información y el conocimiento del cliente que tiene como propósito monitorear las transacciones en curso.

Así pues, dentro de la política de identificación del cliente, se contempla los lineamientos para recabar datos y documentos para la identificación del cliente, verificar la identidad del cliente y autenticidad de los documentos, donde las ITF tienen la obligación de validar los datos y verificar

la autenticidad de los documentos que se obtengan de manera digital de sus posibles clientes para acreditar su identidad que podrá ser de manera remota sobre aquellos obtenidos de manera digital, conforme a disposiciones emitidas por la CNBV. Una identificación y verificación idónea de la identidad es un problema medular en el terreno de las monedas virtuales, dado que las transacciones se realizan en línea, a través de Internet. Por ende, se requiere de una debida diligencia ampliada para identificar y verificar a los clientes, con la finalidad de recopilar el nombre real del cliente, la fecha de nacimiento, la dirección física en el mundo real, identificar al beneficiario real, entre otras, y verificar dicha información. Cuando las ITF realicen operaciones con activos virtuales, además de los datos y documentos de identificación, deberán obtener la denominación o código del activo virtual y el número de unidades, el monto total del equivalente del activo virtual en moneda nacional y la fecha de operación.

A parte de la identificación del cliente, también contempla la identificación de propietarios reales, proveedores de recursos, beneficiarios y terceros autorizados en cuentas abiertas por los Clientes.

En segundo lugar, las ITF deben contar con un modelo de evaluación de riesgos para clasificar a sus clientes por grado de riesgo (alto, medio y bajo), considerando productos y servicios, tipos de clientes, países o áreas geográficas, transacciones y canales de envío o distribución transacciones e infraestructura tecnológica, con las que operan la ITF.

Sobre el conocimiento del cliente, las ITF deben implementar procedimientos para dar seguimiento y monitoreo a las operaciones, actividades o servicios realizados por sus clientes y el perfil transaccional de cada cliente (monto, número, tipo, naturaleza y frecuencia de las operaciones), con la información que proporcionen, el origen y destino de los recursos o bienes objeto de la operación, información sobre la geolocalización del dispositivo móvil del cual se realice la operación o servicio; y por supuesto, considerar los umbrales de operación en cuentas o contratos de clientes, con el propósito de identificar operaciones inusuales de los clientes por las operaciones que no concuerden con su perfil transaccional, para lo que deben contar con un sistema de alerta para el seguimiento y detección oportuna de un cambio en el comportamiento del cliente; y sobre la transaccionalidad del cliente, se debe informar aquellas transacciones que sean igual o rebasen el umbral de 5,000 USDLS en el reporte de operaciones relevantes y aquellas compras de activos virtuales que sean igual o superior al umbral de 7,500 UDIS, en el reporte de operaciones con activos virtuales.

Las ITF, deben conservar por un periodo no menor a diez años la documentación e información que acredite la operación, actividad o servicio de que se trate, los datos y documentos que integran su expediente de identificación, los registros históricos de las operaciones, así como la información relacionada con la generación y envío de los reportes antes mencionados a la SHCP por conducto de la CNBV. Este requisito de conservar los registros tiene el propósito de facilitar la cooperación entre dichos modelos de negocio y las autoridades para la prevención, detección e investigación en casos de LA/FT.

Por otro lado, también deben contar con sistemas automatizados que les permita conservar actualizar y consultar los datos y documentos que se encuentren dentro de los expedientes de cada clientes, generar y transmitir los reportes obligados a enviar, “permitir conocer la trazabilidad y el origen y destino de los activos virtuales con los que operen”, clasificar los tipos de operaciones, productos o servicios que ofrezcan, monitorear las operaciones realizadas por cada uno de los clientes a fin de detectar operaciones inusuales y ejecutar un sistema de alertas cobre el comportamiento o perfil transaccional de un cliente. Cabe destacar que la Ley, no define que se debe entender por trazabilidad, origen y destino de los activos virtuales, ni tampoco establece mecanismos para que dichos sistemas puedan cumplir con estos requisitos.

La obligación de las ITF de reportar operaciones con activos virtuales, tienen la intensión de brindar pistas significativas para las transacciones financieras ilegales y documentar algunas de las grandes transacciones en efectivo cometidas por delincuentes en el lavado de activos.

También, las IFT, pueden intercambiar información sobre las operaciones, actividades o servicios que realicen con sus clientes o de éstos entre sí, con otras ITF, Entidades Financieras como centros cambiarios, transmisores de dinero y asesores en inversiones autorizados apegándose a las leyes que las regulan, así como con Entidades Financieras Extranjeras conviniendo un tratamiento de confidencialidad sobre la información que compartan; esto, con el propósito de fortalecer las medidas y procedimientos para para prevenir y detectar actos, omisiones u operaciones de lavado de dinero o financiamiento al terrorismo.

Mientras que las ITF o IC no están autorizadas para ofrecer al público en general operaciones con activos virtuales, hay entidades que pueden ofrecer servicios relacionados con activos virtuales como las casas de cambio que ofrecen el servicio de compra-venta de activos virtuales al público, mientras no realicen actividades de captación o custodien recursos en moneda nacional o divisas de sus clientes. Esta es la forma en que en México se puede acceder a los servicios de compra-venta de activos virtuales, bajo el riesgo de quien desee realizar este tipo de operaciones, con el entendido de que no están respaldados por alguna institución financiera.

Al no haber una regulación sobre PLD/FT para aquellas personas o entidades diferentes a las entidades financieras que ofrecen servicios de intercambio de activos virtuales por medio de plataformas electrónicas, digitales o similares, que administren, operen, faciliten o realicen operaciones de compra o venta de activos virtuales, o suministren medios para custodiar, almacenar, o transferir activos virtuales. En 2019, se reforma la LFPIORPI para que estas entidades queden sujetas al régimen de esta Ley, al considerar como una actividad vulnerable, la operación de entidades no financieras con activos virtuales estableciéndoles una serie de requisitos, como es la identificación de sus clientes, el llenado de reportes y avisos a la SHCP cuando el monto de la operación sea igual o mayor a 645 UMAS, como en el caso de las ITF.

Aún y cuando no se dice de manera específica, se puede entender que las actividades de una persona o entidad no financiera que pudieran incluir el recibir una forma de valor (moneda/activo virtual convertible) de una persona y transmitir la misma o una forma diferente (moneda/activo

no convertible o totalmente anónimo) de valor a otra persona o ubicación, por cualquier medio electrónico, digital o similar, quedarían cubiertas bajo la reglamentación de LFPIORPI, los riesgos mediante técnicas de anonimización se encuentran mitigados.

Después de este análisis se puede concluir que en México, las entidades financieras no están autorizadas para ofrecer al público en general operaciones con activos virtuales; sin embargo, Banco de México emitió, la "Ley *Fintech*", en prevención del lavado de dinero para regular la organización, la operaciones, el funcionamiento y los servicios financieros que ofrecen las IFC, IFPE y MN, además autoriza que puedan operar con los activos virtuales que determine Banxico bajo las condiciones y términos que éste establezca. También se enfoca en un mecanismo de solicitudes de autorización para operar como ITF, por lo tanto, la "Ley *Fintech*" no considera las, técnicas y herramientas informáticas utilizadas en las transacciones con *bitcoin* y el sistema *blockchain* para conservar el anonimato, en prevención y combate al lavado de dinero, más sin embargo, la regulación los obliga a contar con sistemas automatizados que les permita conocer la trazabilidad, el origen y destino de los activos virtuales con los que operen", clasificar los tipos de operaciones, productos o servicios que ofrezcan, monitorear las operaciones realizadas por cada uno de los clientes a fin de detectar operaciones inusuales y ejecutar un sistema de alertas sobre el comportamiento o perfil transaccional de un cliente.

Por lo anterior, se rechaza parcialmente la Hipótesis 2. "La Ley *Fintech*" considera aspectos regulatorios que previenen y combaten el lavado de dinero mediante disposiciones que permiten identificar las operaciones de mezcla, transaccionalidad e intercambio en el sistema *blockchain*".

Una buena pregunta es saber si las ITF cuentan con los recursos y tecnología necesaria que les permita conocer la trazabilidad y el origen y destino de los activos virtuales con los que operen.

3.4.4 Panorama de México.

Como parte final, es de gran relevancia mencionar las cifras que destaca la UIF en México y la firma *Chainalysis*, Inc., sobre el panorama de México.

De acuerdo a un reporte de Gutiérrez, F. (2022), se destaca lo siguiente:

- La UIF ha actuado de forma constante sobre la vigilancia de las operaciones con activos virtuales, alineada a los criterios del GAFI, contra el lavado de dinero, que dese 2019 ha fortalecido sus recomendaciones para tener mayor alcance sobre estos instrumentos.

- A partir de 2020, la UIF, de las 23 plataformas dedicadas a comercializar activos virtuales e inscritas como actividades vulnerables, empezó a recibir los reportes sobre sus operaciones. Así pues, desde ese año hasta el mes de febrero pasado, la unidad ha recibido 6,375 avisos de operaciones que superan el umbral de los 62,000 pesos de las 23 plataformas dedicadas a esta actividad.

- Por otro lado, la UIF, además, generó un modelo para detectar operaciones de alto riesgo dentro del sistema financiero relacionadas con activos virtuales, mismo que, del 2013 a septiembre del 2021, generó 1,708 reportes de operaciones inusuales, es decir, los bancos han identificado movimientos que tienen relación con criptomonedas. También, permitieron que se identificaran 1,432 sujetos relacionados con operaciones inusuales al realizar transacciones con criptomonedas y los cuales aparecen en las listas de la Unidad de Inteligencia Financiera de Estados Unidos conocida como FinCEN, del Centro Nacional de Inteligencia, entre otras.

- Por su parte, la UIF ha detectado que las criptomonedas son utilizadas como medio de pago en las distintas actividades vulnerables del país, como lo es la compra de joyas, autos e incluso inmuebles. En este contexto, esta instancia ha recibido más de 9,000 avisos de operaciones donde se utilizó algún activo virtual como instrumento de pago los cuales representan una cantidad equivalente a los 6,154 millones de pesos.

- A los investigadores de la UIF, les llama mucho la atención que una cantidad importante de transacciones con criptomonedas se generan desde Jalisco, donde predomina un grupo criminal. A parte de que han detectado más de 12 plataformas que operan ilegalmente al no estar registradas, en la compraventa de estos instrumentos, de las cuales, muchas de ellas, según fuentes de la dependencia se encuentran ancladas en la zona occidente del país.

- La UIF, tiene la esperanza que, en breve, se realicen cambios en la supervisión de estos instrumentos, por una iniciativa de reformas a la Ley antilavado, que se encuentra detenida en el Congreso de la Unión, prevé que la CNBV tome la supervisión de las plataformas registradas como actividades vulnerables dedicadas a la comercialización de criptomonedas, misma que tiene hoy en día, el Servicio de Administración Tributaria (SAT).

Por su parte, *Chainalysis*, en su informe “La Geografía de Criptomonedas 2021”, sobre el análisis de tendencias geográficas en adopción y uso de criptomonedas, reporta que México se encuentra en el lugar 44 en el mundo, dentro de la lista de países con mayor adopción y, de acuerdo a un reporte de la firma *Sherlock Communications*, se espera que en el corto plazo la adopción de estos instrumentos crezca en el país 345 por ciento. (*Chainalysis*,2021).

Según cifras de *Chainalysis*, entre julio del 2019 y junio del 2020, México recibió el equivalente a 2,400 millones de dólares en criptomonedas, mientras que, en dicho periodo, el volumen de transacciones en cuanto a comercio de persona a persona fue el equivalente a 15,600 millones de dólares. También informó que, los flujos ilícitos alcanzaron los 57 millones de dólares, mientras que el valor ilícito enviado a billeteras de otros países fue de 39 millones de dólares. (*Chainalysis*,2021).

Además de lo anterior, por lo que respecta a la red obscura (principal herramienta para lavar dinero): La Unidad de Investigaciones Cibernéticas (UICOT) de la oficina del fiscal general mexicano, informa que es difícil rastrear el uso de *bitcoin* por parte de los delincuentes, incluso con la nueva Ley, debido a que su personal está conformado aproximadamente por 120 personas y para ser competitivo, requeriría aproximadamente cuatro veces eso, agregó. Con la nueva Ley se han activado 1.033 alertas de umbral de *bitcoin* en lo que va del año y los investigadores deben perseguir a cada uno para verificar si podría ser sospechoso y si el usuario está vinculado a algún comportamiento criminal o cárteles. Además, éste sistema solo puede identificar transacciones con compañías comerciales registradas y el equipo tiene una visibilidad limitada de los tratos en la *web* oscura y las plataformas no reguladas, que de acuerdo a los funcionarios estadounidenses y latinoamericanos encubren la verdadera escala del lavado de dinero. (Oré, 2020).

Capítulo 4. Estudio de casos

4.1 Empresas prestadoras de servicio internacionales de activos virtuales

4.1.1 Helix y Coin Ninja.

Empresa de servicios monetarios sin registro en FinCEN, ni programas e informes de acuerdo a la BSA (Ley de Secreto Bancario, sus siglas en inglés) desde que inició sus actividades en 2014 operó sin licencia como intercambiador de monedas virtuales convertibles. Además, evadió sus obligaciones de elaborar, implementar y mantener un programa de cumplimiento contra el lavado de dinero; y no reportar actividades sospechosas, lo que impidió a los investigadores poder recopilar y verificar los nombres, direcciones y otros identificadores de sus clientes en más de 1.2 millones de transacciones y se asoció con direcciones de billetera de moneda virtual que enviaron o recibieron más de $ 311 millones de dólares (FinCEN,2020). También operaba como mezclador de *bitcoins* (*Bitcoin Mixer Helix)* a través de transacciones de *CoinJoin*, y anunciaba sus servicios en la red obscura de Internet como una forma de limpiar *bitcoins* para ocultar la fuente y actividad de las transacciones de sus clientes, y evitar las agencias policiales de Estados Unidos. Los usuarios podían utilizar la herramienta de privacidad (*Bitcoin Mixer Helix*), y un motor de búsqueda de la *darknet* llamado *Grams*, para realizar transacciones en *AlphaBay*, un mercado negro en la red obscura. (FinCEN, 2020; GAFI, S/F; Bastardo,2020).

Larry Dean Harmon, CEO de Helix, del sitio *web Coin Ninja* y fundador del proveedor de criptomonederos *DropBit,* fue arrestado en 2020 y actualmente está siendo procesado por las autoridades del gobierno de Estados Unidos. (Bastardo,2020).

Discusión del caso: El caso de *Helix y Coin Ninja*, empresa de servicios monetarios estadounidense que ofrecía los servicios de intercambio de monedas virtuales convertibles y mezclador de *bitcoin*, por consiguiente, empresa obligada, nos muestra cómo para prestar servicios de intercambio y mezcla de *bitcoin* para ocultar las transacciones de sus clientes de las agencias policiales, incumplió las regulación a la que estaba sujeta, al dar servicio sin tener un registro y licencia ante FinCEN, un programa de cumplimiento contra el lavado de dinero y no reportar actividades sospechosas a las autoridades. En cuanto a los servicios de mezcla, los llevó a cabo mediante una herramienta privada llamada *Bitcoin Mixer Helix* y un motor de búsqueda de la darknet para realizar transacciones en mercado negro *AlphaBay* de la red obscura, a través de transacciones de *CoinJoin* que no requieren la presencia de un intermediario. Así es como logró el blanqueo de recursos (USD 311 millones) proveniente de estupefacientes ilícitos y otras ganancias.

