UNIVERSIDAD SAN FRANCISCO DE QUITO USFQ

Colegio de Jurisprudencia

Criptomonedas como medios comisorios de delitos de estafa y lavado de activos: Mecanismos para impedir el uso delictivo de las criptomonedas

Rafael Gabela Salvador

Director de Tesis
Xavier Andrade Castillo,

Trabajo de titulación como requisito para la obtención del título de Abogado

Quito 28 de mayo del 2019

UNIVERSIDAD SAN FRANCISCO DE QUITO

Colegio de Jurisprudencia

HOJA DE APROBACIÓN DEL TRABAJO DE TITULACIÓN

"Criptomonedas como medios comisorios de delitos de estafa y lavado de activos: Mecanismos para impedir el uso delictivo de las criptomonedas"

Rafael Gabela

Xavier Andrade
Director del Trabajo de Titulación

Santiago Escobar
Lector del Trabajo de Titulación

Fernando Flores
Lector del Trabajo de Titulación

Juan Pablo Aguilar
Decano del Colegio de Jurisprudencia (E)

Quito, julio del 2019

UNIVERSIDAD SAN FRANCISCO DE QUITO

EVALUACION DE DIRECTOR / TRABAJO ESCRITO TESINA

TESINA/TITULO: Criptomonedas como medios comisorios de delitos de estafa y lavado de activos: Mecanismos para impedir el uso delictivo de las criptomonedas.

ALUMNO: Rafael Gabela Salvador

EVALUACIÓN:

a) Importancia del problema presentado.

El movimiento *cypherpunk* de los años noventa, trajo consigo las criptomonedas y en ese contexto, efectos en el sistema financiero. De ello que, las criptomonedas son la base central del tema de estudio, y claro como consecuencia del desarrollo tecnológico de esta era digital, definitivamente, al tratarse de una conducta humana, entrará en las regulaciones del derecho penal, haciendo del tema algo nuevo, innovador y de proyección frente a las posibles conductas criminales de tipo económico que se darán (dan) por el uso de estas formas o medios de pago y sus implicaciones en el patrimonio tanto privado como público de los ciudadanos.

El presente trabajo de titulación, desarrolla el tema de estudio centrándose justamente en estos varios aspectos, esto es, desde la identificación de los *cypherpunks*, como un grupo de activistas con conocimiento en criptografía, que tenia miedo que el gobierno oprima a las masas mediante internet, Satoshi Nakamoto, en su artículo titulado el Bitcoin, planteó las ventajas de una moneda digital, y con ello crea la primera criptomoneda. También se hace un enfoque sobre las ventajas y desventajas de su uso, y el efecto que estas podrían plantear en sus diversas áreas, entre ellas la penal, lo que define de manera particular la importancia de este trabajo.

b) Trascendencia de la hipótesis planteada por el investigador.

La hipótesis del trabajo versa sobre los efectos jurídicos que las criptomonedas pueden producir en actividades comerciales o financieras, es decir, si tienen las características necesarias idóneas para ser usadas como medios comisorios de delitos (estafa-lavado de activos), por un lado, y por otro, los mecanismos necesarios y efectivos a implementar el control, de tal forma que se prevenga su uso delictivo. La hipótesis se base en la afirmación de lo fácil que puede convertirse este mecanismo de pago para engañar a las personas, por lo que recomienda los mecanismos idóneos para su prevención; primero, explicando que son las criptomonedas, sus alcances y usos, funcionamiento y operatividad, y su idoneidad para el fraude en delitos de estafas, y lo mismo la explicación de lo factible de su uso para lavar activos provenientes de delitos; y segundo, la experiencia de otros países para prevenir sus usos fraudulentos, vale decir, que el autor de este trabajo se encuentra a favor del mecanismo pero sostiene que deben crearse formas de prevención o control frente al abuso, lo que da la trascendencia a la hipótesis. El autor propone que con medidas expresas para combatir los "usos criminales de los criptoactivos", es posible evitar los delitos señalados ya que detener el desarrollo de la tecnología es imposible.

c) Suficiencia y pertinencia de los documentos y materiales empleados.

El trabajo refleja el uso de diversas fuentes y utiliza alrededor de 100 fuentes bibliográficas, de las cuales 16 son publicaciones nacionales, y unas pocas extranjeras, (Donna, Argentina). Debe hacerse notar que la mayoría de la información proviene de la web, que se entiende ya que una de las variables de estudio, pertenece al espacio cibernauta. Hay uso de doctrina sobre los tipos penales de estafa y lavado de activos. Además, recoge bibliografía de autores internacionales, encontrando obras que van en ediciones desde el año 1997 (Gutierrez Zarza), hasta el año 2018 (Wegberg Rolf), tanto en varios temas de delitos informáticos, defraudaciones, lavados de capitales y en su mayoría opiniones sobre delitos económicos y *bitcoins*, sumado a referencias normativas del COIP, Código Monetario y resoluciones de la Superintendencia de Bancos y Seguros, en temas generales como la parte especial de sus variables de estudio, es decir, la opinión académica, técnica y jurisprudencial de unos veinte años aproximadamente. Existe poca jurisprudencia nacional por lo nuevo de la discusión, sin embargo, hay evidencia de una amplia revisión de artículos, noticias, y catálogo de jurisprudencia a nivel internacional, como de tribunales internacionales o de países diversos. Así mismo, existe uso y referencia de normativa extranjera de países como Colombia, Inglaterra y España.

Los materiales bibliográficos y los documentos de soporte son complementados con información fidedigna obtenida de una gama amplia de páginas web, generando un adecuado, conveniente y correcto desarrollo estructural de contenidos sobre todos los temas y subtemas investigados.

d) Contenido argumentativo de la investigación (la justificación de la hipótesis planteada).

Desde la introducción el autor propone el problema, una hipótesis y una estructura clara de cómo será comprobada a lo largo del trabajo. El Primer Capítulo, plantea en general los orígenes de las criptomonedas, su naturaleza y funcionamiento. Aquí también se plantea, de manera general, su empleo como herramienta delictiva para realizar crímenes como el lavado de activos y el blanqueamiento de capitales. El autor expone el problema del uso de las criptomonedas dentro del sistema tecnológico que se vive en la actualidad, pero que, sin embargo, también añade características que hacen que esta moneda digital sea descentralizada y ayuda a mejorar le economía. Plantea que si bien los bitcoins ayudan de forma casi gratuita a realizar transacciones bancarias al instante, puede ser usada gracias a su caracterización de privacidad y anonimato, llevando a cabo, actos ilícitos sin conocer el autor de ellos. Señala y da la explicación técnica sobre las características de las criptomonedas, sus componentes y de la tecnología blockchain (pp. 6-10). Continúa explicando como funcionan los Bitcoins con cuadros ilustrativos. Parte de su explicación es sobre el uso de los prototipos de las criptomonedas, propuestas en 1998 de crear una moneda, digital y descentralizada, ofreciendo un método de pago entre dos interventores sin ningún intermediario, para que no haya un traslado de información personal a terceros mediante encriptaciones (pp. 6-10). Plantea una serie de ventajas a la vista del sistema financiero, tales como costos gratuidad y en transferencias de valor instantáneo velocidad inmediata de envió y recibimiento, hace transferencias sin importar la cantidad y es instantáneo

a comparación de una transacción bancaria (pp. 10-12). Agrega que el segundo grande aporte de los bitcoins es introducir a personas que no tenían cuentas bancarias al mundo monetizado, al no pedir nada más que una cuenta de correo electrónico para poder abonar tu cuenta. Señala que la tercera ventaja es la privacidad que tienen las personas y funciona similar al dinero metálico, y finalmente, la cuarta ventaja es transparencia y seguridad a los usuarios, para por último sumar que, el bitcoin es resistente a la inflación, estimando así valores de hasta 21 millones de bitcoins para el 2041. Hace un primer acercamiento de primeros usos de las monedas virtuales y las criptomonedas en la comisión de ilícitos, señala a los casos Liberty Reserve y Silk Road, para sustentar su tema (pp. 12-14) y termina con la "Problemática sobre el uso de las criptomonedas y los sistemas blockchain", explicando que con la aparición de la moneda electrónica, se dio paso a facilitar actos delictivos, por lo que supone un gran desafío para órganos de control y legisladores, regular esto, aclarando que los bitcoins no son ilícitos en su naturaleza, si no que el problema radica en la forma en como la gente los usa, es decir, como el medio de pago para cometer actos fraudulentos, como la estafa y el lavado de activos.

Es de relieve el Segundo Capítulo, cuando el autor refuerza su hipótesis exponiendo mediante doctrinas, que el uso de criptomonedas no es algo ilícito, pero el empleo de ellas en actos criminales, como los delitos denominados de cuello blanco (pp. 15-16) o delitos informáticos (pp. 17-18), son posibles, incluso como una característica del delito de estafa (pp. 18-19). Profundiza en el delito de cuello blanco, donde define que las personas de alta esfera económica realizan crímenes no violentos, pero es inmensa la posibilidad de incurrir en esta conducta por varios factores, detallando que son difíciles de detectar y de penar. Revisa en este capítulo a la ciberdelincuencia y sus componentes, señalando que son difíciles de entender, ya que para ello se necesita de la definición técnica del área informática frente al concepto de delito informático, y el uso de la tecnología para cometer crímenes. Estudia a la estafa y la apropiación fraudulenta por medios electrónicos, aclarando que el uso de *bitcoins* como medio de fraude cabe como una modalidad de estafa, más que el delito de apropiación fraudulenta por medios electrónicos (penalizado en otros países). Incluso hace algunas apreciaciones del empleo de *Initial Coin Offerings y Smart Contracts,* como medios para realizer fraude. Termina este capítulo con un amplio estudio del lavado de activos (pp. 30-37) incluso detallando la manera en como esta forma de monedas puede ser utilizadas como medio en este delito. Explica que es la nueva técnica para blanquear dinero, ya que es un tema donde las criptomonedas no dejan un rastro sólido para poder ratrear o perseguir, gracias a su anonimato, donde el lavado es hacer creer que algo es lícito -sin que sea verdad- por actividades criminales, mediante engaños para dar una imagen de licitud para dichas ganancias. Además, se resalta que, el lavado de activos, gracias a la criptomoneda, se ha vuelto el método ilícito más popular, ya que cuando se gana criptomonedas no se declara de donde vienen –su origen- o si es lícito. Explica al *mixer* o mezclador de monedas, al que define como la herramienta más eficaz para aumentar el anonimato de las criptomonedas, donde se mezclan o combinan con transacciones de otras personas en un banco central, llamado *blockchain*, y que como es obvio, al mezclarse todas las transacciones, no se sabe de dónde vinieron o sus orígenes, lo que implica que se vuelvan creíbles.

El Capítulo Tercero, se encuentra el panorama normativo internacional y posibles regulaciones aplicables (pp.40-57), el cual estudia la prohibición de las criptomonedas en el Ecuador o su regulación para poder ser admitidas. Señala las diferentes posiciones que han tomado los países

del mundo al momento de regular la criptomoneda. Señala a tres aproximaciones sobre el dilema de la criptomoneda, puntualizando que son: la inacción, la prohibición y la regulación. Defiende que con la regulación y experiencia de otros países se cumple con todo el objetivo de prevenir el uso delictivo de éstas. Fundamenta que los mecanismos de regulación que han tomado en países como Malta y EEUU, para reglar negocios relacionados con estas, son aceptables, y que el Ecuador también debería tomar medidas para prevenir sus usos ilícitos y quedarse en la inacción o prohibición. Incluso hace una interesante propuesta sobre la creación de una fiscalía especializada contra la ciberdelincuencia (p. 51), la ayuda de cooperación internacional (p. 53), y las medidas para evitar estafas y lavado de activos (p. 54) con lo que finaliza su investigación y comprueba su hipótesis de estudio.

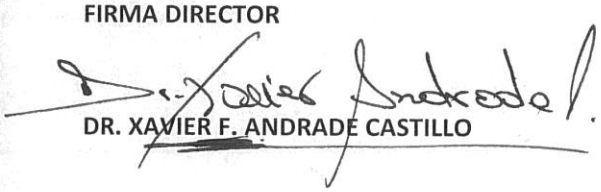
El Capítulo Cuarto termina con 10 conclusiones y recomendaciones.

e) Cumplimiento de las tareas encomendadas a lo largo del desarrollo de la investigación.