Recordemos que la técnica *CoinJoin* es cuando un grupo de personas acuerdan mezclar una determinada cantidad de fondos y unen sus fondos fuera de línea, creando una transacción con varias entradas y salidas que se firma por todos los participantes y luego realiza la transacción en línea, publicándola en *blockchain.*

Con este caso podemos decir que con el intercambio de monedas virtuales a moneda fiduciaria u otra moneda virtual y con la técnica *Coin Join,* al mezclarce los fondos mediante una transacción fuera de línea (*blockchain*), no se vulnera la seguridad e inmutabilidad del sistema *blockchain* para conservar el anonimato en las transacciones con *bitcoin* para lavar dinero. Por tanto, se rechaza la Hipótesis 1.

4.1.2 BestMixer.io.

Ofreció servicios para mezclar las criptomonedas y se considerada como máquina virtual de lavado de dinero para obscurecer el camino de las transacciones y hacer más difícil que los investigadores puedan rastrear los activos digitales en el sistema *blockchain*. Y ha anunciado descaradamente sus servicios de lavado de dinero. Opera en Europa y presta servicios a clientes de muchos países del mundo".

Es la primera confiscación pública de un servicio de mezcla de *bitcoins*. Fue un gran golpe y la primera acción legal por parte de las autoridades de la UE que, igualmente, busca activamente centros de lavado de dinero en el mundo real y virtual. (Europol, S/F).

En el transcurso de un año lavó por lo menos $200 millones de dólares en criptomonedas. En 2019, las autoridades de la UE cierran e incautan el mezclador de transacciones de *Bitcoin*. Se confiscaron seis servidores con sede en Luxemburgo y los Países Bajos. Además, gran parte del dinero "tenía un origen o destino delictivo". (Osborne, 2019; Europol, S/F).

John Fokker, Jefe de Investigaciones de Ciberseguridad de McAfee (firma que apoyó a la investigación de este caso) explica que mezclar, implica dividir la criptomoneda en cientos de pequeñas transacciones que se pierden en transacciones de otras fuentes. (Osborne, 2019).

De acuerdo al sitio *web* (BestMixer.io,2020), el servicio de mezcla funcionaba de la siguiente manera:

1. El vaso de monedas rompe la conexión entre las direcciones de envío y recepción, lo cual es necesario para el anonimato criptográfico.
2. Al hacer girar las monedas, se puede anonimizar la información sobre dónde se guardan las monedas, a dónde se envían y de dónde se reciben.
3. Al recibir las monedas, se ingresan en un grupo de monedas de otros depositantes. Luego, el motor de mezcla hace girar todas las monedas.
4. Las monedas que se reciben como resultado de la mezcla, se integran por bits de muchas fuentes diferentes, lo que codifica sus orígenes garantizando que las monedas que se reciben no se puedan rastrear.
5. Utiliza grupos formados por diversos grados de monedas anónimas para mezclar sus monedas, lo que garantiza que las monedas que recibe no se puedan rastrear.

6. La manera de defenderse contra las formas sofisticadas de análisis de *blockchain* es enviando monedas a la billetera de los clientes que se componen de fragmentos increíblemente pequeños de monedas de diferentes fuentes, codificando así el origen de sus monedas para siempre y brindándole el anonimato absoluto y libertad.
7. Para proteger la privacidad de los clientes, no almacena ninguna información sobre los mismos y tampoco solicita información de identificación.
8. Una vez cumplidas todas las condiciones de mezcla y ejecutado la orden, el historial de la orden se borra dentro de las 24 horas.
9. Para mayor seguridad del cliente, recomienda el uso de la nueva función de retardos de tiempo al mezclar, ya que, con un retraso de tiempo, es imposible que el análisis de *blockchain* detecte y rastree la transacción.

Además, en una *web* de tutoriales y guías BestMixer.io describe que para mezclar las criptomonedas, el usuario envía sus criptomonedas por la plataforma, confirma la transacción, y la dirección que asigne para que reciba las criptomonedas que le envíen, pero de una dirección totalmente distinta a la suya y que no estará relacionada con él.

Cuando el usuario envía las criptomonedas, éstas se depositan en un fondo propio de la plataforma, donde se intercambian por otras completamente distintas, ésta asigna la o las direcciones receptoras, donde *BestMixe*r permite enviar hasta 10 direcciones diferentes desde un depósito único. Entre más direcciones receptoras, mayor anonimato, esto implica una pequeña comisión extra por cada nueva dirección.

Cuenta con tres reservas para mezclar, donde se puede seleccionar entre los 3 tipos diferentes de fondos:

- Alpha: fondos con la comisión más baja; pertenecen a los activos de otros clientes dentro de la plataforma de *BestMixer.*
- Beta: están los fondos que provienen de las grandes transacciones de fondos. Estos poseen una comisión intermedia, y
- Gamma: Estos provienen de los fondos privados y criptomonedas de inversores. Son fondos Premium con la más alta comisión.

Así pues, al elegir un fondo con mayor comisión, estamos eligiendo criptomonedas menos rastreables. Por lo tanto, el elegir la reserva, solo dependerá del nivel de anonimato que deseamos.

Después, se reparte el porcentaje que recibirá cada una de las direcciones receptoras y finalmente, está el retardo de transferencia para garantizar un buen anonimato en cada depósito, *BestMixer* fija periodos distintos a cada uno de ellos; esto para el caso de múltiples depósitos.

También, para protegerse de los análisis de *blockchain*, envía a las billeteras de sus clientes, las monedas compuestas de fragmentos extraordinariamente pequeños de monedas de diferentes fuentes, codificando así el origen de sus monedas.

La incautación de *Bestmier* es un ejemplo de cómo está aumentando en las actividades para aplicar la Ley en servicios puros de cripto a cripto. (Higgins, 2019).

Discusión del caso: El caso de BestMixer.io (mezclador centralizado), proveedor de servicios de mezcla de criptomonedas líder, que operaba en Luxemburgo y ofrecía sus servicios de mezcla en todo el mundo, mezclaba varias criptomonedas como *bitcoin*, *litecoin* y *bitcoincash*, entre otras. Su servicio ofrecía garantizar tanto el anonimato de las transacciones como la privacidad de los usuarios, al no tener ningún registro de solicitud de servicio o datos personales; sin embargo, al poco tiempo de empezar a operar, empezó a ser investigada por la policía, recabando información sobre interacciones, direcciones IP, detalles de transacciones, direcciones *bitcoin*, así como mensajes de chat hasta que fue confiscada por las autoridades de la UE.

Este caso es muy interesante, considerando que uno de los investigadores que participó en el caso, explica de una manera fácil y concreta, que mezclar las criptomonedas, “es dividir la criptomoneda en cientos de pequeñas transacciones que se pierden en transacciones de otras fuentes”. Con esto, se rompe el vínculo que hay entre las direcciones de envío y recepción. Lo cual, se logra al momento ingresar las monedas de un usuario con las de otros depositantes en un vaso y el motor de mezcla hace girar todas las monedas y, las monedas que se reciben, se integran por bits de muchas fuentes diferentes, codificando su origen, asegurando que las monedas que se reciben no se puedan rastrear. También, para proteges de los análisis de *blockchain*, envía a las billeteras de sus clientes, las monedas compuestas de fragmentos extraordinariamente pequeños de monedas de diferentes fuentes, codificando así el origen de sus monedas.

Retomando el apartado de Técnicas y herramientas para conservar el anonimato de las criptomonedas, podemos decir que el mezclador BestMixer.io, se utilizó como herramienta *CoinSwap,* al fungir como un tercero que entra a las transacciones para que las direcciones del remitente y del receptor no puedan ser identificadas.

Y por otro lado, tomando en cuenta que la característica de inmutabilidad de la tecnología *blockchain*, refiere a que una vez que se incluye algo en la cadena de bloques no se puede alterar, sólo se permite añadir transacciones, mediante una función hash criptográfica, con efecto avalancha para hacerla segura y, la característica de seguridad de *blockchain*, donde la criptografía garantiza la seguridad mediante el uso de dos llaves, una pública y una privada, así que para transferir *bitcoins* de una dirección a otra, la transacción debe firmarse con la llave privada.

Con este caso podemos decir que la herramienta *CoinSwap* aprovecha las características propias del funcionamiento y protocolo de las transacciones para realizar la mezcla de criptomonedas cuando los usuarios depositan las monedas en un vaso para que el motor de mezcla gire las monedas de todos los depositantes, y las monedas que se reciban de los usuarios, se integre por bits de muchas fuentes diferentes, pero no altera el registro de transacciones ya hechas, más bien, divide las criptomonedas en cientos de transacciones nuevas, por lo tanto no se estaría vulnerando la inmutabilidad ni la seguridad de la tecnología *blockchain* se rechaza la Hipótesis 1.

4.1.3 Bitcoin Fog.

Bitcoin Fog, fundada en 2011, administrada por Roman Sterlingov, ofreció servicios de mezcla durante una década, para ocultar las transacciones de *bitcoin* (la fuente y el destino de la criptomoneda) de sus clientes, permitiéndole a los usuarios mezclar sus transacciones con las de otros para así evitar que cualquiera que revisara la cadena de bloques de *Bitcoin* pudiera rastrear los pagos de cualquier individuo, lo que la convierte en una de las instituciones más venerables en la economía de la *web* oscura. Lavaba dinero para varias plataformas de *darknet* y lo llaman el "servicio de lavado de dinero de *bitcoin* de más larga duración en la *darkne*t" como *Silk Road, Silk Road 2.0, AlphaBay, Agora y Evolution Market*, entre otras; de hecho, las autoridades que investigaron el caso, reportaron que de los $ 336 millones de lavado identificados, por lo menos, $ 78 millones pasaron a través del servicio a varios mercados de la *web* oscura que venden narcóticos como *Silk Road, Agora y AlphaBay* en los años siguientes. (De, 2021; Haig, 2021; Greenber, 2021).

La forma en que las autoridades (IRS) rastrearon a Sterlingov fue haciendo uso del mismo análisis de *blockchain* que el propio servicio de *Bitocin Fog* estaba consignado a vencer. Parece ser que las transacciones que Sterlingov usó en el año de 2011 para configurar el alojamiento del servidor de *Bitcoin Fog* son las que pusieron al *Internal Revenue Service* (IRS) en su camino. Esto se dio gracias a que *Blockchain* continúa mostrando la evidencia que identifica la compra de moneda de *Liberty Reserve* (casa de cambio) que hizo Sterlingov con *bitcoins*, y se pudo ver que primero intercambió euros por los *bitcoins* en el primer intercambio de criptomonedas *Mt. Gox,* luego movió esos *bitcoins* a través de varias direcciones posteriores y finalmente los intercambió en otro intercambio de divisas por los fondos de *Liberty Reserve* que usaría para configurar el dominio de *Bitcoin Fog. (*Greenber, 2021).

Posteriormente, se identificaron las cuentas de Mt. Gox que usaban la dirección y el número de teléfono de Sterlingov, así como una cuenta de Google que incluía un documento en ruso en su Google Drive con instructivo para ocultar los pagos de *Bitcoin* que supuestamente utilizó para comprar los fondos de *Liberty Reserve.*

Ahora bien, tanto el análisis de las transacciones de *bitcoin*, de los registros financieros y registros de los proveedores de servicios de Internet, como del correo electrónico, y demás información, por parte de los investigadores, fue posible que pudieran identificar a Roman Sterlingov, como el

principal operador de *Bitcoin Fog*. Y lo más interesante es que la información que les sirvió de apoyó en el desarrollo de la investigación, provenía de datos históricos de años atrás que el gobierno de los Estados Unidos tiene sobre los usuarios en las plataformas BTC-e, Mt. Gox y Liberty Reserve.

Así pues (Greenber, 2021), menciona que el libro de contabilidad de la cadena de bloques de las transacciones de *Bitcoin* desde los inicios de la criptomoneda frecuentemente ha servido como un medio para que las autoridades rastreen las transacciones de hace años. Y refiere que el análisis de la cadena de bloques muestra que tan atrás en el tiempo pueden llegar los investigadores con esas técnicas de "seguimiento del dinero", según lo expres Sarah Meiklejohn (científica informática del University College of London) cuyo trabajo fue pionero en las técnicas de rastreo de *Bitcoin* en 2013.

También, como parte de la investigación, un agente encubierto del IRS envió una pequeña cantidad de *bitcoin* de una billetera a otra, y a los investigadores no les fue posible rastrear ningún vínculo directo entre las dos billeteras, demostrando así que el servicio de mezcla se utilizaba para perturbar las transferencias, y validaron que la plataforma no estaba realizando verificación alguna sobre el conocimiento de sus clientes.

Cabe destacar que *Liberty Reserve* (casa de cambio mundial con sede en Costa Rica, hoy confiscada), permitía a sus clientes abrir cuentas y mover dinero anónimamente utilizando su moneda virtual. Durante el periodo de 2006 a 2013, fue "la opción bancaria para el mundo criminal" y los fiscales la refieren como la mayor operación de lavado de dinero en línea en la historia, utilizando el intercambio digital financiero como método eficiente para lavar dinero, sirviendo a piratas informáticos, ladrones de identidad y personas involucradas en la pornografía infantil y el narcotráfico, de acuerdo a una acusación federal de Estados Unidos.

Discusión del caso: *El caso de Bitcoin Fog, conocido como Bitcoin* niebla, es un caso que nos muestra, por un lado, cómo operaba la empresa para ofrecer sus servicios, era una empresa de servicios monetarios estadounidense que también se dedicó al servicio de mezcla y que operó sin licencia ante FinCen. Mezclaba los fondos que le enviaban los usuarios con los fondos transferidos de otros usuarios para evitar que el análisis a la cadena de bloques de *Bitcoin* pudiera rastrear sus pagos. El servicio se realizaba a través de su billetera digital, a la cual sólo se podía acceder desde una red oscura *(TOR),* donde la gran mayoría de las criptomonedas que mezclaban, venían de mercados (plataformas) de la red oscura y estaba vinculada a narcóticos ilegales, actividades de fraude, abuso informático, además de robo de identidad. A parte, su plataforma no estaba realizando la debida diligencia y verificación sobre la identificación y conocimiento de sus clientes.

Lo anterior demuestra que no se vulnera la seguridad e inmutabilidad del sistema *blockchain* para conservar el anonimato en las transacciones con *bitcoin* para lavar dinero. Por tanto, se rechaza la Hipótesis 1.

Por otro lado, nos muestra cómo es que las autoridades pudieron vincular a Roman Sterlingov (CO de *Bitcoin* FOG) con la plataforma *Bitcoin Fog,* mediante el análisis de *blockchain*, aprovechando la característica de transparencia de la tecnología *blockchein* que a través una dirección pública se mostrará el historial de transacciones, y los beneficios de integridad y trazabilidad que ofrece, ya que, al ser inmutable, tiene toda la trazabilidad completa de lo que ha pasado, y una vez que se registra una transacción, se guarda y ya no se puede borrar, lo que es bueno para auditores e investigadores, ya que es imposible falsear.

Estas características y beneficios de la tecnología *blockchain*, exhibió la trazabilidad de todos los movimientos que realizó Roman Sterlingov, desde el análisis de sus transacciones de *bitcoin*, de los registros financieros y los registros de los proveedores de servicios de Internet, hasta de su correo electrónico, y demás información, pudiendo identificar la compra de monedas en las casas de cambio Liberty Reserve y Mt. Gox, así como el movimiento de *bitcoins* a través de varias direcciones y su posterior intercambio de divisas por los fondos de Liberty Reserve, mismas que utilizó para configurar el dominio de *Bitcoin* Fog. Partiendo de Información que venían de datos históricos de años atrás que el gobierno de los Estados Unidos tiene sobre los usuarios en las plataformas BTC-e, Mt. Gox y Liberty Reserve.

Así entonces, la identificación de Roman Sterlingov como administrador de *Bitcoin* Fog, y su arresto, dejó evidencia de cómo sí es posible que los auditores e investigadores con recursos, herramientas y capacidad técnica adecuada pueden beneficiarse de la trazabilidad y transparencia de la criptomoneda y con un análisis de la cadena de bloques pueden rastrear los flujos de fondos provenientes de actividades ilícitas y que a pesar de que se creía que *Bitcoin* era una poderosísima herramienta para realizar transacciones anónimas, imposibles de rastrear, para lavar dinero, al final ha resultado ser todo lo contrario. Es decir, “Un mito”.

4.1.4 BTC-e.

Mercado en línea para compradores y vendedores de *bitcoins* y otras criptomonedas, fundada en 2011 y dirigida y supervisada por Alexander Vinnik en su operación y finanzas de 2011 a 2017, fue uno de los intercambios de divisas digitales más grandes y utilizados del mundo, que operó como negocio de servicios monetarios sin el registro en el Departamento del Tesoro de los Estados Unidos, por lo tanto, no contaba con un programa antilavado de dinero, ni con un sistema para la verificación de "conozca a su cliente conforme a la Ley federal, y la emisión de reportes. (Eckel, 2019).

De acuerdo a funcionarios estadounidenses y de otros países, el modelo de negocio de *BTC-e* dependía en gran medida de la delincuencia criminal, así como de personas y entidades interesadas en el anonimato o las transacciones difíciles de rastrear. (Eckel, 2019).

BTC-e, facilitó varios delitos que van mucho más allá de la falta de regulación del intercambio de *bitcoins* que operaba. También robó identidades, facilitó el tráfico de drogas y ayudó a lavar ganancias criminales de sindicatos y recibió las ganancias criminales de numerosas intrusiones

informáticas e incidentes de piratería, estafas de *ransomware*, esquemas de robo de identidad, funcionarios públicos corruptos y redes de distribución de narcóticos. Al parecer, tiene una base de operaciones en las Islas Seychelles y sus dominios *web* se encuentran registrados a empresas fantasma, en Singapur, las Islas Vírgenes Británicas, Francia y Nueva Zelanda, por mencionar algunos. Vinnik desarrolló una base de clientes para *BTC-e* que dependía en gran medida de los delincuentes, incluso no les exigía a los usuarios que validaran su identidad, ocultaba y anonimizaba las transacciones y la fuente de fondos. (Departamento de Justicia de Estados Unidos, 2017).

Compradores y vendedores del mercado de drogas en el sitio llamado *Hydra* dentro de la *darknet*, utilizaron *Binance* para realizar pagos en criptomonedas.

A partir de febrero de 2015 manejó alrededor del 3% de todo el volumen de intercambio de *bitcoin*. Hasta el 25 de julio de 2017, permitía el comercio entre el dólar estadounidense, el rublo ruso y las monedas de euro, y las criptomonedas *bitcoin*, *Litecoin, Namecoin, Novacoin*, *Peercoin, Dash y Ethereum*. Fue un componente del Índice de Precios de *Bitcoin* de *CoinDesk* desde la formación del índice en septiembre de 2013. Comercializó al menos $ 4 mil millones en *bitcoins* con "altos niveles de anonimato". (Eckel, 2019; CipherTrace 2021).

Un investigador que rastrea las transacciones de *blockchain*, estimó que a partir de 2016 hasta el 70 % de todos los casos criminales de criptomonedas a nivel mundial involucraron a *BTC-e*. (Del Rey, 2013).

El 25 de julio de 2017, Vinnik fue arrestado en Grecia a pedido de los EE. UU. Bajo sospecha de lavar $ 4 mil millones a través de *BTC-e*., y los fiscales estadounidenses presentaron otra denuncia contra Vinnik y BTC-e, y se movieron para incautar alrededor de $ 100 millones de cuentas congeladas de BTC-e por presuntas violaciones de las leyes bancarias de los Estados Unidos y el 28 de julio del mismo año, las autoridades estadounidenses incautaron el nombre de dominio *BTC-e*.com y el 38% de todos los fondos de los clientes. (Departamento de Justicia de Estados Unidos, 2017).

El agente especial *Hess* a cargo del FBI, expresó que la investigación de Alexander Vinnik fue altamente compleja, y su arresto fue el resultado de un esfuerzo multinacional, también muestra los beneficios de la cooperación global entre las fuerzas del orden estadounidenses e internacionales y el compromiso para identificar y perseguir a los delincuentes en todo el mundo. (Departamento de Justicia de Estados Unidos, 2017).

Discusión del caso: *Este caso* nos muestra que la como la empresa de servicios monetarios de Intercambio *BTC-e,* brindó sus servicios para disfrazar u ocultar los recursos provenientes de una actividad ilícita para anonimizar la relación entre remitentes y destinatarios de transacciones dentro del sistema *Bitcoin*, la cual también operó incumpliendo la regulación de la SBA al no contar con un registro y autorización por parte del Departamento del Tesoro de los Estados

Unidos, con un programa de antilavado de dinero, con un sistema de verificación de “conozca a su cliente”, ni tampoco para la emisión de reportes, puesto que su negocio dependía de recursos proveniente de actividades ilícitas, facilitando el tráfico de drogas y el lavado de ganancias criminales de sindicatos, funcionarios públicos corruptos y redes de distribución de narcóticos, de incidentes de piratería, estafas de ransomware, esquemas de robo de identidad.

Con este caso, por un lado, se confirma lo señalado por (Serrano, 2020) sobre el uso potencial de cambiadores de monedas virtuales que no tienen licencia o no están registrados para ocultar los recursos de procedencia ilícita, y por el otro, para identificar y perseguir un delito o algún delincuente, no basta solamente aprovechar las característica de transparencia y los beneficios integridad y trazabilidad de la tecnología *blockchein* y un buen análisis de *blockchain*, y el uso de quipos y herramientas, también es importante una sinergia multinacional, y cooperación global entre las fuerzas del orden propios de cada gobierno e internacionalmente y el compromiso para identificar y perseguir a los delincuentes en todo el mundo.

Con este caso se comprueba que no se vulnera la seguridad e inmutabilidad del sistema *blockchain* para conservar el anonimato en las transacciones con *bitcoin* para lavar dinero. Por tanto, se rechaza la Hipótesis 1.

4.1.5 Binance.

Binance, plataforma de intercambio de origen chino, con las criptomonedas más populares a escala global para comerciar más de 100 activos digitales. En 2017 trasladó su sede y servicios a Japón por la prohibición del comercio de criptomonedas por parte del gobierno chino. Abrió una oficina en Malta y Singapur, está incorporada en las Islas Caimán. No cuenta con una sede corporativa.

Desde 2018, se ha considerado como la plataforma de intercambio con mayor volumen comercial en el mundo. Es la más grande y permite hacer más cosas con *bitcoin*, ofrece futuros, compra/venta de criptomonedas, una tarjeta de débito, NFT, *stacking* para Ethereum 2.0, mercados y trading entre otras. (Solé, 2021).

La compra de criptomonedas se puede hacer mediante tarjetas de débito, intercambio P2P o pago de terceros (empresas que están asociadas con *Binance* como *Simplex, Koinal,* TrustToen y Paxo**).** Ofrece un servicio de mercado simplificado para usuarios principiantes y para quienes cuentan mayor conocimiento de trading.

En enero 2018, su token (BNB) llegó a una capitalización de mercado de USD 1.3 mil millones. (Schoenberg, 2021).

En la actualidad, la plataforma tiene más de 13,5 millones de usuarios y compite con Coinbase, la primera empresa de criptomonedas en cotizar en el índice Nasdaq. (El Cronista, 2021)

Cuenta con la plataforma *Binance DEX*, que es una plataforma de intercambio que opera dentro de una *blockchain* y que no almacena los fondos ni datos personales de los usuarios en sus servidores.

Su plataforma *Binance Lab*, es una rama del intercambiador que apoyan a proyectos y empresas jóvenes en fase inicial de creación y construcción que están enfocadas en el segmento de las criptomonedas. Cuenta con presencia en África, América Latina y Europa.

Changpeng Zhao, (fundador y CEO de *Binance*) informa que *Binance* sigue de cerca las reglas de Estados Unidos, que bloquea a los estadounidenses de su sitio *web* y utiliza tecnología avanzada para analizar las transacciones y detectar indicios de lavado de dinero y otras actividades ilícitas. (Schoenberg, 2021).

Actualmente está siendo investigado por el Departamento de Justicia y el Servicio de Impuestos Internos de Estados Unidos, debido a que en los últimos cinco años, *Binance* ha procesado por lo menos USD 2.350 millones en transacciones de criptomonedas procedentes de *hackeos*, fraudes de inversión y ventas ilegales de drogas**.** La investigación de acuerdo a la agencia internacional de noticias Reuters esta cifra surge a partir de registros judiciales, declaraciones de la policía y datos de *blockchain*, que se recopilaron a través de dos exploradores que fueron respaldados por expertos en el sector. (Schoenberg, 2021).

De acuerdo a una investigación periodística de *Reuters*, por el periodo de 2017 a 2022, los compradores y vendedores del mercado de drogas en el sitio llamado *Hydra* dentro de la *darknet*, utilizaron *Binance* para realizar pagos en criptomonedas por un importe de USD 780 millones datos obtenidos de la firma de análisis Crystal *Blockchain* y otra anónima. Además, en 2019, una usuaria de Moscú, compró mefedrona y ketamina en el sitio *Hydra*. Los pagos los realizó a través de *Binance* mediante un nombre de pila**.** El anonimato del sistema hizo posible la compra de medicamentos en la red oscura. (Infobae, 2022).

Chainalysis Inc.[22](firma forense de *blockchain* que incluye entre sus clientes a las agencias federales de Estados Unidos), determinó que, en 2020, entre las transacciones que examinó, los fondos vinculados a actividades delictivas que fluían a través de *Binance*, eran más que cualquier otro intercambio de cifrado.

Las investigaciones persiguen un informe de *Chainalysis* sobre transacciones criminales. Esta firma rastreó *bitcoins* por un valor de $ 2.8 mil millones que sospecha que corresponden a delincuentes y determinó que aproximadamente el 27%, o $ 756 millones, terminaron en *Binance*. (Schoenberg, 2021).

[22] ***Chainalysis***. Compañía internacional líder en materia de análisis de la tecnología *blockchain* a nivel global utiliza el análisis de la cadena de bloques para cuantificar diferencias y reforzar sus datos, hallazgos e información con conocimientos de expertos de la industria de todo el mundo.

Discusión del caso: *El caso de Binance*, nos muestra que a pesar de ser una empresa exitosa de servicios monetarios registrada y autorizada para operar como intercambio que actualmente ocupa uno de los primeros lugares en mercado por su volumen de transacciones y otros servicios que ofrece con *bitcoin*; con una solides y reputación que le permite tener su propio *token* (BNB), además de que apoya a proyectos y empresas jóvenes enfocadas en el segmento de las criptomonedas, con una presencia en África, América Latina y Europa, manifestando que opera con apego a la regulación de Estados Unidos, que cuenta con un programa de antilavado de dinero con un procedimiento para identificar a sus clientes y el uso de tecnología avanzada para analizar las transacciones y detectar indicios de lavado de dinero y otras actividades ilícitas.

Resulta que, dentro de su página *web*, cuenta con una plataforma de intercambio llamada *Binance DEX* que opera dentro de una *blockchain*, la cual no almacena los fondos ni datos personales de los usuarios en sus servidores. Y está siendo investigada por procesar en transacciones de criptomonedas que provienen de *hackeos*, fraudes de inversión y ventas ilegales de drogas**,** además de que ha facilitado el pago en criptomonedas a compradores y vendedores del mercado de drogas en el sitio llamado *Hydra* dentro de la *darknet*.

Este caso es una evidencia más de que no se vulnera la seguridad e inmutabilidad del sistema *blockchain* para conservar el anonimato en las transacciones con *bitcoin* para lavar dinero y mediante el análisis de transacciones, una firma forence de *blockchain* pudo identificar fondos vinculados a actividades delictivas. Por tanto, se rechaza la Hipótesis 1.

4.2 Casos de delincuentes (narcotraficantes) en México

4.2.1 Cárteles del crimen.

Informe de autoridades estadounidenses y mexicanas sobre Cártel de Jalisco Nueva Generación y Cártel de Sinaloa.

Las autoridades estadounidenses y mexicanas comentan que las bandas de narcotraficantes como el Cártel Jalisco Nueva Generación (CJNG) y el Cartel de Sinaloa están aumentando el uso de *bitcoin* para lavar dinero, según las autoridades de México y los Estados Unidos. Se cree que, solamente en México, los cárteles mexicanos blanquean unos 25.000 millones de dólares al año. (ONU, 2022).

Oré (2020), refiere que el desplome en las incautaciones de divisas, de $ 741 millones en 2011 a $ 234 millones en 2018, supone que se debe al incremento de las nuevas tecnologías, incluyendo el lavado de criptomonedas, provenientes principalmente de carteles colombianos y mexicanos, de acuerdo al informe de la Agencia Antidrogas de los Estados Unidos (DEA) publicado en enero de 2020.

Además, menciona que alrededor del 98% de todas las transacciones de México por encima del umbral de los 56,000 pesos en 2020 fueron identificadas por una plataforma criptográfica registrada, en Jalisco, estado natal del cártel del CJNG, de acuerdo a datos del gobierno mexicano, vistos por Reuters (Agencia de Noticias, principalmente financieras, con sede en el Reino Unido).

Para no superar el umbral de las operaciones bancarias que hacen saltar las alarmas, que es de 7.500 dólares, los delincuentes generalmente dividen su efectivo ilícito en pequeñas cantidades y los depositan en varias cuentas bancarias, técnica conocida como "pitufo", y luego usan esas cuentas para comprar una serie de pequeñas cantidades de *bitcoin* en línea, oscureciendo así, el origen del dinero y permitiéndoles pagar a los asociados en otras partes del mundo.

Tanto las Organizaciones Criminales Transnacionales (TCO) mexicanas como las colombianas están incrementando el uso de la moneda virtual debido su anonimato y la velocidad de las transacciones. Se dice que el uso de la moneda virtual va en aumento con cara al futuro.

Discusión del caso: Las autoridades estadounidenses y mexicanas reportan que las bandas de narcotraficantes como el Cártel Jalisco Nueva Generación (CJNG) y el Cartel de Sinaloa están aumentando el uso de las criptomonedas (*bitcoin*), al considerar que la mayor parte de todas las transacciones de México que están por encima del umbral de los 56,000 pesos, en 2020, fueron identificadas por plataforma criptográfica con registro en el estado de CJNG, Jalisco, además del descenso de las incautaciones de divisas que se ha presentado en el periodo de 2011 ($741 millones) a 2018 (234 millones), que se presenta como un reflejo del terreno que está ganando las nuevas tecnologías, en particular, el lavado de criptomonedas.

El aumento del uso de las monedas virtuales por las Organizaciones Criminales Transnacionales (TCO), tanto mexicanas como colombianas, se debe por su anonimato y la velocidad de las transacciones. Se piensa que el uso de etas monedas va en aumento con cara al futuro. También, utilizan la técnica conocida como "pitufo", que consiste en dividir su efectivo ilícito en pequeñas cantidades y los depositan en varias cuentas bancarias, y después usan esas cuentas para comprar una serie de pequeñas cantidades de *bitcoin* en línea, oscureciendo así, el origen del dinero.