Este trabajo de investigación fue desarrollado durante cinco meses aproximadamente. Los diversos borradores del primer capítulo se presentaron en el mes de enero del 2019 y a los cuales se realizaron observaciones de forma y fondo. Así, en el Primer Capítulo se realizaron observaciones respecto a ampliaciones de temas y disminución de información sobre la historia y el origen de las criptomonedas, se sugirió la aplicación de citas y notas bibliográficas y pequeñas correcciones ortográficas. El Segundo Capítulo, fue entregado el 21 de febrero y su revisión el 28 del mismo mes. Las observaciones fueron respecto a incorporación de más citas, ampliación del fondo de los delitos de cuello blanco, del error como elemento de la estafa y el dolo, además de la ampliación de ideas propias y ejemplos. El Capítulo Tercero, se entregó el 3 de mayo y su revisión fue el 14 de mayo, donde se recomendó la eliminación de cierta información poco relevante de manera que se de prioridad a las variables de estudio, criptomonedas, medios comisorios, estafa, lavado de activos y los mecanismos de prevención en su uso, por lo que incluso hubo la necesidad de realizar la modificación del tema del trabajo de titulación en la medida de la investigación, los temas y subtemas tratados, sin alteración ni de la forma ni del fondo del trabajo. De esta forma, tras la revisión final y las correcciones a las observaciones realizadas se concluyó con el trabajo de investigación tras un proceso de aproximadamente 5 meses y medio.

Por último, se cumplieron todos los requerimientos de investigación y recomendaciones de tutoría, bibliografía mínima y metodología para el desarrollo de trabajos de titulación según las exigencias y reglamento de la USFQ, por lo que, lo apruebo.

FIRMA DIRECTOR



DR. XAVIER F. ANDRADE CASTILLO

© DERECHOS DE AUTOR

Por medio del presente documento certifico que he leído la Política de Propiedad Intelectual de la Universidad San Francisco de Quito y estoy de acuerdo con su contenido, por lo que los derechos de propiedad intelectual del presente trabajo de investigación quedan sujetos a lo dispuesto en la Política.

Asimismo, autorizo a la USFQ para que realice la digitalización y publicación de este trabajo de investigación en el repositorio virtual, de conformidad a lo dispuesto en el Art. 144 de la Ley Orgánica de Educación Superior.

Firma del estudiante:	----------
Nombre y apellidos:	Rafael Gabela Salvador
Código:	00116795
Cédula de Identidad:	1718721218
Lugar y Fecha:	Quito, 28 de mayo del 2019

Agradecimientos:

A mis padres, Rocío y Diego, por su apoyo incondicional y por ser las personas que me inspiran a mejorar día a día;

A mi hermano, Gabriel, porque somos los dos contra el mundo;

A mis profesores por los valiosos conocimientos que me han impartido;

A Xavier Andrade, por sus enseñanzas, compromiso y colaboración durante toda la carrera y en especial durante el desarrollo de este trabajo;

*A mis amigos de la facultad de derecho por todos los buenos momentos que hemos compartido***.**

Resumen

Las criptomonedas son un nuevo tipo de activos virtuales que han sido motivo de varias discusiones acerca de las repercusiones jurídicas que su surgimiento conlleva. Las características intrínsecas de las criptomonedas de anonimidad, descentralización e independencia frente a intermediarios tales como instituciones financieras o gobiernos han provocado que sean empleadas en la comisión de delitos. El presente trabajo de investigación busca dilucidar los componentes y propiedades esenciales de las criptomonedas y exponer los métodos por los cuales los criminales utilizan las criptodivisas para la ejecución de sus actividades delictivas. De igual manera, busca formular propuestas de medidas que se deben implementar para la prevención y persecución de los delitos cometidos a través del uso de las criptomonedas.

Abstract

Cryptocurrencies are a new type of virtual assets that have been the subject of several discussions about the legal repercussions that their emergence entails. The intrinsic characteristics of cryptocurrencies of anonymity, decentralization and independence from intermediaries such as financial institutions or governments have caused them to be used in the commission of crimes. This research work seeks to elucidate the components and essential properties of cryptocurrencies and expose the methods by which criminals use cryptocurrency for the execution of their criminal activities. Similarly, it seeks to formulate proposals for measures that must be implemented for the prevention and prosecution of crimes committed through the use of cryptocurrencies.

Tabla de contenidos

INTRODUCCIÓN

En las sociedades del siglo veintiuno, debido a que vivimos en una era digital, el cambio es una constante. El surgimiento de nuevas tecnologías hace que cada aspecto de nuestras vidas este en perpetuo desarrollo y transformación. El Derecho, al ser la ciencia que reglamenta las actuaciones humanas, se ve obligado a establecer normas que regulen estas nuevas tecnologías, a pesar de que, dado la naturaleza cambiante de estas, el Derecho siempre va ir un paso detrás. Ahora el Derecho se enfrenta a una nueva tecnología: las criptomonedas.

En los últimos años el fenómeno de las criptomonedas ha crecido de forma vertiginosa. Las innovaciones tecnológicas que proporcionan frente a los medios de pago tradicionales y la alta rentabilidad que han obtenido algunos inversionistas a través de las criptomonedas han fomentado la popularidad y expansión de esta nueva tecnología. Las criptodivisas son un medio digital de intercambio relativamente nuevo que empezó a operar con Bitcoin en 2009. Estas monedas virtuales obtienen su nombre por su naturaleza encriptada, ya que están protegidas a través de codificación, es decir son anónimas[1]. Utilizan un sistema de transacciones descentralizados conocido como *blockchain* y por lo tanto no son controladas por un banco o gobierno. El intercambio de estas se da de forma directa entre usuario a usuario lo que las hace no depender de instituciones financieras o gubernamentales como intermediarios. Los defensores de esta nueva tecnología afirman que las criptomonedas son la nueva gran revolución tecnológica, ya que agilitan y simplifican las transferencias de valor, reducen los costos de las transacciones, proveen seguridad y transparencia, y son resistentes a fenómenos económicos que afectan al dinero fiduciario como la inflación. Por el otro lado, los detractores de esta nueva tecnología creen que su uso principal es como medio comisorio de ilícitos; su anonimidad y descentralización han proporcionado a los criminales una nueva forma de encubrir y ocultar sus transacciones.

[1] Algunos autores sostienen que no es correcto hablar de anonimidad en sentido estricto, ya que consideran que hay ciertas criptomonedas que son seudónimas dado la existencia de datos vinculados al emisor y receptor de las transacciones (direcciones o llaves públicas de dichas criptomonedas). *Vid*. Xesús Pérez López. "Las Criptomonedas: consideraciones generales y empleo de las criptomonedas como instrumento de blanqueo de capitales en la Unión Europea y en España". *Revista de Derecho Penal y Criminología* 3/18 (2017), pp.141-187.

Esta es una tecnología aún embrionaria la cual no se encuentra regulada en la gran mayoría de legislaciones. Esto significa que la percepción sobre la idoneidad de las criptomonedas como medios comisorios de ilícitos varia de país a país; aún no hay claridad acerca de cuáles son los verdaderos riesgos que presentan las criptomonedas como facilitadoras de la comisión de delitos. La realidad es que tanto los partidores como los opositores de las criptomonedas tienen razón en algunas cosas y se equivocan en otras.

Por lo tanto, el problema jurídico que tratara esta tesis se lo puede desarrollar en las siguientes preguntas: ¿acaso las criptomonedas poseen características que les hacen herramientas útiles para ser medios comisorios de ilícitos?, si este es el caso entonces ¿qué ilícitos son los que se ejecutan con la asistencia de criptomonedas?, ¿qué métodos utilizan los criminales para cometer estos delitos coadyuvados por esta tecnología?, y finalmente, ¿que medidas o mecanismos se pueden implementar para minimizar el uso ilícito de las criptodivisas? La hipótesis de este trabajo es demostrar que las criptomonedas poseen características inherentes que facilitan la comisión de delitos, en especial son muy eficientes para la ejecución de los delitos de estafa y lavado de activos, y por lo tanto se deben implementar mecanismos prevenir su uso delictivo.

Para fundamentar la hipótesis del trabajo el primer capítulo expondrá los orígenes de las criptomonedas, su naturaleza y funcionamiento y su relación con la comisión de ilícitos. Se analizará la ideología detrás de la creación de las criptomonedas y los sucesos cruciales que dieron paso a la aparición de estas monedas virtuales. Se prosigue a detallar las propiedades técnicas del funcionamiento y operación de las criptomonedas y del *blockchain.* Luego se presentará como las criptomonedas y otras monedas digitales han sido usadas para la perpetración de crímenes mediante la exposición de los casos Silk Road y Liberty Reserve. El segundo capítulo profundizará sobre la estafa y lavado de activos, los dos delitos llevados a cabo por los cibercriminales de forma más reiterada asistidos por el uso de las criptomonedas. En este capítulo se explicará los conceptos doctrinarios de delitos de cuello blanco y delitos informáticos ya que su entender es crucial para asimilar como se corresponder estos dos conceptos a los tipos penales antes mencionados. Haré una aproximación a la estructura típica de los delitos de estafa y lavado de activos por medio de apreciaciones doctrinarias de importantes autores, lo que permitirá identificar los elementos objetivos y subjetivos típicos de estos delitos. Para concluir este capítulo, se presentará algunos métodos por los cuales los criminales se

sirven de las criptomonedas para llevar a cabo los ilícitos de lavado de activos y estafa. Finalmente, en el tercer capítulo examinaré las diferentes posturas que han tomados los países a la hora de tratar con el dilema que representan las criptodivisas. Se proveerá argumentos para determinar qué postura es la adecuada para prevenir los usos delictivos de las criptomonedas. Finalmente se expondrá las medidas que el Ecuador debe implementar para combatir los usos criminales de los criptoactivos.

1. CAPÍTULO I: ANTECEDENTES HISTÓRICOS Y CONCEPTOS

Este capítulo desarrolla los orígenes de las criptomonedas, su naturaleza y funcionamiento, y su relación con la comisión de ilícitos. El propósito fundamental de este capítulo recae en sentar la base conceptual que sustenta la hipótesis de la presente tesis. Se presentará una crónica de hechos históricos que permitieron el surgimiento de las criptomonedas en el mercado mundial y se identificará la ideología subyacente de las criptomonedas al provenir estas de las ideaciones del movimiento *cypherpunk.* Posteriormente se detallará los aspectos técnicos del funcionamiento y operación de las criptomonedas y, sus ventajas frente al sistema financiero vigente. Finalmente se expondrá sobre el empleo de las criptomonedas y otras monedas digitales en la ejecución de actos delictivos a través de la presentación de los casos de Liberty Reserve y Silk Road.

1.1 Origen y desarrollo histórico de las criptomonedas

El génesis de las criptomonedas surge del movimiento *cypherpunk* de principios de los años noventa. En palabras de Julian Assange, una de las principales figuras de este movimiento, un *cypherpunk* es "un activista que utiliza la criptografía como forma de acción directa no violenta para alcanzar un cambio político y social"[2]. Los *cypherpunks* en sus comienzos eran un grupo de activistas con altos conocimientos de criptografía, informática y programación que estaban muy preocupados por la posibilidad de que el gobierno utilice el internet como mecanismo de represión en contra de las personas y viole su privacidad y libertad personal. Un pequeño grupo de este conglomerado de activistas, los miembros de *cryptography mailing list*[3], constantemente hablaban sobre la necesidad y la posibilidad de que una divisa digital fuera anónima o pudiera anonimizarse usando criptografía. Y esta es precisamente la base ideológica de las criptomonedas. El objetivo del grupo de *cryptography mailing list* era de crear una divisa electrónica

[2]Julian Assange, Jacob Appelbaum, Andy Muller-Maguhn, y Jeremie Zimmermann. *Cypherpunk:. La Libertad y el Futuro de Internet.* Barcelona: Deusto, (2012), p.15.

[3] La *cryptography mailing list* era una lista de correo creada por Tim C. May y John Gilmore con el propósito de entablar comunicación con otros miembros del movimiento *cypherpunk* con la aspiración de intercambiar ideas para la creación de un protocolos o sistemas que hagan posible la elaboración de una divisa virtual descentralizada, entre los miembros más importantes que se encontraban dentro de la *cryptography mailing list* estaban David Chaum (creador de Digicash), Hal Finney (desarollador de R PoW), Phil Zimmermann (desarrollador de PoP encryption), Wei Dai (creador de B money), Nick Szabo (creador de Bit Gold), Adam Back (creador Hash cash) y Satoshi Nakamoto (creador de Bitcoin) *víd* Nikolei M. Kaplanov. "Nerdy Money: Bitcoin, The Private Digital Currency, and The Case Against its Regulation" Loyola Consumer Law Review Vol.25 (2012), pp. 12-45.

descentralizada que fuera empleada como una alternativa al dinero fiduciario emitido por los gobiernos. Las características que debía poseer esta moneda debían ser las siguientes: (1) que se sea anónima, (2) descentralizada y, (3) el intercambio entre los usuarios de esta moneda digital tenía que ser directo y no depender de instituciones bancarias o financieras como intermediarios[4].

Antes de la creación de las criptomonedas, los *cypherpunks* desarrollaron varios prototipos de divisas electrónicas tales como BitGold, B Money y DigiCash. Estos primeros prototipos no funcionaron por los siguientes factores: (1) no existía el desarrollo tecnológico adecuado para implementarlas de forma funcional (2) el internet todavía no estaba integrado totalmente al comercio internacional y, (3) no existía un mercado de personas dispuestas a adquirir estos productos porque no veían una necesidad real de apartarse de las monedas de curso legal a las cuales ya estaban familiarizadas[5]. El sueño *cypherpunk* de la divisa electrónica ajena a cualquier gobierno o institución parecía una utopía. Sin embargo, un evento sentó las bases para que ese sueño se materialice. Ese acontecimiento fue la crisis financiera del 2008.

En el año 2008 se desató una crisis económica mundial producto del desplome del mercado financiero de los Estados Unidos. El origen de esta crisis se debe principalmente a que en los principios de la década del 2000 los bancos y las instituciones financieras crearon las hipotecas *subprime* como un tipo de producto financiero estructurado para obtener grandes beneficios económicos a, lo que en un principio se creyó, un riesgo muy bajo[6]. Estás eran hipotecas de tasa de interés variable que estaban orientadas a usuarios con malos historiales crediticios y precarios recursos económicos; de modo que estos usuarios suponían un alto riesgo de morosidad en los pagos de dichas hipotecas[7]. Los bancos e instituciones financieras obtuvieron grandes ganancias a través de estas hipotecas, pero crearon una burbuja financiera que estalló ya que a finales del año 2007 millones de deudores entraron en morosidad de forma simultánea al no poder pagar los

[4]Julian Assange, Jacob Appelbaum, Andy Muller-Maguhn, y Jeremie Zimmermann. *Cypherpunks: La Libertad y el Futuro de Internet. Óp. cit.*, p.23.
[5]Julie Pitta. *Requiem for a Bright Idea*. https://www.forbes.com/forbes/1999/1101/6411390a.html#436b692715f6 (acceso: 22/1/2019).
[6] Jesús Zurita Gonzáles, Juan Froilán Martínez Pérez, y Francisco Rodríguez Montoya. "La crisis financiera y económica del 2008. Origen y consecuencias en los Estados Unidos y México". *Revista El Cotidiano*, núm. 157, septiembre- octubre, (2009), pp. 17- 27. Universidad Autónoma Metropolitana Unidad Azcapotzalco. Distrito Federal, México.
[7]Ron Rimkus. *The Financial Crisis of 2008.* https://www.econcrises.org/2016/08/17/the-financial-crisis-of-2008/ (acceso: 23/1/2019).

intereses de las hipotecas[8]. Muchos bancos, empresas y otras instituciones financieras comenzaron a quebrar tales como Circuit City, Washington Mutual y la famosa Lehman Brothers[9]. Frente a la crisis, la Reserva Federal de los Estados Unidos intervino y comenzó a hacer préstamos de emergencia a los bancos a través del Programa TARP[10], conocido coloquialmente como el Rescate Bancario.

El rescate bancario fue duramente criticado por la población estadounidense ya que muchas familias quedaron en la quiebra y perdieron sus viviendas mientras veían como el gobierno rescataba a los bancos y empresas que habían sido los principales causantes de la crisis[11]. La indignación en el país norteamericano aumento cuando observaron que no se tomaron medidas legales para condenar a los responsables de la ruina económica. Todos estos factores condujeron a que muchas personas sintieran desconfianza y repudio de las instituciones financieras y bancarias; de repente, las ideas que tenían los *cypherpunks* parecían alineadas con el sentir de la población, ahora las criptomonedas parecían factibles de implementar en el mercado. Dos semanas después de la quiebra de Lehman Brothers un usuario en la *criptography mailing list*, cuya verdadera identidad aún sigue siendo un misterio, Satoshi Nakamoto, púbico un artículo titulado Bitcoin: Un Sistema de Efectivo Usuario-a- Usuario proponiendo un protocolo informático para crear la primera criptomoneda[12].

1.2 Explicación técnica sobre las características de las criptomonedas, sus componentes y de la tecnología *blockchain*

1.2.1 Cómo funciona Bitcoin

Para el desarrollo del Bitcoin, Satoshi Nakamoto utilizó las ideas base de los prototipos y precursores de las criptomonedas, en especial se fijó en las ideas de Wei Dai que ya había propuesto la idea en 1998 de crear una moneda virtual anónima utilizando criptografía en la *criptography mailing list*[13], En esencia las criptomonedas son monedas

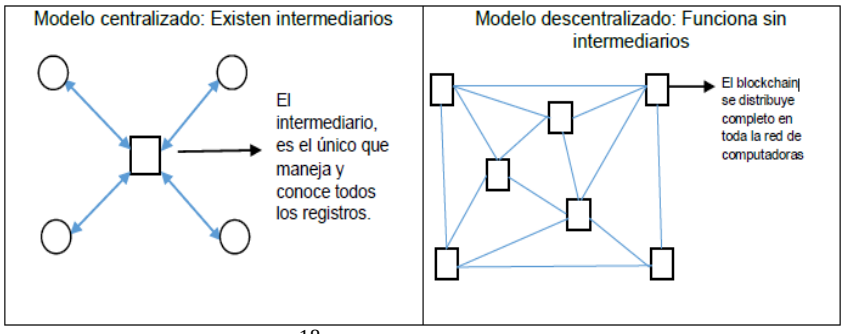
[8] *Ibíd.*
[9] *Ibíd.*
[10]Programa de Alivio de Activos Problemáticos. TARP: Troubled Assets Relief Program. A través de este programa se destinó USD $ 700 mil millones para rescatar a los bancos y apuntalar otros sectores de la economía tales como los fabricantes de automóviles, y a multinacionales como AIG
[11]Austin Murphy. *An Analysis of the Financial Crisis of 2008: Causes and Solutions.* https://ssrn.com/abstract=1295344 or http://dx.doi.org/10.2139/ssrn.1295344 (acceso: 23/1/2019).
[12]Satoshi Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System*. https://bitcoin.org/bitcoin.pdf (acceso: 23/1/2019).
[13] *Ibíd.*

virtuales que operan por un sistema de pagos descentralizado que emplea el método "peer-to-peer" (P2P)[14]. El Bitcoin ofrece un medio de transferencias de valor entre dos usuarios sin la participación de un intermediario. Las criptomonedas no poseen reconocimiento como moneda de curso legal, se desempeñan sin la injerencia de una autoridad gubernamental o de institución bancaria, su uso se realiza mediante la utilización de una red distribuida a nivel mundial[15]. Las transacciones entre pares están encriptadas para evitar que ocurra un traslado de información personal de los usuarios; es decir, las transferencias son anónimas. Todas las transacciones son almacenadas en un registro global, un libro contable mayor que es público para todos los usuarios, el *blockchain*[16]. A continuación, analizaremos las características del Bitcoin a profundidad.

Según los autores Lara y Muñoz el sistema Bitcoin cumple su función de descentralización de la siguiente manera:

> […] el sistema puede operar bajo una base de datos distribuida. Esta base de datos es conocida como la cadena de bloques o Blockchain que funciona como un libro contable descentralizado donde se registran todas las transacciones de la red. El Blockchain se distribuye completo en todos los nodos de la red, lo que le confiere una de sus principales características, no hay una entidad o banco central que regule este sistema monetario, sino que todo está manejado por una serie de computadoras descentralizadas[17].

La gráfica siguiente ilustra el modelo de distribución de la plataforma Blockchain:



Fuente: (Lopez, 2015)[18]

El sistema Bitcoin depende de que personas utilicen los procesadores de sus computadoras para generar bitcoins, a este proceso se lo conoce como *mining* o minado

[14] Omri Marian. "Are Cryptocurrencies 'Super' Tax Havens?" 112 Michigan Law Review First Edition (2013), p. 38.
[15] *Ibíd.*
[16] *Id.*, p. 14.
[17] John Alexander Lara Lara y Manuel Alejandro Muñoz Agudelo. "Análisis de los Principales Elementos del Bitcoin como Criptomoneda y Producto Commodity en el Comercio Nacional". Universidad Lasalle (2017), pp. 4 y sic.
[18] Alejandro López. (2015). *Implicaciones jurídicas del uso del bitcoin en Colombia. Validez del contrato de compraventa comercial con bitcoins.* Universidad de Nariño. pp. 18-22.

de Bitcoins. Según Lara y Muñoz la forma como trabajan los mineros consiste en ejecutar "en sus máquinas software para resolver complejos cálculos matemáticos (llamados hashes) basados en criptografía con el fin de procesar y validar las transacciones"[19]. Cuando estos cálculos se resuelven, se los ingresa a un bloque que contiene el registro de aproximadamente 2000 transacciones; el minero que crea el bloque lo que hace es agregar dicho bloque a la cadena del libro contable, esta información es entonces enviada a todos los usuarios de la red para que aprueben el contenido de esta[20]. Para que el bloque sea aceptado tiene que contar con la aprobación del 51% de los mineros en la red. Si el bloque no contiene errores y no es un bloque fraudulento, el bloque se añade correctamente al *blockchain* y el minero recibe una recompensa de 12 bitcoins por su trabajo. Cada bloque muestra de manera cronológica todas las transacciones que se han realizado donde se incluyen los datos de emisor, receptor, cantidad de la transferencia, el día, la fecha, y la hora[21].

De acuerdo a las autoras Acevedo y Rodríguez hay 3 tipos de *blockchain*:

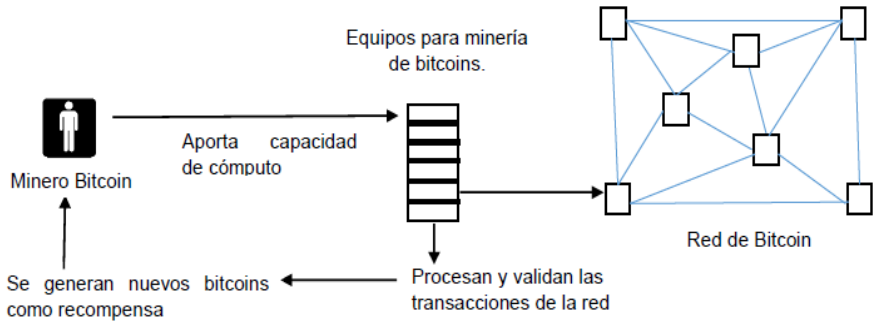
> **1. Blockchain público:** En la red pública o completamente descentralizada, cualquier persona puede introducir ordenes en el sistema, cualquier persona puede crear bloques y participar en el proceso de validación. La confianza de este sistema se basa en la actividad de minería. ***Este sistema es la base de gran parte de las criptomonedas.***
> **2. Blockchain en forma de consorcio:** Difiere en el mecanismo de validación de los bloques. En ese caso, una serie de nodos preseleccionados son los encargados de validar las transacciones, y no cualquiera. Se considera que es un sistema parcialmente descentralizado.
> **3. Blockchain privada:** En este caso, la escritura está centralizada en una sola empresa u organización. La lectura de dichas operaciones puede ser pública o limitada en función de la decisión de la organización primera[22]. (lo resaltado me pertenece)

El hecho de que todas las transacciones consten en el historial de *blockchain* el cual está registrado en todos los nodos del sistema hace que sea imposible el doble gasto, de esta forma el sistema *blockchain* proporciona seguridad a los usuarios de que no haya posibilidad de falsificar una transacción[23].

La siguiente gráfica muestra el proceso de minería de Bitcoins:

---

[19] *Ibíd*.
[20] Stephen Small. "Bitcoin: The Napster or Currency", 37 Hous. J. Int'l L. 581 (2015), p. 5.
[21] *Ibíd*
[22] Eliana Acevedo y Raíza Rodríguez. "Análisis del Bitcoin como técnica usada para el blanqueo de capitales en el sistema de Panamá". III Congreso Investigación, Desarrollo e Innovación de la Universidad Internacional de Ciencia y Tecnología (2018), pp. 231-253.
[23] Nikolei M. Kaplanov. "Nerdy Money: Bitcoin, The Private Digital Currency, and The Case Against its Regulation" *Óp. cit.*, pp. 12-24.