Al señalarse el uso de la técnica "pitufo", que no es más que dividir su efectivo ilícito en pequeñas cantidades y depositarlas en varias cuentas bancarias, para después usar esas cuentas para comprar pequeñas cantidades de *bitcoin* en línea; y como ya se dijo anteriormente, que el intercambio de monedas virtuales a moneda fiduciaria u otra moneda virtual no vulnera la seguridad e inmutabilidad del sistema *blockchain*. Entonces, se rechaza la Hipótesis H1. “Se vulnera la seguridad e inmutabilidad del sistema *blockchain* mediante la mezcla o el intercambio de las criptomonedas para conservar el anonimato en las transacciones con *bitcoin* para lavar dinero.”

4.2.2 Caso Ignacio Santoyo.

El caso de Ignacio Santoyo (presunto traficante de personas), muestra que entre mayo y noviembre de 2018, Santoyo y su hermana adquirieron unos $ 441,000 pesos (22.260 dólares) en *bitcoin* en Bitso, que es una plataforma de negociación en México y Argentina; sin embargo, fue hasta abril de 2019, cuando la policía mexicana arrestó a Ignacio Santoyo en Playa del Carmen después de vincularlo con una red de prostitución que se extendía por toda América Latina. Fue arrestado después de haber comprado *bitcoins*. Al realizar sus transacciones a través de una plataforma registrada, Santoyo brindó sus datos personales incluyendo su número de teléfono y dirección. Su arresto representó un éxito para la nueva Ley en México, la cual requiere que todas las plataformas de comercio de criptomonedas registradas informen transferencias superiores a 56,000 pesos ($ 2,830), así como también, conocer a su cliente (Oré, 2020).

4.2.3 Caso Héctor Ortiz.

El caso de Héctor Ortiz, muestra que, en mayo de 2019, la detención del supuesto líder de la pandilla Héctor Ortiz en el estado de Guanajuato, se llevó a cabo, después de gastar "decenas de miles de dólares" en *bitcoin*, y activar el sensor de umbral de *bitcoin* y permitir a los investigadores seguirlo a través de su teléfono. (Oré, 2020).

Su arresto y el de Ignacio Santoyo fueron el resultado de la aplicación de la legislación de México, diseñada para rastrear las transacciones ilícitas de criptomonedas. Según Reuters, “las plataformas que comercian criptodivisas registradas en México, tienen la obligación de informar de las transferencias superiores a 2.830 dólares, lo que actualmente equivale a alrededor de 0,20 *Bitcoin*”. Así pues, las transacciones marcadas llevaron a estos arrestos. (Chipolina, 2020).

4.2.4 Caso Zaragoza.

El caso de Rodrigo Zaragoza reportado por la UIF, muestra la participación de una familia entera, de una plataforma clandestina de intercambio de AV (activos virtuales) y de la operadora financiera del grupo como parte de una estrategia para lavar dinero, provenientes del narcotráfico, la delincuencia organizada y la defraudación fiscal y describe la forma en que operaron para cometer el delito de lavado de dinero. El monto, así como el origen y destino de los recursos, y las operaciones relacionadas con criptomonedas, provocó que el sistema financiero activara sus alarmas. Aproximadamente entre julio del 2020 a mayo del 2021, Rodrigo Z. compró *bitcoin* por una cantidad equivalente a 9.1 millones de pesos**.** A partir de esto, empezó el rastreo de la ruta del dinero. (Gutiérrez, 2021).

Los miembros de la familia recibían depósitos en efectivo en distintos lugares del país, particularmente en Jalisco y Michoacán, donde el crimen organizado tiene mayor presencia, después triangularon los recursos entre sí, por medio de una serie de operaciones. Luego se estratificaron para comprar criptomonedas principalmente en *CT OPTION TRADING* (con su aplicación móvil *Citiwallet*), plataforma clandestina que no tiene el registro ante el Servicio de

Administración Tributaria ni ante ninguna autoridad, para prestar este tipo de servicios. Después, la familia Zaragoza, así como la plataforma de intercambio, estuvieron transfiriendo y recibiendo grandes cantidades de dinero desde y hacia el extranjero como fue a los Emiratos Árabes, uno de los países con mayor riesgo por sus actividades financieras, económicas, corporativas y comerciales. Finalmente, los recursos regresaron a sus beneficiarios finales, para concretar la triangulación de recursos.

Por lo que se refiere a Andrea Z., se le encontraron depósitos en efectivo millonarios, por casi 1.9 millones de pesos**,** además de recursos que provenían de CT O, Rodrigo Z. y de algunas empresas reportadas por desvío de dinero. (Gutiérrez, 2021).

También se encontraron operaciones que estaban relacionadas con Guadalupe Z. (la tía) identificando entre el 2019 y el 2020 realizó depósitos en efectivo por 2.7 millones de pesos y, entre noviembre del 2019 a abril del 2020, hizo depósitos por un monto de 28 millones de pesos, mismos que se enviaron a Rodrigo Z y la firma CT O. (Gutiérrez, 2021).

Además, se detectaron movimientos de Andrea Z. (prima), Víctor Z. (primo) y Carlos Z. (familiar), relacionados con *CT O* y otras empresas que la autoridad mexicana considera fachada, que tienen relación con criptomonedas.

En los registros financieros de *CT O*, se muestran transferencias por 1.9 millones de dólares a Estados Unidos y de 960,000 dólares a Emiratos Árabes, realizadas en noviembre del 2019**.** Y durante el periodo de diciembre 2020 y abril 2021, estuvo recibiendo cantidades por un total de 2.9 millones de dólares provenientes de la nación emiratí**.** (Gutiérrez, 2021).

De acuerdo al conteo completo de la UIF, la red de movimientos arrojó un saldo de 66 millones de pesos transaccionados**,** además de que se identificaron operaciones relacionadas con fraude, crimen organizado y con la firma CT O. (Gutiérrez, 2021).

Es de gran relevancia señalar el gran movimiento internacional de operaciones en efectivo que realizó esta organización, utilizando de manera conjunta a instituciones bancarias y una plataforma de activos virtuales para comprar *bitcoin*. Se gastaron más de 9 millones de pesos en compra de *bitcoins* y se identificaron más de 30 movimientos por cantidades millonarias en pesos y en dólares, realizándose la mayor parte durante el periodo de 2019 a 2021, utilizando diferentes mecanismos del sistema financiero formal, como transferencias vía el Sistema de Pagos Electrónicos Interbancarios, así como movimientos en plataformas dedicadas a la operación de criptomonedas.

Al respecto, la Unidad de la Secretaría de Hacienda presentó una denuncia en contra del principal operador de la familia Zaragoza, así como de familiares en tercer y cuarto grado de parentesco, el socio fundador de la plataforma clandestina, la operadora financiera del grupo, y otros; por los hechos de que resultan posiblemente constitutivos de delito, relacionados con operaciones con

recursos de procedencia ilícita, delincuencia organizada, narcotráfico y defraudación fiscal", señaló la UIF.

Discusión de casos Ignacio Santoyo, Héctor Ortiz y Zaragoza: Como se puede observar, en México la UIF proporciona información muy general sobre los casos detectados de lavado de dinero con criptomonedas. Aun así, se puede ver *cómo va en aumento y ganando terreno el uso de criptomonedas (bitcoin)* para lavar dinero, por su anonimato y la velocidad de las transaccionales, ejemplo de ello, son el 98% de las transacciones de México, que estaban por encima del umbral de los 56,000 pesos, que fueron identificadas por una plataforma criptográfica registrada, en el estado de Jalisco.

También se presentan algunas técnicas y mecanismos utilizadas por estas bandas criminales para lavar dinero mediante el uso de *bitcoin* como la famosa técnica "pitufo", que consiste en dividir el efectivo ilícito en pequeñas cantidades y depositarlas en varias cuentas bancarias, y después usar esas cuentas para comprar una serie de pequeñas cantidades de *bitcoin* en línea, oscureciendo así, el origen del dinero (ONU, 2022). Por su parte, el caso de Zaragoza, muestra la participación de una familia en conjunto con una plataforma clandestina de intercambio activos virtuales y una operadora financiera para mover cantidades millonarias en efectivo, mediante la triangulación de recursos, compra de *bitcoins* y transfiriendo y recibiendo recursos hacia y del extranjero.

Además de lo anterior, estos casos muestran el éxito que ha representado la nueva Ley en México (LFPIORPI), la cual requiere que todas las plataformas de comercio de criptomonedas registradas informen transferencias superiores al umbral de 56,000 pesos ($ 2,830), así como también, identificar y conocer a sus clientes.

Por último, con los casos de Ignacio Santoyo y Héctor Ortíz, al referir solamente, que fueron identificados por haber rebasado los umbrales en sus transacciones (compra y gastos) con *bitcoin* en una plataforma registrada y haber proporcionado sus datos personales y que muestran el éxito que ha representado la nueva Ley en México (LFPIORPI). Al señalarse el uso de plataformas de intercambio registradas; como hemos mencionado, con el intercambio de monedas virtuales a moneda fiduciaria u otra moneda virtual no se vulnera la seguridad e inmutabilidad del sistema *blockchain*. Por tanto, se rechaza la Hipótesis H1. “Se vulnera la seguridad e inmutabilidad del sistema *blockchain* mediante la mezcla o el intercambio de las criptomonedas para conservar el anonimato en las transacciones con *bitcoin* para lavar dinero.”

El caso de Zaragoza, al señalar el uso de una plataforma clandestina de intercambio activos virtuales, al respecto, el intercambio de monedas virtuales a moneda fiduciaria u otra moneda virtual no se vulnera la seguridad e inmutabilidad del sistema *blockchain*. Por tanto, se rechaza la Hipótesis H1. “Se vulnera la seguridad e inmutabilidad del sistema *blockchain* mediante la mezcla o el intercambio de las criptomonedas para conservar el anonimato en las transacciones con *bitcoin* para lavar dinero.”

Y por lo que se refiere al uso de una operadora financiera para mover cantidades millonarias en efectivo, mediante la triangulación de recursos, compra de *bitcoins* y transfiriendo y recibiendo recursos hacia y del extranjero, no es posible confirmar o rechazar la Hipótesis **H1.** “Se vulnera la seguridad e inmutabilidad del sistema *blockchain* mediante la mezcla o el intercambio de las criptomonedas para conservar el anonimato en las transacciones con *bitcoin* para lavar dinero.”

En el Anexo I, se presenta un cuadro resumen de los casos de estudio.

Después de haber analizado todos los casos, a continuación, se presenta un cuadro con un resumen sobre el cumplimiento de la Hipótesis 1:

Cuadro 4.1

Resumen de Resultados del Estudio de Casos de Empresas Prestadoras de Servicios Internacionales de Activos Virtuales

	Caso	Empresa Prestadora de Servicio (Modelo de negocio)	Técnica para lavar dinero	Herramienta	Cumplimiento Hipótesis H1
1	Helix y Coin Ninja	Intercambiador de monedas virtuales convertibles. y Mezclador de bitcoin través de transacciones de CoinJoin.	Intercambio y Mezcla con CoinJoin	Para Mezclar: 1. Herramienta de privacidad *(Bitcoin Mixer Helix*). 2. Motor de búsqueda de la *darknet.* 3. Grams, para realizar transacciones en *AlphaBay* , un mercado negro en la red oscura.	Con el intercambio de monedas virtuales a moneda fiduciaria u otra moneda virtual y con la técnica Coin Join, para mezclar fondos no se vulnera la seguridad e inmutabilidad del sistema *blockchain,* por lo tanto, **se rechaza la Hipótesis H1.**
2	BestMixer.io	Mezclador de criptomonedas líder en el mundo	Mezcla con CoinSwap	Plataforma Bestmixer.io con vaso para mezclar.	Con la técnica CoinSwap, para mezclar fondos no se vulnera la seguridad e inmutabilidad del sistema *blockchain,* por lo tanto, **se rechaza la Hipótesis H1.**
3	Bitcoin Fog	Servicio de Mezcla	Mezcla con CoinSwap	1. *Bitcoin mixer,* que consiste en ocultar la fuente de una criptomoneda licuándola con otros fondos. 2. Billetera digital. 3. Red oscura Tor. 4. Desarrolladores profesionales de aplicaciones web seguras.	Con la técnica CoinSwap, para mezclar fondos no se vulnera la seguridad e inmutabilidad del sistema *blockchain,* por lo tanto, **se rechaza la Hipótesis H1.**
4	BTC-e	Intercambio de monedas virtuales	Intercambio	Plataformas de compra y venta de terceros para poder adquirir criptomonedas.	Con el intercambio de monedas virtuales a moneda fiduciaria u otra moneda virtual no se vulnera la seguridad e inmutabilidad del sistema *blockchain,* por lo tanto, **se rechaza la Hipótesis H1.**
5	BINANCE	Intercambio de monedas virtuales	Intercambio	1.Plataforma de intercambio de criptomonedas. 2. Binance DEX plataforma de intercambio opera dentro de una *blockchain* que no almacena los fondos ni datos personales de los usuarios en sus servidores. 3. Red *blockchain* propia.	Con el intercambio de monedas virtuales a moneda fiduciaria u otra moneda virtual no se vulnera la seguridad e inmutabilidad del sistema *blockchain,* por lo tanto, **se rechaza la Hipótesis H1.**

Fuente: Elaboración propia con datos del estudio de los casos de empresas prestadoras de servicios internacionales de activos virtuales.

Cuadro 4.2

Resumen de Resultados del Estudio de Casos de Delincuentes (Narcotraficantes) en México

	Casos de México	Actividad	Técnica para lavar dinero	Herramienta	Cumplimiento Hipótesis H1
1	CJNG y Cártel de Sinaloa	Narcotraficante	Técnica conocida como "pitufo".	Plataforma de intercambio.	Con la técnica pitufo, al dividir su efectivo ilícito en pequeñas cantidades y depositarlas en varias cuentas bancarias, para después usar esas cuentas para comprar pequeñas cantidades de bitcoin en línea, no se vulnera la seguridad e inmutabilidad del sistema *blockchain,* por lo tanto, **se rechaza la Hipótesis H1.**
2	Ignacio Santoyo	Red de Prostitución	Intercambio en plataforma.	Plataforma de intercambio registrada.	Con el intercambio de monedas virtuales a moneda fiduciaria u otra moneda virtual no se vulnera la seguridad e inmutabilidad del sistema *blockchain,* por tanto**, se rechaza la Hipótesis H1.**
3	Héctor Ortiz	Narcotraficante	Intercambio en plataforma.	Plataforma de intercambio registrada.	Con el intercambio de monedas virtuales a moneda fiduciaria u otra moneda virtual no se vulnera la seguridad e inmutabilidad del sistema *blockchain,* por lo tanto, **se rechaza la Hipótesis H1.**
4	Zaragoza	Narcotraficante	Intercambio. Triangulación de recursos. Transferencias de recursos hacia y del extranjero.	Plataforma de intercambio clandestina, uso de una operadora financiera para mover cantidades millonarias en efectivo.	Con el intercambio de monedas virtuales a moneda fiduciaria u otra moneda virtual no se vulnera la seguridad e inmutabilidad del sistema *blockchain.* Por lo tanto, **se rechaza la Hipótesis H1.**

Fuente: Elaboración propia con datos del estudio de los casos de Delincuentes (Narcotraficantes) en México.

Como se puede observar, de los cinco casos de empresas de servicio internacionales de activos virtuales, las cinco rechazaron la hipótesis 1, y de los cuatro casos de delincuentes (narcotraficantes), los cuatro también rechazaron la hipótesis 1; por lo que se concluye que la Hipótesis:

H1. Se vulnera la seguridad e inmutabilidad del sistema *blockchain* mediante la mezcla o el intercambio de las criptomonedas para conservar el anonimato en las transacciones con *bitcoin* para lavar dinero, **se rechaza.**

Conclusiones

Esta investigación tuvo como objetivo identificar cómo se conserva el anonimato en las transacciones con *bitcoin*; evaluar si se vulnera *blockchain* para lavar dinero, e identificar si la "Ley *Fintech*" considera aspectos regulatorios que permitan identificar las operaciones de mezcla, transaccionalidad e intercambio en el sistema *blockchain*.