Fuente (López 2015)[24]

Todos los usuarios que deseen enviar o recibir bitcoins necesitan crear una cartera Bitcoin conocida como *Bitcoin wallet.* Según la explicación que proporciona el autor Small:

> Estas billeteras digitales contienen una clave pública y una clave privada (conocidas como *keys*); la clave pública es similar a una dirección de correo electrónico que un usuario compartirá con otros usuarios de Bitcoin para que puedan enviar bitcoins. Alternativamente, la clave privada es similar a un número pin para una tarjeta de débito, cuyo propósito es confirmar que un usuario desea gastar bitcoins en su cartera[25].

Uno puede adquirir criptomonedas como pago por bienes o servicios, de igual forma uno puede obtener bitcoins de *exchangers* (físicos o virtuales) que son empresas cuya función es intercambiar estas criptomonedas por otras criptomonedas o por dinero fíat (euros, dólares, yens, pesos, etc)[26]; estas empresas operan de forma similar a las casas de cambio. Otro método en el cual un usuario puede obtener bitcoins utilizando dinero en efectivo es mediante el uso de cajeros automáticos de Bitcoin, los cuales usualmente también permiten hacer transacciones con otras criptomonedas. Estos cajeros automáticos permiten comprar bitcoins mediante el depósito de dinero en efectivo o de realizar transacciones directamente en dichos cajeros[27].

El Bitcoin se valora según la oferta y demanda que exista en el mercado; al ser descentralizado este es el único factor que determina su valor[28]. La demanda de criptomonedas generalmente crece cuando se dan acontecimientos que se piensa que

---

[24] Alejandro López. (2015). *Implicaciones jurídicas del uso del bitcoin en Colombia. Validez del contrato de compraventa comercial con bitcoins. Óp. cit.*, pp. 22-23.
[25] *Id*. p.7.
[26] Instituto Nacional de Tecnologías de la Comunicación INTECO. *Bitcoin una moneda Criptográfica*.https://www.incibecert.es/sites/default/files/contenidos/estudios/doc/int_bitcoin.pdf (acceso: 23/1/2019).
[27] Grupo BTC. *El Bitcoin.* (2016), p. 7.
[28] Bitcoin Foundation. *FAQ*. https://bitcoin.org/es/faq#seguridad (acceso: 24/1/2019)

pueden crear inestabilidad de la economía de algún país o de la economía global[29]. Por el contrario, el valor del Bitcoin y otras criptomonedas baja cuando ocurren acontecimientos que afectan la credibilidad de las criptomonedas como un sistema seguro y fiable[30].

1.2.2 Ventajas del Bitcoin

Bitcoin posee una serie de ventajas frente al sistema financiero actual. En primer lugar, el sistema *blockchain* hace que los costos de las transacciones sean prácticamente gratuitos y la transferencia de valor es instantánea; mientras que las transacciones en el sistema financiero están sujetas a comisiones y cobros de porcentajes elevados y, debido a la centralización, la validación de una transacción o transferencia se demora mucho más[31]. Bitcoin posee la habilidad de hacer transferencias sin importar el tamaño de dicha transferencia, por ejemplo, enviar cinco o diez dólares de una cuenta a otra en diferentes continentes es posible mientras que, en el sistema financiero actual, la misma transferencia no sería posible por el elevado porcentaje de comisión que cobraría la institución financiera que esta de intermediario de la transacción. La segunda ventaja que proporciona Bitcoin es que permitiría que millones de personas que no se encuentran bancarizadas puedan participar en el mercado financiero[32]. Al no pedir ningún tipo de requisitos más que una cuenta de correo electrónico esto facilitaría a millones de personas a poder hacer transferencias de dinero, recibir remesas y hacer depósitos y extracciones en cajeros automáticos[33]. La tercera ventaja que ofrece Bitcoin es privacidad a sus usuarios en sus compras, aquí el bitcoin actúa de forma similar al dinero en metálico. Según los autores Lara y Muñoz "[e]sta privacidad puede ser deseable en cualquier

[29] Ejemplo de esto son la elección presidencial de Donald Trump que ocasionó la caída de varios mercados de valores tales como el europeo que cayo 4%; sin embargo, Bitcoin subió de valor en un 21% a consecuencia de este evento. Otros eventos que han ocasionado que Bitcoin suba de valor considerablemente han sido Brexit y la creciente popularidad del partido de extrema derecha holandés liderado por Geer Wilders *víd.* Cristina Fernández Esteban. *Por qué sube y baja el precio del Bitcoin.* https://www.ticbeat.com/innovacion/fintech/por-que-sube-y-baja-el-precio-del-bitcoin/ (acceso: 24/1/2019).; y RCN noticias. *Mercados Financieros caen tras inesperada elección de Trump como presidente de EE.UU.* https://noticias.canalrcn.com/internacional-economia/mercados-financieros-caentrasinesperada-eleccion-trump-presidente-eeuu (acceso: 24/1/2019).

[30] Por ejemplo, en 2014 el hackeo de la casa de cambio de criptomonedas más grande del mundo Mt Gox, que represento una pérdida de 460 millones de dólares avaluados en bitcoins, y la posterior quiebra de dicha empresa ocasionar que el valor de Bitcoin baje en un 53%. El hackeo de Ethereum, la segunda criptomoneda más usada en el mundo después de Bitcoin, ocasiono que la mayoría de criptomonedas en el mercado pierdan entre el 40 al 80% de su valor de mercado. *víd.* Cristina Fernández Esteban. *Por qué sube y baja el precio del Bitcoin. Óp. cit.*

[31] Grupo BTC. *El Bitcoin. Óp. cit.*, p.7.

[32] Instituto Nacional de Tecnologías de la Comunicación INTECO. *Bitcoin una moneda Criptográfica. Óp. cit.*

[33] Joseph A. Mann. *El Desafío de Llegar a la Población no Bancarizada.* http://latintrade.com/es/el-desafio-de-llegar-a-la-poblacion-no-bancarizada/ (acceso: 26/1/2019).

ámbito, pero sobre todo en cuestiones especialmente personales como sexualidad, creencias o salud.[34]" La cuarta ventaja que aporta Bitcoin a través de su sistema de *blockchain* es transparencia y seguridad en las transacciones al ser todas estas almacenadas en un registro público que esta replicado en todos los nodos de la red[35]. Por último, el Bitcoin es resistente a la inflación ya que, como el oro o la plata, existe un número finito de bitcoins. A diferencia del dinero fíat que puede ser impreso de forma indefinida por un banco central, el sistema bajo el que opera Bitcoin está programado para emitir un total de 21 millones de bitcoins algo que se calcula que sucederá en el año 2041[36]. Sin embargo, muchos expertos señalan que a pesar de que Bitcoin sea resistente a la inflación esto no evita que pueda ser perjudicado por un proceso de deflación debido factores tales como que existe un número límite establecido para la circulación total de bitcoins, que la mayoría de usuarios acaparan bitcoins porque especulan con ellos y porque hay una reducción progresiva del ritmo de emisión de los bitcoins en el proceso de minado[37]. Todas las características antes mencionadas hacen que esta tecnología sea ideal para la transferencia de dinero, pero esto es apenas la primera aplicación que se ha dado uso para esta nueva tecnología. Se espera que en el futuro los usos para las criptomonedas y los sistemas blockchain crezcan de forma exponencial.

Sin lugar a dudas las criptomonedas con su innovadora tecnología disponen de una serie de ventajas que tienen el potencial de transformar la economía mundial, sin embargo, las características que poseen también las convierten un instrumento para la comisión de delitos. De hecho, las criptomonedas saltaron a la fama global a raíz de que los investigadores del FBI descubrieron en el 2011 que el mercado negro virtual llamado Silk Road conducía todas sus transacciones utilizando la moneda Bitcoin, ya que dichas transacciones requerían ser descentralizadas y anónimas[38]. Cada día se descubre que las criptomonedas son empleadas en formas cada vez más novedosas para cometer ilícitos que van desde el lavado de activos, financiamiento del terrorismo, compraventa de armas

[34] John Alexander Lara Lara, Manuel Alejandro Muñoz Agudelo. "Análisis de los Principales Elementos del Bitcoin como Criptomoneda y Producto Commodity en el Comercio Nacional". *Óp. cit*., pp. 4 y sic.
[35] Paul Vigna y Michael Casey. *The Age of Cryptocurrency: How Bitcoin and Digital Money are Challenging the Global Economic Order*. Editorial St Martin´s Press (2015), p. 44.
[36] Nikolei M. Kaplanov. "Nerdy Money: Bitcoin, The Private Digital Currency, and The Case Against its Regulation". *Óp. cit.*, p. 24.
[37] Bit2Me. *¿Por qué el Bitcoin tiende a la deflación?* https://academy.bit2me.com/deflacion-en-bitcoin/ (acceso: 26/1/2019).
[38] Andrew Greenberg. *Silk Road 2.0 Launches, Promising A Resurrected Black Market Fort the Dark Web*. https://www.forbes.com/sites/andygreenberg/2013/11/06/silk-road-2-0-launches-promising-a-resurrected-black-market-for-the-dark-web/#6f9bb4535714 (acceso: 26/1/2019).

y drogas en mercados negros, evasión fiscal, ataques *ransomware*, *pharming, phishing*, fraude informático, hasta la estafa.

1.3 Las criptomonedas y el mundo criminal

1.3.1 Primeros usos de las monedas virtuales y las criptomonedas en la comisión de ilícitos; casos Liberty Reserve y Silk Road

Antes de la creación de las criptomonedas, otras monedas virtuales también fueron empeladas en la comisión de ilícitos. De hecho, el caso más grande de lavado de activos por medios electrónicos de la historia involucro una moneda virtual como medio para la ejecución de dicho delito, esa moneda era la "LR" de la compañía Liberty Reserve[39]. Liberty Reserve era "una compañía de procesamiento de pagos y transferencias de divisas con sede en Costa Rica[40]", la cual fue acusada por haber realizado blanqueo de capitales por un total estimado de 6 mil millones de dólares de los Estados Unidos de América a través de 55 millones de transacciones por internet[41].

Según los autores Brill y Keene, Liberty Reserve operaba de la siguiente manera:

> Para abrir una cuenta de Liberty Reserve y canjear las monedas LR, se les solicitaba a los usuarios que proporcionen solo una dirección de correo electrónico activa, indiferentemente de que sea anónima. A diferencia de los bancos o entidades financieras legítimas, Liberty Reserve no verificaba la identidad de sus usuarios y por una tarifa adicional de 75 centavos de dólar estadounidense por transacción, la "tarifa de privacidad", esta compañía ocultaba el número de cuenta de dichos clientes en las transacciones haciendo que la transferencia sea completamente imposible de rastrear. Los usuarios de Liberty Reserve debían realizar depósitos o retiros mediante el uso de *Exchangers* (intercambiadores/ casas de cambio), lo que permitía a Liberty Reserve evitar la recopilación de información sobre sus usuarios a través de transacciones bancarias u otra actividad que dejara un rastro centralizado de información financiera. El *Exchange* convertiría las LR en monedas de curso legal para transferirlas a la cuenta bancaria del beneficiario. Los *Exchangers* de Liberty Reserve tendían a ser negocios de transferencia de dinero sin licencia, que operaban sin una supervisión o regulación gubernamental significativa, concentrados en Malasia, Rusia, Nigeria y Vietnam[42]. (traducción libre)

El sistema por el cuál operaba Liberty Reserve presentaba muchas de las propiedades que poseen los sistemas que actúan con criptomonedas. Las características que ambos

[39] Allan Brill y Lonnie Keene. "Cryptocurrencies: The Next Generation of Terrorist Financing?". *Defence Against Terrorism Law Review. Vol 6. No. 1, Spring & Fall* (2014), pp. 7- 30.
[40] *Ibíd.*
[41] Marc Santora, William K. Rashbaum, y Nicole Perlroth. *Online Currency Exchange Accused of Laundering $6 Billion*. https://www.nytimes.com/2013/05/29/nyregion/liberty-reserve-operators-accused-of-money-laundering.html (acceso: 27/1/2019).
[42] Allan Brill y Lonnie Keene. "Cryptocurrencies: The Next Generation of Terrorist Financing?". *Defence Against Terrorism Law Review. Óp. cit.*, pp. 7- 30.

sistemas comparten son el anonimato, alcance global, velocidad, facilidad de uso y la dificultad de seguimiento por parte de las autoridades[43].

Como se mencionó anteriormente, las criptomonedas adquirieron notoriedad en el año 2013 cuando se descubrió que el mercado negro virtual Silk Road llevaba todas sus transacciones en bitcoins, aprovechando el anonimato y descentralización que ofrecían estos cripto-activos. Silk Road comenzó a operar en el año 2011 y ofrecía gran cantidad de productos y servicios de origen ilícito, tales como la compraventa de drogas ilegales, armas y municiones, documentos de identidad robados o falsificados, servicios de hackeo a de redes sociales o cuentas bancarias, hasta servicios de sicariato[44]. Para estar fuera del alcance de las autoridades, Silk Road no solo utilizó el Bitcoin como medio de pago, sino que implementó a su software la red "The Onion Router", conocida comúnmente como red "TOR" por sus siglas en inglés. Según Brill y Keene esta era "una red especial de computadoras en Internet, distribuida en todo el mundo, diseñada para ocultar las direcciones IP verdaderas y, por lo tanto, las identidades de los usuarios de la red TOR"[45]. El 23 de julio de 2013 las autoridades federales de los estados unidos arrestaron al creador y dueño del Silk Road, Ross Ulbricht[46]. Ulbricht fue condenado a cadena perpetua por los delitos de lavado de activos, hackeo de computadoras y por violar la ley anti narcóticos de los Estados Unidos[47]. Por otra parte, el vicepresidente de aquella época de Bitcoin Foundation y fundador de BitInstant (el primer *Exchanger* de bitcoins en Estados Unidos), Charlie Shrem, también fue arrestado ese año por facilitar operaciones de lavado de dinero a usuarios del mercado online Silk Road[48]. Al momento del cierre de Silk Road este contaba con 957,079 cuentas de usuarios registradas, había generado 1.2 billones de dólares en ventas y 80 millones de dólares en comisiones[49]. A partir de los eventos suscitados entre Bitcoin y el Silk Road, otros mercados negros en línea han comenzado a proliferar al adoptar criptomonedas para hacer sus transacciones; ejemplos de mercados negros virtuales que han hecho esto son Oasis, Alpha Bay, Zion y Silk Road 3.0 que

[43] *Ibíd.*
[44] *Ibíd.*
[45] *Ibíd.*
[46] United States District Court/ Southern Disctrict of New York. *United States of America v. Ross William Ulbricht.* Legal Information Institute, Cornell University, Law School.
[47] *Ibíd.*
[48] Daniel Cawrey. *Charlie Shrem Indicted on Federal Charges for Money Laundering.* https://www.coindesk.com/charlie-shrem-indicted-federal-charges-money-laundering (acceso: 28/1/2019).
[49] Allan Brill y Lonnie Keene. "Cryptocurrencies: The Next Generation of Terrorist Financing?". *Óp. cit.*, pp. 7-30.

utilizan criptomonedas con mayor anonimato y dificultad de rastreo tales como Monero o Zcash, las cuales, a diferencia del Bitcoin, son criptomonedas privadas y poseen *blockchain* privados en los cuales no se registra las verdaderas llaves públicas del emisor ni del receptor y las cifras verdaderas de la transferencia se alteran para que aparezca un valor diferente del que se efectuó en la transacción de las dos cuentas[50].

1.3.2 Problemática sobre el uso de las criptomonedas y los sistemas *blockchain*

El surgimiento de las criptomonedas y la tecnología que albergan han proporcionado un nuevo y poderoso instrumento a los criminales para facilitar sus operaciones delictivas y suponen un gran desafío para los legisladores y órganos de control. Cabe mencionar que la mayoría de usuarios de criptomonedas no utilizan estas divisas electrónicas con el fin de cometer ilícitos, sino que, emplean las criptomonedas como una inversión para ganar rédito a través de la especulación. Sin embargo, los usos criminales de las criptomonedas están presentes y, de la vasta gama de tipos delictivos que su comisión se ha visto facilitada por esta nueva tecnología, hay dos tipos penales que merecen ser analizados, ya que, son los delitos que mayor preocupación han infundido a las autoridades por su gravedad y proliferación exponencial en el mundo de la ciberdelincuencia. Estos delitos han ocupado un lugar prioritario dentro de las discusiones sobre las posibles medidas de regulación que se deben imponer a las criptomonedas. Estos ilícitos son la estafa y el lavado de activos[51].

2 CAPÍTULO II: CRIPTOMONEDAS Y CRIMEN

Este capítulo analiza los delitos de estafa y lavado de activos, los dos tipos penales que, asistidos por la tecnología de las criptomonedas, son perpetrados con mayor frecuencia por los cibercriminales. Primero se definirá los conceptos de delitos de cuello blanco y delitos informáticos a partir de los criterios doctrinarios más relevantes y prevalentes, ya que, tras una explicación de estos conceptos, se podrá evidenciar como se

[50] Matthew Asner y Alex Mitter. *A White-Collar Lawyer's Guide to Virtual Currency. White Collar Crime Report, 09 WCR 158, 03/07/2014*. http://www.bna.com (acceso: 28/1/2019).

[51] La empresa Chainalysis, la cuál es proveedora de servicios de *compliance* especializada en criptoactivos, elaboro un reporte acerca el fenómeno criminal que está vinculado a las criptomonedas. Dicho informe indica que los dos delitos que se perpetuán con mayor frecuencia, según la investigación de esta empresa, son el lavado de activos y la estafa. Por esta razón se ha escogido estos dos delitos para analizar en la presente tesis y no otros. Chainalysis. *Crypto Crime Report: Decoding increasingly sophisticated hacks, darknet markets, and scams, January 2019.* pp. 3- 29.

acoplan a las características de los tipos penales de estafa y lavado de activos. Además, se definirá los delitos de estafa y lavado de activos desde su estructura típica, proporcionando criterios y valoraciones doctrinarias acerca de los elementos objetivos y subjetivos típicos de estos ilícitos. Finalmente, esta sección detallara los métodos empleados por los ciberdelincuentes en la ejecución de estos tipos penales por medio del uso de las criptomonedas.

2.1 Definición crimen de cuello blanco y delito informático

2.1.1 Delitos de cuello blanco

En 1951, el criminólogo estadounidense Edwin Sutherland publicó *White Collar Crime,* libro que supuso el comienzo de un nuevo estudio en la criminología y el derecho penal, al instaurar el concepto de delito de cuello blanco. Las características que Sutherland proporciono en su análisis del perfil criminal del delincuente de cuello blanco, distan significativamente de las características clásicas atribuidas a los sujetos criminales. Tradicionalmente se creía que los delincuentes pertenecían de forma casi exclusiva a estratos sociales y económicos bajos; los casos perpetrados por sujetos pertenecientes a las altas esferas sociales y económicas eran considerados como pequeñas anomalías de la tendencia general, la cuál consideraba que la consumación de crímenes violentos era intrínseca de las clases más bajas. Sutherland demostró que los delincuentes de cuello blanco no pertenecen a un estrato social o económico bajo, sino que son personas que gozan de una posición social alta con acceso al poder[52]. Estos criminales son personas que ocupan puestos privilegiados en la sociedad, son individuos con altos conocimientos en su profesión y se presentan como miembros valiosos y honrados ante el resto de ciudadanos. Los crímenes de cuello blanco no son crímenes violentos pero su transgresión contra el patrimonio y en especial al orden socio económico es inmensa. Estos delitos son difíciles de ser descubiertos, porque son delitos técnicos perpetrados por criminales inteligentes.

Sutherland en su libro también hace una relevante distinción entre el delito de cuello banco y el delito de guante blanco, términos que son usados de forma equivalente cuando en realidad son conceptos diferentes y que es importarte de aclarar. Dicha diferenciación expuesta por Sutherland es la siguiente:

[52] Edwin Sutherland. *El delito de cuello blanco.* Buenos Aires: B de F, (2009), p. XIV.

> […] el delito de cuello blanco no es lo mismo que el de guante blanco, a pesar de la semejanza lingüística, dado que el primero es relativo al poder de que disponga el autor de la conducta delictiva, en tanto que el segundo se refiere a la actuación impoluta del agente crimina. El delito de guante blanco es el que se realiza de forma impecable, tal como un hurto con gran destreza, la estafa a un casino, el homicidio preciso y sin derramamiento de sangre. Como puede apreciarse, en el delito de guante blanco lo inmaculado es la forma de ejecución en cuanto a la precisión de la acción delictiva y va frecuentemente vinculado al profesionalismo de su ejecutor, mientras que el de cuello blanco acarrea una determinada posición de privilegio en la sociedad, como la de empresario, médico, abogado, gobernante, periodista o quien lleva una vida de relación que contenga acceso y disponibilidad al poder[53].

A pesar de que Sutherland acuño el término de crimen de cuello blanco, el estudio que él realizó se centró en las grandes multinacionales, por lo tanto, la definición que él proporcionó solo contemplaba cuatro conductas: prácticas contra el libre comercio, publicidad falsa, infracciones de normas sobre patentes y otros derechos de propiedad industrial e incumplimiento de la legislación sobre derechos de los trabajadores[54]. La definición de crimen de cuello blanco ha incorporado más conductas delictivas a través de los años. Los estudios más recientes sobre el crimen de cuello blanco comprenden las siguientes categorías:

> […]prácticas contra la libre competencia y fijación de precios en el mercado (*antitrust violations*), quiebra fraudulenta, delitos contra la propiedad industrial, revelación de secretos de empresa, espionaje industrial, delitos informáticos, delitos contra la salud de los consumidores, delitos contra el medio ambiente, defraudación tributaria, lavado de dinero, crimen organizado, financiamiento del crimen organizado, falsificación, fraude, estafas, delitos contra la administración pública (peculado, malversación de fondos, tráfico de influencias, etc), perjurio y obstrucción de justicia[55].

2.1.2 Delitos informáticos/ ciberdelitos

Existen muchas discrepancias en cuanto a cuál es la definición correcta de la ciberdelincuencia y cuales son todos los componentes que la integran. Sin embargo, el objetivo de la presente tesis no es ahondar minuciosamente en todos los pormenores y nimiedades de esta discusión jurídica sino de aportar una definición que pruebe que los delitos asociados a las criptomonedas entran dentro de la categoría de los ciberdelitos.

---

[53] *Ibíd.*

[54] No todas las conductas descritas por Sutherland son conductas penales, la principal crítica que recibió Sutherland cuando público su estudio fue que su concepto de crimen de cuello blanco era excesivamente amplio y no se reducía a la legislación penal, sino que abarcaba la regulación administrativa o civil. Sus críticos más ilustres fueron Tappan y Edelhertz. *Vid.* María Ángeles Gutiérrez Zarza. "Investigación y enjuiciamiento de los "delitos de cuello blanco" en el sistema judicial norteamericano". *Anuario de Derecho Penal, Vol. L*, (1997), pp.579-653.

[55] *Cfr.* María Ángeles Gutiérrez Zarza. "Investigación y enjuiciamiento de los "delitos de cuello blanco" en el sistema judicial norteamericano". *Óp. cit.* pp. 579-653.