Con base en un análisis cualitativo del funcionamiento de las criptomonedas y la tecnología *blockchain*, su uso en el sistema financiero y su participación en la economía de México, se puede concluir lo siguiente:

La innovación tecnológica no sólo está modernizando nuestra forma de vivir, de trabajar o relacionamos; sino también, la economía, la industria y las finanzas, y por supuesto, a las actividades ilícitas como el lavado de dinero, a nivel global. En el área de las finanzas trajo consigo, la era de las criptomonedas como *bitcoin*.

En México, están revolucionado el sistema financiero al ser más competitivas que los servicios bancarios, al ofrecer una mayor eficiencia de pago, reducción de costos en transacción de pagos y transferencias de fondos y la eliminación de intermediarios, además de que son irreversibles, rápidas, accesibles, seguras y les permiten a las partes de una transacción un grado de anonimato mayor que los medios de pago tradicionales, (Puvogel Rojas, 2018). Lo que ha llevado a los bancos a innovar. México ocupa el puesto 44 en el mundo dentro de la lista de países con mayor adopción según la firma *Chainalysis*.

Las *Fintechs* en México, se caracterizan por ofrecer servicios de banca tradicional, como realizar pagos por Internet a diversos comercios y servicios, así como para la recepción de remesas desde el extranjero con bajas tarifas y rapidez. Y están identificando grandes oportunidades de negocio, al comercializar más de 1,000 millones de pesos en *bitcoin*s. El mercado mexicano es uno de los más importantes de Latinoamérica en casas de cambio de criptomonedas que ofrecen sus servicios a través de plataformas, para comprar y vender monedas digitales, usando *bitcoin*s como moneda de cambio o con pesos.

A pesar de que México se ha posicionado en segundo lugar como el ecosistema *Fintech* más importante de América Latina, y han traído grandes beneficios para la sociedad, también representan un riesgo emergente, aquellas ITF proveedoras de servicios con activos virtuales, al poder contar con potentes herramientas para la realización de delitos.

Las criptomonedas

Las criptomonedas como *bitcoin*, se definen como una representación digital con un sistema de pago descentralizado, que funcionan como medio de cambio o intercambio por bienes o servicios, monedas fiduciarias o virtuales, siendo su principal característica, la "tecnología *blockchain*", para su funcionamiento.

Blockchain, es una base de datos descentralizada (pública) donde se registran todas las transacciones que hacen los usuarios en cualquier criptomoneda y está formada por bloques que se encuentran encadenados. Las transacciones registradas, no se puede alterar, sólo se permite agregar transacciones. Algunos de los beneficios que ofrece son seguridad, integridad, trazabilidad, y privacidad. A través de la criptografía asimétrica, con la combinación de llaves público-privadas, protege la información. La llave pública es como un número de cuenta bancaria donde se recibe fondos y la llave privadas es una clave o PIN de una cuenta bancaria que permite usar los *bitcoins*.

Cualquiera puede usar la tecnología para ejecutar y poseer sus propias cadenas de bloques. Así, las criptomonedas *bitcoin* operan en la red *Bitcoin*, red abierta y descentralizada que opera directamente de persona a persona, sin intermediarios. En la red *Bitcoin*, los usuarios sólo se identifican con su dirección de *bitcoin* (larga cadena de números y letras), sin proporcionar algún dato personal. Por esto, las criptomonedas "*bitcoin*" brindan "cierto nivel de anonimato".

Si bien es cierto que la comercialización de las monedas virtuales convertibles por Internet, permite inversiones y transferencias anónimas, al no estar identificada la identidad del inversionista, remitente o destinatario. También es cierto que, las transacciones con *bitcoin* "no son anónimas", porque al formar parte de *blockchain*, la información financiera y las direcciones de todas las transacciones, es pública. Además, a pesar de que la relación entre las cuentas de *bitcoin* y las identidades civiles de sus propietarios es desconocida, las direcciones de *bitcoin* se pueden identificar con personas reales, aunque esto no sea muy fácil. (Möser, Böhme y Breuker, 2013).

Una ventaja de *blockchain*, es que puede identificar que los *bitcoins* de una dirección han sido mezclados (AMLC, 2017); por eso, las transacciones realizadas a través de un servicio de mezcla se consideran sospechosas por la capa adicional de anonimato que se le proporciona.

Lavado de dinero y criptomonedas

A pesar de que las criptomonedas cuentan con muchos atributos que le permiten generar una ventaja competitiva sobre el sistema financiera tradicional, fomentando una mayor inclusión financiera de todas aquellas personas no bancarizadas; también, representan una amenaza para la estabilidad de los sistemas financieros y el desarrollo económico global, al fomentar su creciente uso por los delincuentes para lavar dinero, al pensar de manera errónea que si pagan con éstas, no corren el riesgo de ser rastreados por alguna autoridad, por su característica de "anonimato". (Investing México).

Otra de las amenazas de las criptomonedas es la propia innovación tecnológica al ser utilizada por proveedores de servicios para crear técnicas/herramientas para anonimizar y ocultar el origen las transacciones y brindar servicios para ocultar los recursos provenientes de una actividad

ilícita. Las principales técnicas utilizadas son los cambiadores de criptomonedas y servicios de mezcla.

Si se identificaran a los clientes en el momento de intercambian las criptomonedas *bitcoin* por productos y servicios o monedas normales, se podrían identificar actividades sospechosas, pero lamentablemente se ofrecen servicios para anonimizar la relación entre remitentes y destinatarios de transacciones dentro del sistema *Bitcoin*. (Möser, Böhme y Breuker, 2013).

Aunque hay programas de anonimato, como redes oscuras y mezcladores, diseñados para ocultar el origen de una transacción con *bitcoin* y facilitar el anonimato, gracias al surgimiento de nuevas técnicas para descubrir las identidades de los usuarios, ya no se puede garantizar el anonimato.

El lavado de dinero con criptomonedas se presenta como una oportunidad para poder rastrear con mayor facilidad a los delincuentes en sus esfuerzos por convertir sus fondos en efectivo, por la transparencia inherente de las cadenas de bloques.

Regular a la red *Bitcoin*, al remitente, a los receptores, mineros o el equipo de desarrollo de *Bitcoin*, resultaría ser algo difícil, poco factible, o poco eficiente. Pero los cambiadores de *Bitcoin*, al tratar con monedas fiduciarias, les permite caer con mayor facilidad bajo las leyes de cambio de moneda y las de transmisión de dinero, por lo que es probable que la regulación de *Bitcoin* en los intercambios de divisas, tengan el mayor efecto con la menor inversión de recursos. (Bryan, 2014).

Prevención de Lavado de dinero

La prevención al Lavado de Dinero, el combate al Financiamiento al Terrorismo han sido algunas de las principales prioridades de la comunidad internacional, por su riesgo para la estabilidad de los Sistemas Financieros.

Una de las mejores prácticas para mitigar los riesgos de LD a través de monedas virtuales es: corroborar la información de identidad de los clientes, rastrear sus direcciones IP y buscar en Internet información que confirme la relación entre su actividad y su perfil transaccional; adoptar procedimientos de licencia o registro para todos aquellos VASP, para reducir la naturaleza transfronteriza de las transacciones y “limitar la fuente de financiamiento a una cuenta bancaria, tarjeta de crédito o débito”, y que se sujeten y apliquen todas las obligaciones aplicables en las Recomendaciones de GAFI.

También, las señales de alerta de LD/FT difundidas por GAFI, ha contribuido a que los sujetos obligados relacionados con activos virtuales, puedan incrementar su efectividad en la detección, investigación y aseguramiento de los activos virtuales involucrados en actos delictivos.
México, al ser miembro de GAFI y adoptar sus recomendaciones, medidas regulatorias y operativas, le ha dado la oportunidad de robustecer su régimen de PLD/CFT/CFPADM, crear la

UIF y disposiciones en materia de prevención al LD/FT aplicables a su Sistema Financiero y actividades no financieras como la LFPIORPI y la “Ley *Fintech*”, en cumplimiento a dichas recomendaciones.

A través de la regulación en materia de prevención al LD/FT y los sistemas de reportes a la UIF, han generado aproximadamente 1,708 reportes de operaciones inusuales en el periodo de 2013 a septiembre 2021 y más de 9,000 avisos de operaciones en México donde se utilizó algún activo virtual como instrumento de pago los cuales representan aproximadamente 6,154 millones de pesos.

Regulación

Del análisis cualitativo que se realizó sobre la regulación de las Jurisdicciones de Estados Unidos, Europa y México, países miembros de GAFI, se concluye lo siguiente:

México, a pesar de haber iniciado sus acciones para combatir el LD y FT, muchos años después que Estados Unidos y La Unión Europea, hoy en día se encuentra a la vanguardia en su marco regulatorio con la LFPIORPI y la “Ley *Fintech*”. Y para la prevención y el combate contra el LD y FT. Ocupa el séptimo lugar a nivel mundial en la regulación del sector *Fintech* (CNBV, 2019b, párr. 1).

El alcance del marco legal en los es diferentes países no es igual algunos aspectos, ejemplo de ello es que, mientras que Estados Unidos y La Unión Europea reconocen a los activos virtuales como monedas virtuales, clasificándolas como monedas virtuales convertibles y no convertibles, mientras que México no los reconoce como una moneda, por no cumplir con las funciones de la definición clásica del dinero. Sólo son una representación de valor registrada electrónicamente y utilizada entre el público como medio de pago, cuya transferencia sólo puede realizarse a través de medios electrónicos.

Por lo anterior, es que, en México, IC y las ITF no están autorizadas para ofrecer al público en general operaciones con activos virtuales, sólo pueden operar con activos virtuales que correspondan a operaciones internas; sin embargo, la regulación no impide que otras empresas no financieras puedan ofrecer servicios relacionados con activos virtuales, como el intercambio o la compraventa. En consecuencia, la compra-venta de activos virtuales en México, se realiza a través de casas de cambio que ofrecen el servicio de compra-venta de activos virtuales al público, bajo riesgo, al no estar respaldadas por alguna institución financiera.

A pesar de no estar permitido que las IC e ITF ofrezcan servicios con activos virtuales, Banco de México, emitió La “Ley *Fintech*” para regular a las ITF, en prevención al LD y FT y proteger a los consumidores. Esta Ley, se enfoca principalmente en un mecanismo de solicitudes de autorización para operar como ITF, dirigida a las Instituciones de Financiamiento Colectivo, a las de Fondos de Pago Electrónico y Modelos Novedosos, abarcando aspectos de su organización, operación, funcionamiento, servicios financieros y operaciones con activos virtuales. Sobre la

operación de activos virtuales, señala que éstas instituciones, previa autorización de Banco de México, podrán operar con los activos virtuales que éste determine y en los términos, condiciones y plazos que establezca.

Despliega una serie de disposiciones en cumplimiento con las recomendaciones de GAFI como: es el implementar un programa antilavado de activos asociados con monedas virtuales, donde establezca medidas y procedimientos para prevenir y detectar actos, omisiones u operaciones que se ubiquen en los delitos de operaciones con recursos de procedencia ilícita (art. 400 bis.) y financiamiento al terrorismo (art. 139 quáter) previstos en el Código Penal Federal; así como una metodología para evaluar los riesgos a los que se estén expuestos; y la presentación de reportes ante la CNBV.

Además, a parte de la identificación del cliente, contempla la identificación de propietarios reales, proveedores de recursos, beneficiarios y terceros autorizados en cuentas abiertas por los Clientes.

También comprende el conocimiento y la debida diligencia del cliente que considera umbrales de operación en cuentas o contratos de clientes; los sistemas automatizados para su operación y que además les permita conocer la trazabilidad y el origen y destino de los activos virtuales con los que operen. Sobre la transaccionalidad de los clientes está el presentar ante las autoridades los siguientes reportes: el reporte de operaciones inusuales para aquellas operaciones que no concuerden con su perfil transaccional, el reporte de operaciones que sean igual o rebasen el umbral de 5,000 USDLS y el reporte de compras de activos virtuales que sean igual o superior al umbral de 7,500 UDIS. Y finalmente, el resguardo e intercambio de información entre ITF y con otras entidades financieras nacionales y extranjeras, por señalar algunas.

En consecuencia, hasta el momento, esta Ley no considera las técnicas y herramientas informáticas utilizadas en las transacciones con *bitcoin* y el sistema *blockchain* para conservar el anonimato, en prevención y combate al lavado de dinero y el intercambio.

Por lo que se refiere a que los sistemas automatizados permitan conocer la trazabilidad y el origen y destino de los activos virtuales, cabe mencionar que la Ley, no define que debe de entenderse por trazabilidad, origen y destino de los activos virtuales, así como tampoco los mecanismos para que dichos sistemas puedan cumplir con estos requisitos.

Por lo tanto, se rechaza parcialmente la Hipótesis 2. La “Ley *Fintech* considera aspectos regulatorios que previenen y combaten el lavado de dinero mediante disposiciones que permiten identificar las operaciones de mezcla, transaccionalidad e intercambio en el sistema *blockchain*”.

Sin embargo, es de importancia destacar que para poder regular aquellas personas o entidades no financieras que ofrecen servicios de intercambio de activos virtuales por medio de plataformas electrónicas o digitales, además de administrar, operar, facilitar o realizar operaciones de compra o venta de activos virtuales, o suministrar medios para custodiar, almacenar, o transferir activos

virtuales, la LFPIORPI incluye en su lista de actividades vulnerables, la operación de entidades no financieras con activos virtuales, quedando así sujetos todos estos servicios al régimen de esta Ley, estableciéndoles una serie de requisitos en atención a las recomendaciones de GAFI.

Así mismo, dentro del contexto de esta misma Ley, al entender que, la actividad de una persona o entidad no financiera que considere recibir una forma de valor (activo virtual convertible) de una persona y transmitir la misma, o en una forma diferente de valor (activo no convertible o totalmente anónimo) a otra persona o ubicación, por medio electrónico, o digital, queda cubierta bajo la reglamentación de esta Ley y, por lo tanto, se estaría mitigando los riesgos mediante técnicas y herramientas de anonimización.

Estudio de Casos

Los resultados del estudio de casos sobre las cinco empresas prestadoras de servicios internacionales de activos virtuales y sobre los cuatro casos de delincuentes (narcotraficantes) en México, para comprobar la hipótesis H1, permiten concluir lo siguiente:

- Con el intercambio de monedas virtuales a moneda fiduciaria u otra moneda virtual no se vulnera la seguridad e inmutabilidad del sistema *blockchain*. (Casos: *Helix y Coin Ninja, BTC-e, BINANCE,* Ignacio Santoyo y Zaragoza).

- *Con la técnica Coin Join,* al mezclar los fondos mediante una transacción fuera de línea (*blockchain*), no se vulnera la seguridad e inmutabilidad del sistema *blockchain* para conservar el anonimato en las transacciones con *bitcoin* para lavar dinero. (Caso Helix y Coin Ninja).

- La técnica *Coin Swap* aprovecha las características propias del funcionamiento y protocolo de las transacciones para realizar la mezcla de criptomonedas. No altera el registro de transacciones ya hechas, más bien, divide las criptomonedas en cientos de transacciones nuevas, por lo tanto, no se estaría vulnerando la inmutabilidad ni la seguridad de la tecnología *blockchain*. (Caso *BestMixer.io y Bitcoin Fog*).