Por lo tanto, a fin de conseguir el objetivo previamente mencionado, utilizaremos la definición del Dr. Nava Garcés, la cual define los delitos informáticos de la siguiente manera:

> […] delito informático en un sentido amplio es cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como **método**, **medio** o fin y que, en un sentido estricto (concepto típico) son las conductas típicas, antijurídicas y culpables en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como **método**, **medio** o fin[56]. (lo resaltado me pertenece)

Algunos organismos internacionales también han proporcionado definiciones sobre el concepto de la ciberdelincuencia, de las cuales, la definición aportada por la Unión Internacional de Telecomunicaciones (en adelante UIT) en su *Guía de Ciberseguridad para los Países en Desarrollo,* es la más completa. Dicha definición es la siguiente:

> […] delito informático es aquel cuyo objeto o **medio** de realizarlo es un sistema informático, está relacionado con las tecnologías digitales y se integra en los propios de la delincuencia de cuello blanco. El ciberdelito es una forma de delio informático que **recurre a las tecnologías de Internet para su comisión**, refiriéndose por tanto a todos los delitos cometidos en el ciberespacio[57]. (lo resaltado me pertenece)

Los delitos que utilizan a las criptomonedas como medio para su comisión encajan perfectamente con estas dos definiciones ya que los cibercriminales utilizan las criptomonedas y sus tecnologías anexas como un medio o instrumentos para la perpetración de delitos. En lo referente a este tema Pérez López manifiesta lo siguiente sobre la relación de los usos ilícitos de las criptomonedas y las características de la ciberdelincuencia:

> […] en tanto que fenómenos exclusivamente digitales, las criptomonedas se amoldan perfectamente a las características clásicas de la ciberdelincuencia: instantaneidad (rapidez de las transacciones); distancia entre el infractor y el lugar de comisión de una parte sustancial del *iter* criminoso del delito; **carácter transfronterizo**, con **la problemática jurídica asociada a la determinación de la jurisdicción competente para conocer de la infracción y a la cooperación internacional** indispensable para perseguirla; inmaterialidad y, por tanto, facilidad de eliminación de las pruebas (esta última, sin embargo, reducida en alguna medida debido al carácter público del *ledger* (**libro contable o *blockchain***))[58]. (lo resaltado me pertenece)

[56] Enrique Alberto Nava Garcés. *Análisis de los Delitos Informáticos*. México: ed. Porrúa, (2005), p.20.
[57] Unión Internacional de Telecomunicaciones. *Guía de Ciberseguridad para los Países en Desarrollo*. http://www.itu.int/ITU-D/cyb/publications/2007/cgdc-2007-s.pdf (acceso: 5/2/2019).
[58] Xesús Pérez López. "Las Criptomonedas: consideraciones generales y empleo de las criptomonedas como instrumento de blanqueo de capitales en la Unión Europea y en España". *Revista de Derecho Penal y Criminología* 3/18 (2017), pp.141-187.

Hay que destacar un elemento muy importante de los ciberdelitos; su naturaleza transfronteriza y multinacional. Muchas veces las conductas criminales relacionadas con los ciberdelitos son iniciadas en un país, pero su ejecución y efectos se pueden propagar a una multitud de naciones en continentes diferentes. Es por esto que la gran mayoría de países busca establecer convenios y tratados de cooperación judicial con otras naciones con el objetivo de establecer redes y sistemas efectivos para la prevención, investigación y persecución de ciberdelitos. Uno de los ejemplos de dichos convenios es el Convenio de Budapest sobre la delincuencia de 2001, el cuál el Ecuador no es un país signatario[59].

2.2 Estafa y apropiación fraudulenta por medios electrónicos

La estafa es un delito atávico, sus orígenes son difusos ya que al ser un delito tan antiguo no se puede establecer con precisión el surgimiento exacto de esta conducta delictiva. Los antecedentes de figuras afines a lo que hoy modernamente se conoce como estafa se ven manifestados en legislaciones y códigos morales milenarios tales como el Código de Hammurabi, el Corán, la Biblia, el Avesta Persa, etcétera[60]. Pese a sus antiguos orígenes este delito mantiene su relevancia en el mundo actual, y, debido a los cambios tecnológicos que se han suscitado en las últimas décadas han surgido nuevas modalidades de este delito.

Aquí es pertinente hacer una crucial aclaración: las actividades ilícitas que realizan los cibercriminales mediante el uso de criptomonedas no encajarían con el tipo penal de estafa bajo la legislación ecuatoriana; el tipo penal adecuado para sancionar estos actos delictivos sería la apropiación fraudulenta por medios electrónicos tipificada en el artículo 190 del COIP. Dicho artículo está prescrito de la siguiente manera:

> **Art. 190.- Apropiación fraudulenta por medios electrónicos**. - La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años.
>
> La misma sanción se impondrá si la infracción se comete con inutilización de sistemas de alarma o guarda, descubrimiento o descifrado de claves secretas o encriptadas, utilización

[59] Convenio Sobre la Ciberdelincuencia (2001).
[60] Edgardo Alberto Donna. *Derecho Penal: Parte Especial.* Tomo II-B. Rubinzal-Culzoni: Buenos Aires, (2001), p.256.

de tarjetas magnéticas o perforadas, utilización de controles o instrumentos de apertura a distancia, o violación de seguridades electrónicas, informáticas u otras semejantes[61].

Sin embargo, la apropiación fraudulenta por medios electrónicos es considerada como una modalidad de estafa en la mayoría de legislaciones de otros países. Prácticamente su tratamiento como una modalidad de la estafa es aceptada universalmente. Albán Gómez ilustra esto de la siguiente manera:

> La tipificación de esta modalidad de apropiación fraudulenta, prevista en el Art. 190, es de una marcada y no justificada complejidad. Si el delito consiste, en su esencia, en una apropiación de bienes utilizando fraudulentamente medios electrónicos, se podría concluir que se trata de una modalidad de estafa, para lo que sería suficiente una redacción similar a la del Art. 284 del Código español: *"Los que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro"* [62].

Una vez puntualizado el hecho evidente de que el delito de apropiación fraudulenta por medios electrónicos no es más que una modalidad de estafa que, por razones ajenas al sentido común, se encuentra tipificado como un delito autónomo, es importante examinar los componentes clave del delito de estafa.

2.2.1 Elementos del tipo penal de estafa y apropiación fraudulenta por medios electrónicos

El Código Orgánico Integral Penal (COIP) establece en su artículo 186 el delito de estafa de la siguiente manera:

> **Art. 186.- Estafa.** - La persona que, para obtener un beneficio patrimonial para sí misma o para una tercera persona, mediante la simulación de hechos falsos o la deformación u ocultamiento de hechos verdaderos, induzca a error a otra, con el fin de que realice un acto que perjudique su patrimonio o el de una tercera, será sancionado con pena privativa de libertad de cinco a siete años[63].

En cuanto a los elementos que configuran el delito de estafa la jurisprudencia y la doctrina han establecido que dichos elementos son: el dolo, que comprende el ánimo de

[61] Código Orgánico Integral Penal. Art. 186. Publicado en el Registro Oficial Suplemento 180 de 10 de febrero de 2014.
[62] Ernesto Albán Gómez. *Manual de Derecho Penal Ecuatoriano. Parte Especial.* Tomo I. Ediciones Legales: Quito, (2018), p. 204
[63] Código Orgánico Integral Penal. Art. 186. Publicado en el Registro Oficial Suplemento 180 de 10 de febrero de 2014.

lucro, el engaño y la entrega[64]. Esto se ve evidenciado en el siguiente fallo de la Corte Nacional de Justicia en el año 2013:

> […] el delito de estafa, tipificado en el artículo 563 del Código Penal, tiene una estructura compleja, por lo que si se alega su existencia se debe demostrar su integración típica, siendo de especial preponderancia el engaño, como elemento característico de esta incriminación; pero además, es indispensable que se establezca el perjuicio, esto es la lesión al bien jurídico protegido que es la propiedad en un sentido amplio, siendo el núcleo de la acción el hacerse entregar bienes ajenos con la finalidad de apropiarse de ellos [65].

En cuanto doctrina se refiere, Albán Gómez establece los principales elementos de este ilícito los cuales son inducir a error (núcleo), ánimo de lucro (propósito de obtener un beneficio patrimonial para sí o para un tercero) y engaño (la simulación de hechos falsos o la deformación u ocultamiento de hechos verdaderos) [66].

Cabe señalar que la Estafa y la apropiación fraudulenta por medios electrónicos se encuentran tipificados bajo la sección novena del COIP, la cual trata sobre los Delitos contra el derecho de propiedad. Este conglomerado de delitos, como su nombre lo indica, atacan al bien jurídico que es el derecho de propiedad que poseen los individuos. La distinción entre el derecho de propiedad como está definido en el Código Civil y el derecho de propiedad establecido en el COIP merece ser explicada para evitar confusiones. Albán Gómez aclara la diferencia de estas dos definiciones de derecho de propiedad de la siguiente manera:

> La observación se relaciona con el alcance que la palabra propiedad tiene en el Código Civil (Art. 599), como sinónimo del derecho real de dominio (para gozar y disponer de una cosa corporal), pues señalan que la protección penal va más allá de este concepto, e inclusive afirman que algunos de los delitos más característicos (el hurto y el robo, por ejemplo) no afectan al dominio, que no se pierde con tales hechos. En tales casos se afecta de una manera directa la posesión de la cosa y aun la mera tenencia; y en otros casos, se lesionan otros derechos reales. Pero hay que considerar que el Derecho Penal no necesariamente emplea ciertos términos en el mismo sentido que tienen en otras ramas jurídicas, en este caso en el Derecho Civil. Por lo que el término propiedad debe entenderse aquí como un derecho en un sentido más amplio, cercano al que quiere darle la Constitución (Arts. 66.26 y Arts.321 y siguientes), dentro del ámbito de la vida económica de una sociedad. Este derecho se concreta en bienes materiales y aun en

[64] *Cfr*. Bernardo Maya Arroyo. *Delimitación entre el delito de estafa y el dolo civil como vicio del consentimiento.* Tesis pregrado. Universidad San Francisco de Quito. Quito, (2014), p.42.
[65] Corte Nacional de Justicia. Primera Sala de lo Penal. Juicio No. 014-2010. Registro Oficial Suplemento 26, 22 de Julio del 2013.
[66] *Cfr.* Ernesto Albán Gómez. *Manual de Derecho Penal Ecuatoriano. Parte Especial. Óp. cit.,* p. 192.

> derecho inmateriales, en relación a las cosas corporales e incorporales, de las que habla el Código Civil [67].

En la siguiente sección se analizarán el tipo objetivo y tipo subjetivo del tipo penal de estafa. Se realizará una descripción del tipo objetivo a través de los elementos de: el engaño, el error, y del acto de disposición. En lo referente al tipo subjetivo se examinará el dolo y el ánimo de lucro.

2.2.1.1 Elementos objetivos

Dentro de la dogmática penal, la tipicidad objetiva se refiere a los actos exteriorizados que deben ser realizados por el sujeto activo para que dicha conducta sea punible por el ordenamiento penal. A continuación, los elementos objetivos respectivos del delito de estafa.

2.2.1.2 El engaño

El Código Penal español en su artículo 248.1 define al delito de estafa como la conducta que consiste en "utilizar, con ánimo de lucro, **engaño bastante** para producir error en otro, induciéndolo a realizar un acto de disposición propio o ajeno."[68] (lo resaltado me pertenece). Por otro lado, en la legislación ecuatoriana el legislador utiliza la frase "[…] mediante la simulación de hechos falsos o la deformación u ocultamiento de hechos verdaderos […]"[69] para ejemplificar el concepto de engaño.

La doctrina ha establecido que un el engaño debe ser *idóneo* o *bastante* para ser considerado penalmente relevante, ya que no toda falta a la verdad puede ser considerada como un engaño. Pastor Muñoz y Coca Vila comentan lo siguiente sobre este tema:

> A tal efecto no es suficiente que el engaño haya sido "eficaz" (esto es, que haya conducido a la víctima a un error y a un acto de disposición perjudicial), pues ello solamente indica que existe un vínculo causal entre el engaño y el error. Para ser "bastante" (para constituir un riesgo típico), el engaño ha de ser *ex ante* adecuado, idóneo para conducir al disponente a un acto de disposición perjudicial; si lo es, concurre una tentativa de estafa; si, además, *ex post*, el disponente realiza el acto de disposición y se

[67] *Id*. p. 171.
[68] Código Penal Español. Ley Orgánica 1&2/2015. Boletín Oficial del Estado, 10 de agosto 2015, núm. 243, pp. 89411 a 89530.
[69] Código Orgánico Integral Penal. Art. 186. Publicado en el Registro Oficial Suplemento 180 de 10 de febrero de 2014.

> genera el perjuicio, se habrá producido la consumación del delito (la realización del riesgo típico en el resultado)[70].

Los autores Manzini, Ortonlán, Chaveau y Pessina, citados por Fontán Balestra en su libro *Tratado de Derecho Penal,* establecen que para que el engaño sea idóneo "basta que el engaño importe una **fuerza superior a los medios ordinarios de defensa individual**, medios de defensa que deben considerarse con relación al sujeto pasivo en concreto"[71] (lo resaltado me pertenece). A raíz de esto se puede interpretar que hay una responsabilidad del sujeto pasivo de tener un deber de auto-protegerse del engaño, debe obrar con determinado grado de diligencia y precaución y, solo cuando el engaño sea de una magnitud tal que supere los medios de defensa que razonablemente se pueden exigir al sujeto pasivo, el engaño se estimaría como idóneo.

2.2.1.3 El error

El verbo rector en el delito de estafa del Art. 186 del COIP, es inducir en error a otra persona. Este es un elemento fundamental del tipo penal ya que para que se consume el delito se necesita que la víctima de forma voluntaria realice la disposición de su patrimonio[72]. Edgardo Donna establece una importante delineación del concepto de error, la cual el autor la despliega de la siguiente manera:

> […] el error adquiere una importancia vital, pues, a diferencia de otros delitos como el hurto o el robo no se trata de "sustraer" o "apoderarse", sino de provocar la colaboración del sujeto pasivo y que éste, engañado, sea quien realice una disposición patrimonial en perjuicio de sí mismo o de un tercero. Se trata de un estado psicológico provocado por el autor del delito, quien induce a la víctima a la realización de una disposición patrimonial perjudicial [73].

Respecto al concepto de error Albán Gómez manifiesta que "El error debe entenderse en su sentido natural como la equivocada o falsa representación de la realidad, conseguida a través de los medios previstos por la ley"[74]. En el delito de Apropiación fraudulenta por medios electrónicos es la utilización de dichos medios electrónicos de forma engañosa la que induce en error al sujeto pasivo. En cuanto al error, Donna

---

[70] Nuria Pastor Muñoz y Ivó Coca Vila. *Lecciones de Derecho Penal. Parte Especial*. Ediciones Atelier: Barcelona, (2015), pp. 254-264.
[71]Carlos Fontán Balestra. *Tratado de Derecho Penal.* Tomo VI: Parte Especial. La Ley: Buenos Aires, (2013), pp. 337-345.
[72] *Cfr*. Bernardo Maya Arroyo. *Delimitación entre el delito de estafa y el dolo civil como vicio del consentimiento. Óp. cit*., pp. 47.
[73] Edgardo Alberto Donna. *Derecho Penal: Parte Especial. Óp. cit.,* pp. 300-301.
[74] Ernesto Albán Gómez. *Manual de Derecho Penal Ecuatoriano. Parte Especial. Óp. cit.,* p. 193.

determina que el elemento del error es un nexo entre el engaño y el resultado del ilícito. Esto quiere decir que "[e]l error debe ser causado por el engaño del autor"[75]. Donna, en la determinación de la relación del error con el engaño, expande el análisis de la siguiente manera:

> […]el tipo penal de estafa se caracteriza por una doble relación entre el engaño y el error, y entre éste y la disposición patrimonial perjudicial. El engaño debe haber sido determinante del error y éste, a su vez, debe haber sido la causa de la disposición"[76].

Es importante recalcar que para que el error sea penalmente relevante el sujeto pasivo debe de poseer cierto grado de conciencia que le permita ejercer el acto de disposición de forma *voluntaria*. Es por tal motivo si el sujeto pasivo es un incapaz jurídico absoluto no se puede determinar con certeza que el acto haya sido *voluntario*, y por lo tanto no se podría configurar el tipo penal de estafa. Esto no quiere decir que la conducta quedaría impune, sino que sería constitutiva de otro delito[77].

Otro aspecto importante de analizar es el nivel de diligencia empleado por el sujeto pasivo y el error. El tipo penal exige que error en el cual incurre el sujeto pasivo es consecuencia directa del engaño perpetrado por el sujeto activo, pero si el error es provocado por otros factores externos como la negligencia o ignorancia no se cumplen las condiciones establecidas por el tipo penal[78]. Donna expone lo siguiente respecto a esta cuestión:

> Cuando la disposición patrimonial ha tenido su causa en un acto derivado de la negligencia del sujeto pasivo, no puede afirmarse que estamos ante un ardid o engaño, sino ante un caso de negligencia culpable de la víctima. El Derecho puede, y debe, exigir un cierto nivel de diligencia, que permita al sujeto descubrir el fraude, por lo que la protección penal no debe producirse cuando la indolencia, la excesiva credulidad y la omisión de precauciones elementales hayan sido las verdaderas causas de la eficacia del engaño[79].

2.2.1.4 Acto de disposición patrimonial

Conforme lo establecido de forma predominante por la doctrina, el acto de disposición es un acto de entrega llevado por el sujeto pasivo[80]. Este acto de disposición conlleva necesariamente un perjuicio patrimonial de la víctima. Aquí cabe una aclaración,

---

[75] Edgardo Alberto Donna. *Derecho Penal: Parte Especial. Óp. cit.* p. 370.
[76] *Id.* p. 372
[77] *Cfr.* Edgardo Alberto Donna. *Derecho Penal: Parte Especial. Óp. cit.,* p. 363.
[78] *Cfr. Ibíd.*
[79] Edgardo Alberto Donna. *Derecho Penal: Parte Especial. Óp. cit.,* p. 375.
[80] *Cfr.* Nuria Pastor Muñoz y Ivó Coca Vila. *Lecciones de Derecho Penal. Parte Especial*. *Óp. cit.,* pp.254-264.

el sujeto pasivo no necesariamente es la víctima del delito de estafa, ya que el sujeto pasivo puede hacer un acto de disposición de un patrimonio que no le es propio. Por ejemplo, un adolescente utiliza la tarjeta de crédito de su padre para comprar unos audífonos a un vendedor que le asegura que se le entregara por domicilio dos días después de la compra, sin embargo, la compañía para la cual el vendedor trabajaba nunca empleo a dicha persona ni poseía los audífonos en su catálogo. Aquí el sujeto activo del delito de estafa es el hombre que se hizo pasar como vendedor de la compañía, el sujeto pasivo es el adolescente, pero la víctima, la persona que efectivamente sufrió el perjuicio patrimonial fue el padre del adolescente.

Respecto a este tema Ernesto Albán manifiesta lo siguiente:

> La norma habla simplemente, en forma general, de la realización de un acto (no se señala negocio jurídico, como en la extorsión, caso que aquí podría ser más pertinente) que perjudique el patrimonio de la víctima. En definitiva, puede tratarse de cualquier acto de disposición: entrega o transferencia de dinero o bienes, constitución de una garantía, prestación de un servicio, etcétera, siempre que produzca un perjuicio patrimonial [81].

2.2.1.5 Elementos Subjetivos

Los artículos 26 al 28 del COIP especifican los elementos subjetivos que pueden integrar un delito penal, siendo estos la culpa, la preterintención y el dolo. El Artículo 190 de apropiación fraudulenta por medios electrónicos establece que la conducta típica se da "en beneficio suyo o de otra persona"[82], mientras que el Art. 186 dispone que la estafa está dirigida a "obtener un beneficio patrimonial para sí misma o para una tercera persona". Esto refleja que existe un ánimo de lucro por parte del sujeto activo, este elemento es algo representativo de la mayoría de delitos contra la propiedad. La doctrina ha determinado que los tipos subjetivos de estos dos delitos es el dolo. Respecto a esto los autores Pastor Muñoz y Coca Vila indican lo siguiente:

> En el tipo subjetivo de la estafa debe concurrir **dolo** y **ánimo de lucro**. […] el ánimo de lucro es un elemento subjetivo del tipo que la doctrina define en términos estrictos, a saber, como persecución de un beneficio patrimonial para el autor o para un tercero, y que la jurisprudencia interpreta de modo más amplio, como finalidad de obtener cualquier utilidad o provecho, sean éstos económicos o no[83].

[81] Albán Gómez, Ernesto. *Manual de Derecho Penal Ecuatoriano. Parte Especial. Óp. cit.*, p. 194.
[82] Código Orgánico Integral Penal. Art. 190. Publicado en el Registro Oficial Suplemento 180 de 10 de febrero de 2014.
[83] Nuria Pastor Muñoz y Ivó Coca Vila. *Lecciones de Derecho Penal. Parte Especial*. *Óp. cit.*, pp.254-264.

El dolo presente en el delito de estafa es un dolo específico, ya que no es simplemente el designio de causar un daño lo que impulsa al autor a cometer el ilícito, sino el dolo debe contener ánimo de lucro. Donna establece que el delito de estafa "[…] supone la existencia de una motivación especial en el autor […] no alcanza con el conocimiento y la voluntad de causar un perjuicio, sino que además se debe obrar con el propósito de obtener una ventaja patrimonial"[84]. El ánimo de lucro comprende dos elementos que vale puntualizar: (1) es que es un lucro ilegítimo el que se persigue ya que "[n]o comete esta quien a través del engaño consigue que se le pague algo que le deben o que creía que le deben"[85] (2) consiste en cualquier tipo de ventaja patrimonial, incluso en la destrucción de la cosa[86]. Donna sobre este tema expresa lo siguiente:

> "[A]unque por su relación con el perjuicio, la ventaja del autor ha de tener un trasfondo patrimonial, no es preciso para admitir la existencia de ánimo de lucro […] que éste se centre exclusivamente en el valor económico de la cosa, ya que el lucro se utiliza en estos delitos con un sentido jurídico equivalente a cualquier clase de utilidad o ventaja, sea o no económica."[87]

2.2.2 Empleo de criptomonedas para la comisión de estafas

El precio del Bitcoin cuando salió recién al mercado en 2009 era menor de 1 centavo de dólar americano por cada una de las criptomonedas, de hecho, durante el 2010 el valor más alto que consiguió el Bitcoin fue de 39 centavos. Para el 16 de diciembre de 2017 el valor de cada Bitcoin ascendió hasta los 19,343.04 dólares de los estados unidos de américa[88]. Actualmente el valor de cada Bitcoin es equivalente a 3,927.41 dólares y posee una capitalización de mercado de 68.92 billones de dólares estadounidenses[89]. Los altos réditos que proporcionaban las inversiones en criptomonedas y en tecnología *blockchain* y todas las historias de individuos que se convirtieron en millonarios gracias a las inversiones en estas criptodivisas generaron el ambiente propicio para que miles de personas contraigan la fiebre de las criptomonedas. Los estafadores han aprovechado esta fiebre para engañar a personas sesgadas por la promesa de obtener grandes rendimientos

[84] Edgardo Alberto Donna. *Derecho Penal: Parte Especial. Óp. cit.,* p. 402.
[85] Bernardo Maya Arroyo. *Delimitación entre el delito de estafa y el dolo civil como vicio del consentimiento.* Tesis pregrado. Universidad San Francisco de Quito. Quito, (2014), p.42. citando a Carlos Fontán Balestra. *Tratado de Derecho Penal.* Tomo VI: Parte Especial. La Ley: Buenos Aires, (2013), p.55
[86] *Cfr. Ibíd.*
[87] Edgardo Alberto Donna. *Derecho Penal: Parte Especial. Óp. cit.,* p. 402.
[88] Coindesk. *Bitcoin Price (BTC).* https://www.coindesk.com/price/bitcoin (acceso: 20/2/2019).
[89] *Ibíd.*

económicos pero que desconocen cómo funciona el mercado de las criptomonedas y la tecnología subyacente.

El número de estafas relacionadas a criptomonedas se ha multiplicado en los últimos años, tanto es así que un reporte de Satis Group LLC publicado por Bloomberg L.P señala que 80% de las ICOs (Initial Coin Offerings) en el mercado son estafas[90]. Lamentablemente los estafadores de criptomonedas también han comenzado a operar en Ecuador, el 23 de enero de 2018 dirigentes de la Comisión de Justicia del Movimiento Indígena y Campesino de Cotopaxi (MICC) denunciaron ante las autoridades un presunto caso de estafa y captación ilegal de dinero que fue perpetrado en contra de 1500 campesinos e indígenas e las comunidades de Otavalo, Cayambe, Ambato, Pujilí y Latacunga[91]. Los denunciantes afirman que asesores de la plataforma digital Bit Trader entablaron una estafa piramidal como medio para estafar a todas estas personas[92].

A continuación, se expondrá los métodos más comunes empleados por los estafadores para cometer ilícitos utilizando las criptomonedas[93].