- La técnica "pitufo", al dividir el efectivo ilícito en pequeñas cantidades en cuentas bancarias y luego comprar pequeñas cantidades de *bitcoin*, tampoco vulnera la inmutabilidad ni la seguridad de la tecnología *blockchain*. (Caso CJNG y Cartel de Sinaloa).

Con base a lo anteriormente expuesto, se concluye que las técnicas de intercambio y mezcla utilizadas para conservar el anonimato en las transacciones con *bitcoin*, no vulneran la tecnología de *blockchain* para lavar dinero, por lo tanto, la Hipótesis: H1**.** “Se vulnera la seguridad e inmutabilidad del sistema *blockchain* mediante la mezcla o el intercambio de las criptomonedas para conservar el anonimato en las transacciones con *bitcoin* para lavar dinero”, se rechaza.

Otras conclusiones a las que se pudieron llegar son:

- El uso de empresas de servicios internacionales de intercambio *de monedas virtuales* que no tienen licencia o no están registradas, para ocultar los recursos de procedencia ilícita. Este resultado coincide con lo señalado por (Serrano, 2020) sobre el uso potencial de los cambiadores sin licencia o registro.

- Las principales herramientas que utilizan los VASP para anonimizar las transacciones con *bitcoin*, son las plataformas en redes obscuras (*darknet)* y mercado negro para lavar dinero (Caso de Big Fog).

- A través del análisis de *blockchain* por los investigadores y firmas forenses, la característica de transparencia de la tecnología *blockchein* y los beneficios que ofrece sobre integridad, trazabilidad e inmutabilidad, es que las autoridades han podido rastrear a los delincuentes y VASP registrados y no registrados, y exhibir la trazabilidad de todos los movimientos que realiza. Lo que representa una buena oportunidad para que los auditores e investigadores puedan rastrear los recursos procedentes de actividades ilícitas. (Caso de Big Fog).

- La detención de algunos delincuentes son evidencia del éxito que ha representado la nueva ley en México ("Ley *Fintech"*), al haber sido identificados por rebasar los umbrales en sus transacciones con *bitcoin* en una plataforma registrada y haber proporcionado sus datos personales. (Casos de Ignacio Santoyo y Héctor Ortíz).

Estos casos son evidencia de cómo sí es posible que tanto las autoridades como investigadores a nivel global, con recursos, herramientas y capacidad técnica adecuada pueden beneficiarse de la trazabilidad y transparencia de la criptomoneda y con un buen análisis de *blockchan*, se pueden rastrear los flujos de fondos provenientes de actividades ilícitas, a delincuentes y VASP. Y, a pesar de que mucho se dice que *Bitcoin* es una herramienta potente para lavar dinero, al realizar transacciones anónimas, imposibles de rastrear. Finalmente ha resultado ser todo lo contrario.

Para identificar y perseguir un delito o algún delincuente, también se requiere de una sinergia multinacional, y acción global entre las autoridades de cada gobierno e internacionalmente y el compromiso para identificar y perseguir a los delincuentes en todo el mundo.

Sin embargo, en México, una de las debilidades de la Unidad de Investigaciones Cibernéticas (UICOT) de la Fiscalía General de la República, es la plantilla de personal (120 personas) con la que se cuenta, para poder atender las alertas de umbral de *bitcoin* que se han activado con la nueva Ley, que el sistema solo puede identificar transacciones con compañías comerciales registradas y el equipo tiene una visibilidad limitada de los tratos en la *web* oscura y las plataformas no reguladas, que de acuerdo a los funcionarios estadounidenses y latinoamericanos encubren la verdadera escala del lavado de dinero. (Oré, 2020).

Temas de línea de investigación sugeridas

En México, la tecnología *blockchain* representa una solución a la corrupción y la falta de transparencia y su mayor uso es en las remesas y cada vez se está teniendo mayor adopción en el sector financiero, gobierno, aseguradoras, consumo, medios y telecomunicaciones, turismo, farmacéuticas y salud, al agilizar los procesos y volverlos más confiables y transparentes.

Sin embargo, unos de los principales retos, es la regulación, debido a que su regulación depende del uso que se le dé a *blockchain* y el giro de la empresa, como es el caso de la "Ley *Fintech*" en México para regular las empresas que operan con criptomonedas como *bitcoin*, en prevención al LD/FT y la personal capacitado, por ello, se sugieren las siguientes líneas de investigación.

- Investigar cómo funciona el análisis de técnicas y herramientas de análisis de *blockchain* y técnicas utilizadas para rastrear a movimientos de recursos de procedencia ilícita con criptomonedas y delincuentes.

- Identificar y analizar los mecanismos, técnicas, herramientas y procedimientos implementados por las *Fintech* para conocer la trazabilidad y origen y destino de los activos virtuales que operen, y si cuentan con los recursos necesarios para dar cumplimiento con el requerimiento de la "Ley *Fintech*".

- Investigar cómo funciona la aplicación de la cadena de bloques en los procesos financieros para garantizar la seguridad, transparencia, controles y cumplimiento regulatorio, como en: las consolidaciones contables entre empresas, detección de fraude y riesgo, planificación de capital y gestión del rendimiento, gestión del ciclo de ingresos, financiamiento comercial, capital de trabajo y mejora del ciclo de efectivo, entre otros.

- Investigar cómo funciona la aplicación de la cadena de bloques en el sector productivo para generar transacciones con menor intermediación, más seguras, transparentes y agilizar los procesos de todas las cadenas estratégicas de negocios. Y su regulación.

Anexo I Cuadro Resumen del Estudio de Casos

Casos de Empresas Prestadoras de Servicios Internacionales de Activos Virtuales

	Caso	Pais	Empresa Prestadora de Servicio (Modelo de negocio)	Técnica para lavar dinero	Herramienta	Cumplimiento Hipótesis H1	Importe de recursos lavados con *bitcoins* (en USD)
1	Helix y Coin Ninja	Estados Unidos	Intercambiador de monedas virtuales convertibles. y Mezclador de bitcoin través de transacciones de CoinJoin.	Intercambio y Mezcla con CoinJoin	Para Mezclar: 1. Herramienta de privacidad *(Bitcoin Mixer Helix*). 2. Motor de búsqueda de la *darknet.* 3. Grams, para realizar transacciones en *AlphaBay* , un mercado negro en la red oscura.	Con el intercambio de monedas virtuales a moneda fiduciaria u otra moneda virtual y con la técnica Coin Join, para mezclar fondos no se vulnera la seguridad e inmutabilidad del sistema *blockchain,* por lo tanto, **se rechaza la Hipótesis H1.**	$311,000,000
2	BestMixer.io	Luxemburgo y paises bajos	Mezclador de criptomonedas líder en el mundo	Mezcla con CoinSwap	Plataforma Bestmixer.io con vaso para mezclar.	Con la técnica CoinSwap, para mezclar fondos no se vulnera la seguridad e inmutabilidad del sistema *blockchain,* por lo tanto, **se rechaza la Hipótesis H1.**	200,000,000
3	Bitcoin Fog	Estados Unidos	Servicio de Mezcla	Mezcla con CoinSwap	1. *Bitcoin mixer,* que consiste en ocultar la fuente de una criptomoneda licuándola con otros fondos. 2. Billetera digital. 3. Red oscura Tor. 4. Desarrolladores profesionales de aplicaciones web seguras.	Con la técnica CoinSwap, para mezclar fondos no se vulnera la seguridad e inmutabilidad del sistema *blockchain,* por lo tanto, **se rechaza la Hipótesis H1.**	336,000,000
4	BTC-e	Bulgaria, sujeto a las leyes de Chipre	Intercambio de monedas virtuales	Intercambio	Plataformas de compra y venta de terceros para poder adquirir criptomonedas.	Con el intercambio de monedas virtuales a moneda fiduciaria u otra moneda virtual no se vulnera la seguridad e inmutabilidad del sistema *blockchain,* por lo tanto, **se rechaza la Hipótesis H1.**	4,000,000,000
5	BINANCE	China	Intercambio de monedas virtuales	Intercambio	1.Plataforma de intercambio de criptomonedas. 2. Binance DEX plataforma de intercambio opera dentro de una *blockchain* que no almacena los fondos ni datos personales de los usuarios en sus servidores. 3. Red *blockchain* propia.	Con el intercambio de monedas virtuales a moneda fiduciaria u otra moneda virtual no se vulnera la seguridad e inmutabilidad del sistema *blockchain,* por lo tanto, **se rechaza la Hipótesis H1.**	2,350,000
							$4,849,350,000

Casos de Delincuentes (Narcotraficantes) en México

	Casos de México	Estado	Actividad	Técnica para lavar dinero	Herramienta	Cumplimiento Hipótesis H1	Importe de recursos lavados con *bitcoins* (en Pesos MX)
1	CJNG y Cártel de Sinaloa	Guadalajara Sinaloa	Narcotraficante	Técnica conocida como "pitufo".	Plataforma de intercambio.	Con la técnica pitufo, al dividir su efectivo ilícito en pequeñas cantidades y depositarlas en varias cuentas bancarias, para después usar esas cuentas para comprar pequeñas cantidades de bitcoin en línea, no se vulnera la seguridad e inmutabilidad del sistema *blockchain,* por lo tanto, **se rechaza la Hipótesis H1.**	No se especifica
2	Ignacio Santoyo	Playa del Carmen	Red de Prostitución	Intercambio en plataforma.	Plataforma de intercambio registrada.	Con el intercambio de monedas virtuales a moneda fiduciaria u otra moneda virtual no se vulnera la seguridad e inmutabilidad del sistema *blockchain,* por lo tanto, **se rechaza la Hipótesis H1.**	$441,000
3	Héctor Ortiz	Guanajuato	Narcotraficante	Intercambio en plataforma.	Plataforma de intercambio registrada.	Con el intercambio de monedas virtuales a moneda fiduciaria u otra moneda virtual no se vulnera la seguridad e inmutabilidad del sistema *blockchain,* por lo tanto, **se rechaza la Hipótesis H1.**	No se especifica
4	Zaragoza	Jalisco y Michoacán	Narcotraficante	Intercambio. Triangulación de recursos. Transferencias de recursos hacia y del extranjero.	Plataforma de intercambio clandestina, uso de una operadora financiera para mover cantidades millonarias en efectivo.	Con el intercambio de monedas virtuales a moneda fiduciaria u otra moneda virtual no se vulnera la seguridad e inmutabilidad del sistema *blockchain,* por lo tanto, **se rechaza la Hipótesis H1.**	No se especifica
							$441,000

Glosario

Asociación de Especialistas Certificados en Delitos Financiero (ACFCS): Es una asociación internacional que ofrece certificación, membresía y capacitación para detectar y prevenir delitos financieros tales como lavado de dinero, fraude, delitos cibernéticos, corrupción y mucho más.

Banco de México: es el banco central del país. Provee la moneda nacional y tiene el objetivo prioritario, establecido en la Constitución, de preservar su valor. Además, promueve el sano desarrollo de los sistemas financiero y de pagos.

***Bitcoin* (con mayúscula)** se refiere al software que hace posible la custodia y transferencia de la criptomoneda. (Infobae)

***bitcoin* (con "b" minúscula)** es una moneda. (Infobae)

Blockchain* de *Bitcoin es una base de datos distribuida, criptográfica e inmutable que usa *proof-of-work* (prueba de trabajo) para documentar el flujo de su moneda nativa, bitcoin. (Infobae)

Capitalización de mercado: La capitalización de mercado es el valor total de las acciones de una empresa en el mercado. A menudo se abrevia como cap. de mercado. La capitalización de mercado es una forma sencilla de determinar el tamaño de una compañía y evaluar el riesgo de invertir en sus acciones.

CipherTrace: Primer equipo forense de *blockchain* del mundo. Expertos en *Bitcoin*, eCrime y pagos colaboran para combatir el cripto crimen con gran experiencia en ciberseguridad, sistemas de pago, minería de *bitcoins* y fueron los primeros participantes en la comunidad de *bitcoins*. Se fundó para producir inteligencia y análisis forense de *blockchain*. Rastrea el *ransomware Locky* hasta *BTC-e* y atribuye el 95% del lavado global de *ransomware* a *BTC-e.*
Lanza el producto API de inteligencia *blockchain CipherTrace* y presenta la aplicación móvil para la investigación y el análisis forense de criptomonedas.

Comisión Nacional Bancaria y de Valores: órgano desconcentrado de la Secretaría de Hacienda y Crédito Público (SHCP), con facultades en materia de autorización, regulación, supervisión y sanción sobre los diversos sectores y entidades que integran el sistema financiero en México, así como sobre aquellas personas físicas y morales que realicen actividades previstas en las leyes relativas al sistema financiero. La Comisión se rige por la Ley de la CNBV.

Agencia de la Unión Europea para la Cooperación Policial (EUROPOL): Ayudar a que Europa sea más segura. Su principal objetivo es lograr una Europa más segura en beneficio de todos los ciudadanos de la UE. Tiene su sede en La Haya, Países Bajos, apoyamos a los 27 Estados miembros de la UE en su lucha contra el terrorismo, la ciberdelincuencia y otras formas graves y organizadas de delincuencia. También trabajamos con muchos estados socios no pertenecientes a la UE y organizaciones internacionales. Sus actividades operacionales se

centran en drogas ilícitas, tráfico de seres humanos, facilitó la inmigración ilegal, ciberdelito, delito de propiedad intelectual, contrabando de cigarrillos, falsificación de euros, Fraude de IVA, blanqueo de capitales y rastreo de activos, grupos móviles de delincuencia organizada, proscribir las bandas de motociclistas, terrorismo.

Financial Crimes Enforcement Network (FinCEN): Es una agencia del Departamento del Tesoro estadounidense creada en 1990, que almacena y analiza información sobre transacciones financieras con el fin de luchar contra los delitos financieros, como el fraude hipotecario, lavado de dinero y financiación del terrorismo. El Director de FinCEN es nombrado por el Secretario del Tesoro y reporta al subsecretario del Tesoro para Terrorismo e Inteligencia Financiera.

Ingeniería de software: La ingeniería del software es una disciplina que implica el uso de estructuras, herramientas y técnicas para construir programas informáticos. Incluye el análisis previo de la situación**,** la redacción del proyecto, la creación del software y las pruebas necesarias para garantizar el correcto funcionamiento del software antes de poner el sistema en funcionamiento.

Inyección de código externo: Una inyección de **código** SQL es una vulnerabilidad que permite al atacante enviar o **inyectar** instrucciones SQL de forma maliciosa dentro del **código** SQL de una aplicación o sitio *web* para la manipulación de bases de datos, de forma que todos los datos almacenados en esta corren peligro.

Riesgo emergente: situación, tendencia delictiva o amenaza regional o incluso mundial con potencial consecuencia negativa para el régimen PLD/CFT/CFPADM que, sin presentar aún una incidencia significativa en términos de índices delictivos, irrumpe en el escenario de determinado país.

Token: es “una unidad de valor que una organización crea para gobernar su modelo de negocio y dar más poder a sus usuarios para interactuar con sus productos, al tiempo que facilita la distribución y reparto de beneficios entre todos sus accionistas”. (William Mougayar, autor del libro ‘*The business blockchain*’, el nuevo término de la economía digital.)

Unidad de Investigaciones Cibernéticas en México: La Unidad de Investigaciones Cibernéticas y Operaciones Tecnológicas, es un órgano de la Procuraduría General de la República dentro de la Agencia de Investigación Criminal, y tiene como objetivo “la ejecución y supervisión de las acciones policiales que apoyen las investigaciones relacionadas con medios electrónicos y tecnológicos bajo la conducción y mando del Ministerio Público de la Federación”.

Bibliografía

Antonopoulos, A.M. (2017). Mastering Bitcoin. Programming the Open Blokchain.

Acuña, H. (2018). CUADERNOS CEF / N°2 Criptomonedas, Aplicaciones Potenciales de Blockchain y Desafíos Regulatorios. Centro de Estudios Financieros. Universidad de los Andes.

Ávila L. (2018). ¿Cómo se debe plantear un curso introductorio a la tecnología Blockchain, que haga uso de la información y los trabajos disponibles, y que también permita aplicar tal tecnología al contexto colombiano? (Tesis para Maestría). Universidad de los Andes

Departamento de Ingeniería Industrial Bogotá D.C, Colombia. Recuperado de https://repositorio.uniandes.edu.co/bitstream/handle/1992/34918/u820829.pdf?sequence=1&isAllowed=y 27 de septiembre 2022.

Bancomext y Proméxico. (2018). México Nación Fintech, Negocios y Ecosistemas en el Sector Financiero Mexicano. México.

Bryans, D (2014). Bitcoin and Money Laundering: Mining for an Effective Solution. Indiana Law Journal: Vol. 89:Iss.1, Article 13. Maurer School of Law Digital Repository. U.S.A. Recuperado de https://www.repository.law.indiana.edu/ilj/vol89/iss1/13

Buterin, V. (06 de febrero de 2017). The Meaning of Decentralization. Recuperado de: https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274.

Cassinelo, N., Cervera, I., Ibañez J.W., & López C. (2017). El desarrollo de las soluciones Fintech en España. Icade. *Revista cuatrimestral de las Facultades de Derecho y Ciencias Económicas y Empresariales, No, 101.* España. Recuperado de https://repositorio.comillas.edu/xmlui/bitstream/handle/11531/27093/ICADE-El%20desarrollo%20de%20las%20soluciones%20Fintech%20en%20Espa%c3%b1a.pdf?sequence=1&isAllowed=y . 7 de enero 2022.

Cruz, A. (2018). El Bitcoin y un nuevo paradigma para el Sistema Monetario Internacional. (Tesis de Maestría en Economía) UNAM. Estado de México.

Enrique, A. y Barrio, E. (S/F) Guía para Implementar el Método de Estudio de Caso en Proyectos de Investigación. Recuperado de https://ddd.uab.cat/pub/caplli/2018/196118/proinvare_a2018p159.pdf. Mayo 2021.

Forde, B. (03 de 07 de 2017). Datos abiertos y 'blockchain': el antídoto contra la opacidad de empresas y gobiernos. Recuperado el 21 de 01 de 2019, de Harvard Business Review en español. Recuperado de https://www.hbr.es/gobiernos/680/datos-abiertos-y-blockchain-el-ant-doto-contra-la-opacidad-de-empresas-y-gobiernos.

GAFI. (2014). Informe del GAFI. Monedas Virtuales Definiciones Claves y Riesgos Potenciales de LA/FT. Recuperado en https://www.bc.gob.cu/ /storage/regulaciones-sbancaria/March2018/2aNN5iaWy2gsCm7JiIIm.pdf.

Grinberg, R. (2011). Bitcoin: An Innovative Alternative Digital Currency. VL 4. Hastings Science & Technology Law Journal. Recuperado de https://www.researchgate.net/publication/228199328_Bitcoin_An_Innovative_Alternative_Digital_Currency.

Gobierno de México (UIF), (2020). Evaluación Nacional de Riesgos 2020. Recuperado de https://www.pld.hacienda.gob.mx/work/models/PLD/documentos/enr2020.pdf 9 de noviembre 2020.

Houben, R. & Snyers, A. (2018). Cryptocurrencies and blockchain. Legal context and implications for financial crime, money laundering and tax evasión (pág. 33) European Parliament. Bruselas. Recuperado de https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf

Lloreda Camacho & Co. (2019). México, Regulación Fintech en Lationamérica, con la colabroación de Creel Abogados, S.C., Bolaños& I. & Botello M. Segunda Edición. Santiago Chile. Recuperado de https://lloredacamacho.com/regulacion-fintech-en-latinoamerica-segunda-edicion/

Medina, M.C., Alcantara A.L., Hernández J.L., & González J.M., (Marzo, 2015) ¿Qué es la Certificación en Prevención de Lavado de Dinero?, Auditoría, Control Interno y Monitoreo Continuo, El Gobierno y los Ingresos por Actividades Ilícitas. Certificación y Auditoría en Prevención de Lavado de Dinero. *Revista Contaduría Pública. IMCP*. México. Recuperado en https://contaduriapublica.org.mx/wp-content/uploads/202015_03.pdf.

Monasterio, A. (2012) Puzzles Criptográficos. Implementación y Evaluación. Proyecto de Fin de Carrera. Universidad Carlos III de Madrid. Departamento de Informática.

Mora, E.A. (2016). Monedas Virtuales se suman al Comercio Electrónico. (Ensayo de Especialización en Gerencia en Comercio Internacional). Facultad de Ciencias Económicas. Universidad Militar Nueva Granada. Bogotá.

Möser, M., Böhme, R., & Breuker, D. An Inquiry into Money Laundering Tools in the Bitcoin Ecosystem. eCrime Researchers Summit (eCrime), 2013.

Naciones Unidas (ONU) (Marzo, 2022). Informe de la Junta Internacional e Fiscalización de Estupefacientes correspondiente 2021. Oficina de las Naciones Unidas en Viena. Recuperado de https://www.unodc.org/documents/mexicoandcentralamerica/2022/Informe_JIFE_2021.pdf. 15 mayo 2022.

Nakamoto, S. Bitcoin. A Peer-to-Peer Electronic Cash System. Recuperado en https://bitcoin.org/bitcoin.pdf.

Nieto, N. (2019). Análisis del fenómeno fintech y su marco regulatorio: el caso de MytripleA. Trabajo fin de grado. Facultad de Ciencias Empresariales y del Trabajo de Soria. Universidad de Valladolid.

Puvogel Rojas, M. (2018). Blockchain y Monedas Virtuales Aproximación Jurídica (Tesis de Licenciatura). Facultad de Derecho. Universidad de Chile. Santiago Chile. URI: https://repositorio.uchile.cl/handle/2250/159493.

Ponce, A. (2018). El Estudio de Caso Múltiple. Una estrategia de Investigación en el ámbito de la Administración Revista Publicando, 5 No 15. (2). 2018, 21 -34. ISSN 1390-9304 Quito, Ecuador. Instituto de Altos Estudios Nacionales, Centro de Gobierno y Administración Pública.

Rodríguez, JE. (2019). Evolución del Bitcoin: Una mirada teórica desde la economía conductual. (Tesis Licenciatura). Facultad de Economía UNAM. México.

Rule,P &Michel, V. (2015) A Necessary Dialogue: Theory in Case Study Research. International Journal of Qualitative Methods 2015. DOI: 10.1177/1609406915611575.

Salort, S. (2012). Revoluciones Industriales, trabajo y Estado del Bienestar. Editorial Silex.

Serrano, JC, (Abri-Junio 2020). Criptomonedas y lavado de activos: un análisis comparativo. *Revista Derecho Penal No. 71,* págs. 5-84. Colombia. Recuperado de https://xperta.legis.co/visor/rpenal/rpenal_67839f1327b04ac685576aa59033315a/revista-de-derecho-penal-contemporaneo/criptomonedas-y-lavado-de-activos%3a-un-analisis-comparativo , el 14 de noviembre 2021.

Smith, A. An Inquiry Into the Nature and Causes of the Wealth of Nations. Books I, II, III, IV y V. Editorial Note. Meta Libri (2007). Recuperado en https://www.ibiblio.org/ml/libri/s/SmithA_WealthNations_p.pdf.

Stake, R (1998). Investigación con estudio de casos. Ediciones Morata, S. L. Primera Edición. España Madrid.

Cibergrafía

Abogados de los EU, Distrito Norte de California. (2017). Departamento de Justicia. Oficina del Fiscal de los Estados Unidos. Intercambio nacional ruso y bitcoin acusado en una acusación de 21 cargos por operar un presunto esquema internacional de lavado de dinero y presuntamente lavar fondos del hackeo de Mt. Gox. Recuperado de https://www.justice.gov/usao-ndca/pr/russian-national-and-bitcoin-exchange-charged-21-count-indictment-operating-alleged .

Acendes, único sistema de originación de crédito que permite administrar todo el proceso de forma 100% digital. Recuperado de https://www.acendes.com. 5 de agosto de 2020, 10:00 pm.

Agencia de la Unión Europea para la Cooperación Policial (EUROPOL). Recuperado de https://www.europol.europa.eu/, el 2 de noviembre de 2021 2:15 am.

Ast Federico (21 de noviembre 2020). Blockchain ¿Qué Es y Cómo Funciona? Publicado en Astec. Recuperado de https://medium.com/astec/blockchain-qu%C3%A9-es-y-c%C3%B3mo-funciona-e5221f780fcc , 23 de noviembre de 2020.

Banco de México. Sobre los activos virtuales, los riesgos relevantes y el posicionamiento del Banco de México. 3. ¿Cómo funciona un activo virtual?, 3.1. Proceso de transacción del primer activo virtual y 3.2. Proceso de compra-venta de activos virtuales. Recuperado de https://www.banxico.org.mx/sistemas-de-pago/3---como-funciona-un-activo.html. Octubre 2021.

Banal, A. (2016). Qué son las Fintech. La Vanguardia. Finanzas Tecnológicas. Barcelona. Recuperado de https://www.lavanguardia.com/economia/management/20160811/403831350794/que-son-fintech.html Marzo 2020, 13:30 pm.

Bastardo, J. (13 de febrero 2020). Arrestan al CEO de Ninja Coin por presunto lavado de USD 311 millones con las herramientas de privacidad de Bitcoin. Cointelegraph en español. Recuperado de https://es.cointelegraph.com/news/coin-ninja-ceo-arrested-for-laundering-311m-with-bitcoin-privacy-tools . 13 de noviembre 2020. 6:25 pm.

BestMixer (2018-2021). Cómo funciona? BestMixer. Recuperado de https://bestmixer.pw/how.html . 17 de noviembre 15:30 pm.

(Bit2meacademy, 2021). Cómo minar bitcoin. Función de la Minería. *Recuperado de https://academy.bit2me.com/que-es-minar-bitcoins*. Diciembre 2021.

Cadenas, Eloisa (2018) ¿Son las criptomonedas una herramienta potencial para el lavado de dinero? Criptomonedas. Recuperado de https://mx.investing.com/analysis/son-las-criptomonedas-una-herramientas-potencial-para-ellavado-de-dinero-200200320 18 de abril 2020. 14:20 pm.

Chipolina, S. (8 de diciembre 2020). Compras de Bitcoin Permitieron Apresar a Dos Criminales de Alto Perfil en México. Las autoridades mexicanas hicieron dos grandes arrestos en 2019 gracias al rastreo de una serie de compras de alto volumen de Bitcoin. Recuperado de https://decrypt.co/es/50828/compras-bitcoin-permitieron-apresar-dos-criminales-mexico 25 de febrero 2021 18:30 pm.

CipherTrace. Cryptocurrency Intelligence (2021). New Zealand Police Seize $90 Million in Investigation of BTC-e Exchange. Cryptocurrency Crime and Anti-Money Laundering Report. February 2021. Recuperado de Recuperado de https://ciphertrace.com/wp-content/uploads/2021/01/CipherTrace-Cryptocurrency-Crime-and-Anti-Money-Laundering-Report-012821.pdf. el 3 de noviembre. 12:23 am.

Comisión Nacional Bancaria y de Valores (20 de enero 2021). CNBV informa respecto al proceso de autorización de Instituciones de Tecnología Financiera. Recuperado de https://www.gob.mx/cnbv/articulos/cnbv-informa-respecto-al-proceso-de-autorizacion-de-instituciones-de-tecnologia-financiera. 27 de marzo de 2021. 11:40 pm.

Coyote, R. (2020) MCCOLLECT. Automatización en el proceso de originación de créditos, como solución digital. Recuperado de https://mccollect.com.mx/2020/10/08/automatizacion-en-el-proceso-de-originacion-de-creditos/ . 7 de agosto de 2020, 11:00 pm.

https://www.uiaf.gov.co/asuntos_internacionales/normatividad_internacional. 20 de noviembre 2021. . falta hora

Crypto Español, (2017) ¿Cómo funciona Blockchain? Explicación sencilla visual en español. (05 de 11 de 2017), Recuperado de https://www.youtube.com/watch?v=hEoYL5j0wYU&t=72s. Consultado el 15 de julio de 2021, 9:30 pm.

Darlington N. (2021). ¿Qué es la tecnología Blockchain? ¿Cómo Funciona? A*ctualizado el 22 de septiembre de 2021. Recuperado de https://blockgeeks.com/guides/what-is-blockchain-technology/. Consultado el 11 de 10 de 2021.*

Distefano B. (2022). Binance se convirtió en un centro de narcos, estafadores y hackers. Reuters. Recuperado de https://www.criptonoticias.com/judicial/investigacion-acusa-binance-convirtio-centro-narcos-estafadores-hackers/ 7 de Junio 2022. 16:35 pm.

De Monteverde, Coty (2019). Institute for Advancer Management (CEU IAM). Blockchain y su aplicación en el ámbito financiero. Recuperado de 9https://www.youtube.com/watch?v=lkO168P39Z0&t=19s. 17 de julio 2021, 8:20 pm.

De, N. (4 de mayo 2021). State of Crypto: The Bitcoin Fog Indictment Shows the Permanence of User Data. CoinDesk. Opinion. Updated Sep 14, 2021 at 7:50 a.m. CDT. Recuperado

de https://www.coindesk.com/policy/2021/05/04/state-of-crypto-the-bitcoin-fog-indictment-shows-the-permanence-of-user-data/ . 19 de noviembre 2021. 11:15 pm

Del Rey, J (2013). What's a Bitcoin Really Worth? CoinDesk Thinks It Has the Answer. AllThings D. Recuperado de What's a Bitcoin Really Worth? CoinDesk Thinks It Has The Answer - Jason Del Rey - Commerce - AllThingsD. Junio 2021 14:30 pm

Eckel, Mike (2019). How Much Did Russian Spy Agencies Rely On Bitcoin? New Hints In Leaked Recordings. Radio Free Europe Radio Liberty. Regions. Rusia. Recuperado de https://www.rferl.org/a/how-much-did-russian-spy-agencies-rely-on-bitcoin-new-hints-in-leaked-recordings-/30297083.html .

El Cronista (2021). Binance fue prohibido en el Reino Unido, ¿qué pasa ahora con Argentina?. La República (Periódico de Colombia). Recuperado de https://www.larepublica.co/globoeconomia/criptomoneda-binance-fue-prohibido-en-el-reino-unido-que-pasa-ahora-con-argentina-3193598 . 11 de noviembre 2021.

FINCEN (2020). Helix y Coin Ninja, primer "mezclador" de Bitcoin. Recuperado de https://www.fincen.gov/news/news-releases/first-bitcoin-mixer-penalized-fincen-violating-anti-money-laundering-laws 20 de octubre 2021 . 10:25 am

GAFILAT. (14 de octubre 2020). Caso de Estudio 6. Uso de mezcla y volteo – Helix. Informe de GAFI Activos Virtuales. Señales de Alerta LDFT. Recuperado de https://www.gafilat.org/index.php/es/biblioteca-virtual/gafilat/documentos-de-interes-17/traducciones/3873-informe-del-gafi-activos-virtuales-senales-de-alerta-de-ld-ft .12 de noviembre 2020 . 9:30 am

Gilson, David (2013). Reviewed: BTC-e crypcurrency Exchange. CoinDesk reviews the BTC-e exchange, which is seeing increased activity due to difficulties withdrawing funds from Mt. Gox. Updated Sep 14, 2021 at 9:11 a.m. CDT. CoinDesk. Recuperado de Revisado: Btc-e intercambio de criptomonedas - CoinDesk .14 de noviembre 2021 6:13 pm.

Greenber Andy (27 de Abril 2021). Feds Arrest an Alleged $336M Bitcoin-Laundering Kingpin. The alleged administrator of Bitcoin Fog kept the dark *web* service running for 10 years before the IRS caught up with him. WIRED. Recuperado de https://www.wired.com/story/bitcoin-fog-dark-*web*-cryptocurrency-arrest/ . 17 de noviembre 2021. 4:30 pm.

Grupo de Acción Financiera de Latinoamérica (2018). Normatividad Internacional, las 40 Recomendaciones de GAFI (Estándares Internacionales sobre la Lucha contra el Lavado de Activos, el Financiamiento del Terrorismo, y el financiamiento de la proliferación de armas de destrucción masiva). Recuperado de

Gutiérrez F. (10 de abril de 2022). Caso Zaragoza, el referente para la UIF en materia de criptomonedas y lavado de dinero. Blanqueo, delincuencia organizada, narcotráfico y defraudación fiscal, se combinaron en este caso que derivó en denuncias y bloqueo de recursos por parte de esta instancia. El Economista. Recuperado de https://www.eleconomista.com.mx/sectorfinanciero/Caso-Zaragoza-el-referente-para-la-UIF-en-materia-de-criptomonedas-y-lavado-de-dinero-20220410-0023.html 11 de abril 2022 16:30 pm.

Gutiérrez F. (16 de junio de 2021). Ley Fintech: Antecedentes y actualidad. Día Fintech. Recuperado de https://diafintech.com.mx/noticia/ley-fintech-origen-y-actualidad/. 28 de julio de 2021.

Haig, S. (29 APR 2021) Atrapan a un ciudadano sueco-ruso que ha operado un servicio multimillonario de lavado de bitcoin durante 10 años. Cointelegraph. Recuperado de https://es.cointelegraph.com/news/alleged-366m-bitcoin-mixer-busted-after-analysis-of-10-years-of-blockchain-data . 8 de Mayo 2021 13:15 pm

Higgins, S. (22 de mayo de 2019). Las autoridades de la Unión Europea han incautado y cerrado un mezclador de transacciones de bitcoins. CoinDesk. Markets. Updated Sep 13, 2021 at 4:13 a.m. CDT. Recuperado de https://www.coindesk.com/markets/2019/05/22/eu-authorities-shut-down-bitcoin-transaction-mixer/ . 12 de noviembre de 2021 8:30 am.

IBM. ¿Qué es la seguridad de la cadena de bloques? Recuperado de https://www.ibm.com/topics/blockchain-security. 8 de noviembre 2021 5:30 pm.

Infobae, (2018). Cuál es la diferencia entre bitcoin y Bitcoin (con mayúscula). Infobae (Diario en Línea de actualidad y economía de Argentina). Recuperado de https://www.infobae.com/cripto247/educacion-cripto247/2018/06/28/cual-es-la-diferencia-entre-bitcoin-y-bitcoin-con-mayuscula/ 17 de marzo 2020.

Infobae, (2022) Acusan a la plataforma cripto Binance de canalizar fondos de actividades ilícitas como el tráfico de drogas y fraude. Infobae (Diario en Línea de actualidad y economía de Argentina). Recuperado de https://www.infobae.com/economia/2022/06/06/acusan-a-la-plataforma-cripto-binance-de-canalizar-fondos-de-actividades-ilicitas-como-el-trafico-de-drogas-y-fraude/#:~:text=Los%20datos%20recopilados%20por%20Reuters,de%20780%20millones%20de%20d%C3%B3lares%E2%80%9D. 28 de junio 2022, 11:20 pm

Innoventia (Teknei y Hill House Capital). (2019). Primer Estudio del Ecosistema Blockchain México. Recuperado en https://medium.com/@Innoventia/primer-estudio-del-ecosistema-blockchain-mexico-a0c3637f3b72 y en https://www.linkedin.com/feed/update/urn:li:activity:6508470672581292032. falta hora

Lansky, Jan (2016). Analysis of Criptocurrencies Price Development. Doi: 10.18267/j.aip.89

López J. (2021). Seguridad en Blockchain: La (in)seguridad en la cadena de bloques. Auditech. Recuperado de https://auditech.es/seguridad-en-blockchain-la-inseguridad-en-la-cadena-de-bloques/. 3 de noviembre 2021. falta hora

López R. (15 febrero 2020). Bitcoin Mixing es un crimen para Departamento de Justicia de EE.UU. Antilavado de Dinero Recuperado de https://www.antilavadodedinero.com/bitcoin-mixing-es-un-crimen-para-departamento-de-justicia-de-ee-uu/ . 30 de octubre 2021. 2:34 pm.

Los debates entre el Gobierno y la comunidad de Bitcoin en México se intensifican. Bitcoin México. Recuperado de https://www.bitcoin.com.mx/los-debates-entre-el-gobierno-y-la-comunidad-de-bitcoin-en-mexico-se-intensifican/. 20 de junio de 2020, 5:45 pm.

Muller, Marion, (2013). ¿Qué es FinCEN: Financial Crimes Enforcement Network?. Recuperado de https://www.fincen.gov/ y de https://www.oroyfinanzas.com/2013/03/fincen-financial-crimes-enforcement-network/, 2 de noviembre 2021, 1:00 am.

Niebla de Bitcoin (2021). ¿Cómo usar Bitcoin Mixer (Btc Blender o Tumbler)? Recuperado de https://bitcoinfog.io/ 22 de noviembre de 2021 11:20 pm.

Nieto, A. (4 octubre 2017, actualizado 7 enero 2018) ¿Qué es una ICO? La tecnología que está revolucionando la financiación empresarial. Recuperado de https://www.xataka.com/empresas-y-economia/que-es-una-ico-la-tecnologia-que-esta-revolucionando-la-financiacion-empresarial. 10 de agosto de 2020, 14:00pm.

Oré Diego (8 de diciembre 2020). Latino American crime cartels turn to cryptocurrencies for money laundering. Reuters. Future of Money. Recuperado de https://www.reuters.com/article/mexico-bitcoin-insight-idUSKBN28I1KD 24 de noviembre 2021. falta hora

Oro y Finanzas (2015). ¿Qué es y qué significa FinTech? Recuperado de https://www.oroyfinanzas.com/2015/03/que-significa-fintech/. 15 de mayo de 2020. 4:00 pm.

Osborne, Ch. (23 de mayo 2019). Bestmixer es incautado por la policía por lavar $ 200 millones en criptomonedas contaminadas. Zdnet. Recuperado de https://translate.google.com/translate?hl=es-419&sl=en&u=https://www.zdnet.com/article/bestmixer-seized-by-eu-police-over-laundering-of-200-million-in-cryptocurrency/&prev=search&pto=aue 6 de noviembre

Responsabilidad Social Empresarial y Sustentabilidad, (S/F) ¿Qué son las empresas FinTech? Definición, tipos, objetivos y ejemplos. Recuperado de https://www.responsabilidadsocial.net/las-empresas-fintech-definicion-tipos-objetivos-ejemplos/ 13 de junio de 2020, 11:15 pm.

Rosic, A. (01 de 03 de 2019). What is Blockchain Technology? A Step-by-Step Guide For Beginners. Recuperado de Blockgeeks 20/04/RCP_https://blockgeeks.com/guides/what-is-blockchain-technology/. 08 de septiembre de 2019. Actualizado el 22 de septiembre de 2021 y consultado el 11 de octubre de 2021.

Schoenberg, T. (13 de mayo de 2021). Binance Faces Probe by U.S. Money-Laundering and Tax Sleuths. Bloomberg. Markets Crypto. Recuperado de https://www.bloomberg.com/news/articles/2021-05-13/binance-probed-by-u-s-as-money-laundering-tax-sleuths-bore-in . 6 de noviembre 2021. 9:00 am.

SHCP & CNBV. Grupo de Acción Financiera Internacional (GAFI). Recuperado de https://www.gob.mx/cms/uploads/attachment/file/80948/VSPP_GAFI___13042016.pdf 2021. 1:35 pm.

Sistema del Portal de Prevención de Lavado de Dinero SAT. Recuperado de (https://sppld.sat.gob.mx/pld/index.html),(https://www.cfatfgafic.org/index.php/es/documentos/gafi40-recomendaciones) y https://www.responsabilidadsocial.net/las-empresas-fintech-definicion-tipos-objetivos-ejemplos/. 9 de agosto de 2020, 9:00 am.

Solé, R (2021) Binance Coin (BNB): La criptomoneda de la exchange Binance. Profesional Review. Recuperado de https://www.profesionalreview.com/2021/07/03/que-es-binance-coin-bnb/ 20 de junio 2021 17:25 pm

Soto, F. (2021). Qué es la tecnología blockchain y cómo funciona. Recuperado de https://dev.to/fransotodev/que-es-la-tecnologia-blockchain-y-como-funciona-3ond . 26 de septiembre 2022. 11:21 pm

Unidad de Información y Análisis Financiero UIAF. Grupo de Acción Financiera Internacional (GAFI). Asuntos Internacionales. Recuperado en https://www.uiaf.gov.co/asuntos_internacionales/organizaciones_internacionales/grupo_accion_financiera_7114 . 15 de Junio, 2020 8:30 pm

Unidad de Inteligencia Financiera. Internacional. Gobierno de México, Recuperado de https://uif.gob.mx/es/uif/internacional 14 agosto 2021, 7:30 am

Unidad de Inteligencia Financiera (2022). Uso Ilícito de Activos Virtuales. Documento. Tipología. Recuperado de https://www.gob.mx/uif/documentos/tipologias-2022?idiom=es. 18 de Mayo, 2022.

United States Department of Justice (2017), Russian National And Bitcoin Exchange Charged In 21-Count Indictment For Operating Alleged International Money Laundering Scheme And Allegedly Laundering Funds From Hack Of Mt. Gox. Recuperado de https://www.justice.gov/usao-ndca/pr/russian-national-and-bitcoin-exchange-charged-21-count-indictment-operating-alleged . 11 de mayo 2021 15:25 pm

Vector ITC, Compañía de Softtek Company. Blockchai, disrupción, valor y seguridad. https://www.vectoritcgroup.com/wp-content/uploads/2018/06/Blockchain-Disrupci%C3%B3n-valor-y-seguridad.pdf.

ZDNet. Recuperado de https://thereaderwiki.com/es/ZDNet. 5 de noviembre 11:20 am.

Wikipedia. BTC-e. Recuperado de https://en.wikipedia.org/wiki/BTC-e. se editó por última vez el 26 de febrero de 2022 a las 00:56 (UTC)

Leyes

Banco de México. Circular 4/2019 Operaciones con activos virtuales de las instituciones de crédito e instituciones de tecnología financiera Sujetos obligados. Instituciones de crédito e instituciones de tecnología financiera. Recuperado de https://www.banxico.org.mx/marco-normativo/normativa-emitida-por-el-banco-de-mexico/circular-4-2019/circular-4-2019.html. 15 de marzo 2020. 11:20 pm.

GAFI. 40 Recomendaciones. Recuperado de https://www.cfatf-gafic.org/es/documentos. 16 de septiembre de 2021, 12:40 pm.

GAFI, 2020. Estándares Internacionales Sobre la Lucha Contra el Lavado de Activos, el Financiamiento del Terrorismo y el Financiamiento de la Proliferación de Armas de Destrucción Masiva. Recomendaciones. Recuperado de https://www.cfatf-gafic.org/es/documentos/recursos-del-gafic/14971-recomendaciones-del-gafi-2012-actualizadas-a-octubre-de-2020-1 . 16 de septiembre 2021 14:30 pm.

Decreto que expide la Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilicita. Diario Oficial (17 de Octubre, 2012). Recuperado dehttps://www.pld.hacienda.gob.mx/work/models/PLD/documentos/lfpiorpi.pdf el 2 de diciembre de 2021.

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. Diario Oficial de la Federación (9 de marzo 2018). Recuperado de https://www.pld.hacienda.gob.mx/work/models/PLD/documentos/LFPIORPI_Reforma090318.pdf. 3 de diciembre 2021.

Ley para regular las Instituciones de Tecnología Financiera (Ley Fintech). Publicada en el Diario Oficial de la Federación (9 de marzo 2018).

Normas APA. Pro. Guía resumen del Manual de Publicaciones con Normas APA Séptima Edición 2020. www.normpasapa.pro Traducción basada en: https://apastyle.apa.org/style-grammar-guidelines/index y en American Psychological Association (2020).

Guidance for a Risk-Based Approach to Virtual Currencies, June, 2015. Paris France.

Periódicos

González A. (3 de septiembre, 2016), Hasta 50 mil mdd al año se lava en el sistema financiero mexicano, l blanqueo de recursos de procedencia ilícita ha crecido, afirma director de TM Sourcing. La Jornada. Recuperado de https://www.jornada.com.mx/2016/09/03/economia/023n1eco 18 de febrero 2020.

Gutiérrez F. (13 de enero, 2020), Bajo la Optica del GAFI. Comienza el reto para regular y supervisar activos virtuales. El Economista. Economía. Recuperado de https://www.eleconomista.com.mx/economia/Comienza-el-reto-para-reular-y-supervisar-activos-virtuales-20200113-0084.html. 5 de agosto 2020, 11:30 pm.

Gutiérrez F. (10 de abril 2022) Unidad lo presenta como tipología. Caso Zaragoza, el referente para la UIF en materia de criptomonedas y lavado de dinero. El Economista. Sector Financiero. Recuperado de https://www.eleconomista.com.mx/sectorfinanciero/Caso-Zaragoza-el-referente-para-la-UIF-en-materia-de-criptomonedas-y-lavado-de-dinero-20220410-0023.html. 12 de abril 2022. 4:20. pm

Guzmán, K. (23 de enero 2020). Nvio Pagos, primera fintech con autorización para operar en México. Periódico Milenio. Recuperado de https://dplnews.com/nvio-pagos-primera-fintech-con-autorizacion-para-operar-en-mexico/. 18 de julio de 2020 9:35 am

Oré, D. (08 de diciembre 2020). Los cárteles del crimen latinoamericanos recurren a las criptomonedas para el lavado de dinero. El futuro del dinero. Reuters. Recuperado de https://www.reuters.com/article/mexico-bitcoin-insight-idUSKBN28I1KD. 13 de febrero 2021.

Pontaza, D. (28 de noviembre de 2018). Siete empresas se unen en pro del blockchain en México. La asociación Blockchain México promoverá el uso de esta tecnología

especialmente enfocada a remesas y transparencia. Expansión. Recuperado de https://expansion.mx/tecnologia/2018/11/28/siete-empresas-se-unen-en-pro-del-blockchain-en-mexico. 16 de septiembre 2021. 10:35 am.

Saldivar, B. (24 de septiembre 2020) Lavado de dinero representa 2.7% del PIB mundial. El lavado de dinero, a nivel mundial, representa 2.7% del Producto Interno Bruto (PIB), indicó el Panel sobre Responsabilidad, Transparencia e Integridad Financiera Internacional (FACTI, por su sigla en inglés) para lograr la Agenda 2030 de la ONU. El Economista. Recuperado de https://www.eleconomista.com.mx/internacionales/Lavado-de-dinero-representa-2.7-del-PIB-mundial-20200924-0129.html 25 de septiembre 2022. 11:00 am.