2.2.2.1 Empleo fraudulento de las *Initial Coin Offerings* (ICO´s)

Antes de profundizar en los mecanismos fraudulentos que emplean los estafadores mediante las ICO´s, es imprescindible explicar que es una ICO. Pérez López detalla de forma proba los pormenores de las ICO´s de la siguiente manera:

> Las ICO´s son un modo de financiación de criptomonedas incipientes que funciona, en cierto modo, de manera similar al ***crowdfunding***, puesto que consiste en la oferta al público (en particular a potenciales microinversores, aunque no sólo), por un precio determinado, de una cantidad de unidades de una criptomoneda en curso de creación, de cada a la creación de una base inicial de titulares de las criptomonedas, al respaldo del valor percibido de la misma por la comunidad (puesto que el valor percibido de cada unidad, al menos en un primer momento, ascenderá al menos a la cantidad que

[90]Sherwin Dowlat. *Cryptoasset Market Coverage Initiation Valuation.* https://research.bloomberg.com/pub/res/d37g1Q1hEhBkiRCu_ruMdMsbc0A (acceso: 22/2/2019).
[91] María Angelina Castillo y Fabián Maisanche. *Indígenas del país denuncian estafa masiva con "criptomonedas".* https://www.elcomercio.com/actualidad/indigenas-denuncian-estafa-criptomonedas-bitcoin.html (acceso: 22/2/2019).
[92] Fabián Maisanche. *Los indígenas de Cotopaxi denuncian una estafa masiva y captación ilegal de dinero en plataformas digitales.* https://www.elcomercio.com/actualidad/indigenas-cotopaxi-denuncian-estafa-criptomoneda.html (acceso: 22/2/2019).
[93] Los métodos de estafa descritos en la presente tesis no son taxativos, existen una multitud de métodos de estafa empleados por los criminales usando criptomonedas. Sin embargo, me limito a describir solo dos métodos por delito debido a que profundizar en cada método existente provocaría que la tesis no cumpla con el máximo de extensión permitido. La forma por la cual abordo el lavado de activos es la misma.

> cada microinversor haya pagado por ella) y a la financiación de los gastos derivados de la misma creación de la criptomoneda de que se trate [94]. (lo resaltado me pertenece)

En síntesis, las ICO´s son una nueva manera de que las compañías de adquirir capital mediante la realización de un *token*[95] digital o criptomoneda y la venden a los inversionistas a cambio de dinero fiduciario u otra criptomoneda (usualmente ether o bitcoin). Las ICO´s proporcionan una serie de beneficios a sus inversionistas además de la entrega de los *tokens.* Los creadores de cada ICO publicaran en la red un *whitepaper*, que detalla el modelo de negocio que pretende implementar la ICO[96]. Dependiendo de lo innovador o lucrativo que el plan de negocios de la ICO puede llegar a parecer a los inversionistas, estos destinaran mayores recursos a la creación de la ICO. En el 2017, 6.6 billones fueron invertidos en ICO´s[97]. La ICO más exitosa de la historia es Ethereum, creadora de los *smart contracts* y las aplicaciones descentralizadas para *blockchain*[98]. Actualmente su criptomoneda *ether* tiene la segunda mayor capitalización de mercado detrás de Bitcoin ($15.438,019 en capitalización de mercado y cada *ether* avaluado en $147.11)[99]. Pero las ICO´s no necesariamente tienen que proponer avances tecnológicos a la tecnología *blockchain* o al mundo de las criptomonedas; Dragon Coin es una criptomoneda desarrollada por los casinos de Macao como medio de pago exclusivo en dichos casinos y que otorga beneficios a sus usuarios tales como descuentos en los servicios del casino y mejores sistemas de pago dentro de las instalaciones[100]. Pandacoin es otra criptomoneda que está enfocada a la protección de los osos panda y propone a sus inversores comprar la criptomoneda, ya que la mitad de los fondos se repartirían entre todas las fundaciones que protegen a los pandas en China y ofrece descuentos para las visitas a los parques nacionales protegidos de los pandas[101].

---

[94] Xesús Pérez López. "Las Criptomonedas: consideraciones generales y empleo de las criptomonedas como instrumento de blanqueo de capitales en la Unión Europea y en España". *Óp. cit.*, pp. 141-187.
[95] Unidad de valor que en la gran mayoría de situaciones se utiliza como sinónimo de criptomoneda, aunque a diferencia de las criptomonedas estos tienen más usos que solo ser un medio de pago al poder representar cualquier activo fungible y negociable. *Vid*. Genny Díaz. *Qué son los tokens y cómo se diferencian de las criptomonedas.* https://www.criptonoticias.com/colecciones/que-son-tokens-como-diferencian-criptomonedas/ (acceso: 22/2/2019) o BBVA. *Qué es un "token" y para qué sirve.* https://www.bbva.com/es/que-es-un-token-y-para-que-sirve/ (acceso: 22/2/2019).
[96] Joao dos Santos y Stefano Vranca. *Blockchain technology and Cryptocurrencies: Emerging Trends.* Expert Witnesses. Vol 14, No. 2, (2018), p. 104.
[97] *Ibíd.*
[98] Xesús Pérez López. "Las Criptomonedas: consideraciones generales y empleo de las criptomonedas como instrumento de blanqueo de capitales en la Unión Europea y en España". *Óp. cit.*, pp. 141-187.
[99] Coindesk. *Ethereum Price Index*. https://www.coindesk.com/price/ethereum (acceso: 22/2/2019).
[100] Dragon Coin. *Token Sale*: https://tokensale.drgtoken.io (acceso: 22/2/2019).
[101] Pandacoin. https://digitalpandacoin.org (acceso: 22/2/2019)

La forma por la cual los criminales estafan a los inversionistas es lanzando al mercado una ICO´s que en realidad es esquema Ponzi, también conocidos como estafa piramidal. Las estafas piramidales operan de la siguiente manera: se consigue un grupo de inversores iniciales a los cuales se les convence de destinar fondos para un negocio que les va dar grandes réditos económicos a corto plazo y a un bajo riesgo, luego se busca un nuevo grupo de inversores y se les promete lo mismo. Con el dinero invertido por el segundo grupo de inversores se les paga a los primeros inversionistas para crear la ilusión de que el negocio está generando ganancias. El proceso se repite una y otra vez, y entre más inversionistas puede captar la estafa piramidal, tiene más opciones de perdurar en el tiempo por el flujo constante de dinero. A la final estas estafas piramidales caen por su propio peso, ya que, o no logran conseguir nuevos inversores para pagar a los inversores existentes, o muchos inversores deciden retirar sus fondos lo que deja sin dinero para pagar a los inversores que aún permanecen en el negocio[102].

El uso fraudulento de las ICO´s han provocado que muchas autoridades se pronuncien sobre los riesgos de las inversiones en ICO´s. La Security Exchange Commission (SEC) de los Estados Unidos publicó el *Investor Bulletins: Initial Coin Offerings* el 25 de julio de 2017, el cuál provee una serie de pautas para invertir en ICO´s y evitar riesgos de ser víctima en operaciones fraudulentas; también, la Autoridad Europea de Valores y Mercados (ESMA) publicó informes en los que alerta a los inversores de los peligros que conlleva invertir en las ICO´s[103]. Por otro lado, el Banco Popular de China (órgano supervisor financiero de la República Popular de China) fue incluso al extremo de prohibir las ICO´s por los riesgos que están representan[104]. Dado el alcance mundial que proporciona el internet, un grupo de estafadores puede lanzar una ICO y captar dinero proveniente de inversores todo el mundo.

2.2.2.2 Empleo fraudulento de los *Smart Contracts*

Otra forma de implementar esquemas Ponzi es utilizando los *smart contracts* (contratos inteligentes/ contratos auto-programables). Para explicar el método como operan las estafas piramidales con esta tecnología es necesario proporcionar una

[102] Massimo Bartoletti, Salvatore Carta, Tiziana Cimoli, y Roberto Saia. *Dissecting Ponzi Schemes on Ethereum: Identification, analysis, and impact.* Dipartimento di Matematica e Informatica- Università di Cagliari. Cagliari, (2017), p. 2.
[103] Xesús Pérez López. "Las Criptomonedas: consideraciones generales y empleo de las criptomonedas como instrumento de blanqueo de capitales en la Unión Europea y en España". *Óp. cit.,* pp. 141-187.
[104] *Ibíd.*

definición de esta tecnología. Según los autores de blockchaintechnologies.com, un *smart contract* es:

> Un código de programa de computadora que es capaz de facilitar, ejecutar y hacer cumplir la negociación o ejecución de un acuerdo (es decir, un contrato) utilizando la tecnología blockchain. Todo el proceso que se automatiza puede actuar como un complemento o un sustituto de los contratos legales, donde los términos del contrato inteligente se registran en un lenguaje informático como un conjunto de instrucciones. […] un contrato inteligente puede describirse como un programa de computadora que actúa como un acuerdo en el que los términos del acuerdo pueden pre-programarse con la capacidad de auto-ejecutarse y auto-cumplirse a sí mismos. El objetivo principal de un contrato inteligente es proporcionar un sistema superior para los acuerdos contractuales basados únicamente en el código de computadora; de lo que actualmente existe basado en procesos judiciales anticuados[105].

Los autores Bartoletti, Carta, Cimoli y Saia han establecido tres razones fundamentales por las cuales los *smart contracts* son medios idóneos para poner en práctica este tipo de estafas, las cuales son las siguientes:

> (1) El iniciador de un esquema Ponzi podría permanecer en el anonimato, ya que crear el contrato y retirar dinero no requiere revelar su identidad; (2) Dado que los contratos inteligentes son "no modificables" e "imparables", ninguna autoridad central (en particular, ningún tribunal de justicia) podría terminar la ejecución del plan o revertir sus efectos para reembolsar a las víctimas. Esto es particularmente cierto para los contratos inteligentes que se ejecutan en cadenas de bloques sin permiso, que están controladas por una red de mineros de igual a igual. (3) Los inversores pueden obtener una falsa sensación de confiabilidad por el hecho de que el código de los contratos inteligentes es público e inmutable, y su ejecución se aplica automáticamente. Esto puede llevar a los inversionistas a creer que el propietario no puede sacar provecho de su dinero, que el plan funcionará para siempre y que tienen una probabilidad justa de obtener los intereses declarados.
>
> Todas estas características son posibles gracias a una combinación de factores, entre los que se encuentran el crecimiento de plataformas para contratos inteligentes, que publicitan el anonimato y la persistencia del contrato como principales puntos de venta, y el hecho de que estas tecnologías son muy recientes y aún viven en una zona gris de los sistemas jurídicos.[106]

Los autores antes mencionados publicaron un artículo para la Universidad de Cagliari en el que describen que crearon una metodología por la cual se puede identificar los esquemas Ponzi en plataformas de *smart contracts* utilizando modelos matemáticos y análisis de datos cruzados con verificaciones del código fuente[107]. Del análisis realizado por los autores se descubrió 137 *smart contracts* que eran estafas piramidales en la

[105] Blockchain Technologies. *Smart Contracts Explained. https://www.blockchaintechnologies.com/smart-contracts/ (*acceso: 23/2/2019).
[106] Massimo Bartoletti, Salvatore Carta, Tiziana Cimoli, y Roberto Saia. *Dissecting Ponzi Schemes on Ethereum: Identification, analysis, and impact. Óp. cit*., pp. 3-4.
[107] *Id.*

plataforma de Ethereum[108]. Los miembros de esta investigación identificaron que hay cuatro principales categorías por las cuales se puede agrupar a las distintas modalidades de estos contratos fraudulentos, las cuales son *array-based pyramid schemes, tree-based pyramid schemes, handover schemes,* y *waterfall schemes*[109]. Estudios similares se han realizado en universidades y centros de investigación en China, Estados Unidos, Suecia, entre otros[110]; esto demuestra que, a pesar de que el surgimiento de estas nuevas tecnologías proporciona intricadas formas de delinquir a los delincuentes que favorecen el encubrimiento de sus actividades criminales, existen métodos de revelar dichas actividades criminales y prevenir que vulneren los derechos de los usuarios de estas plataformas.

2.3 Lavado de activos

Para la mayoría de naciones el delito de lavado de activos representa un desafió complejo en lo relativo a su prevención, descubrimiento y acción legal[111]. El surgimiento de nuevas técnicas para blanquear dinero, las cuales son cada vez más refinadas y complicadas, aumentan la dificultad de estos desafíos. Las criptomonedas se han abierto paso como la técnica de moda para la perpetración de este ilícito. Pero, a diferencia de la complejidad que este delito representa en cuanto a sus múltiples desafíos, el concepto del lavado de activos es fundamentalmente simple. A grandes trazos el lavado de activos consiste en el procedimiento mediante el cual los delincuentes enmascaran la procedencia de sus riquezas obtenidas de actividades criminales para dar una imagen de licitud a dichas ganancias[112].

La definición de lavado de activos que es aceptada por la mayoría de países se encuentra prescrita en el Artículo 6 de la Convención de las Naciones Unidas contra la

---

[108] *Id.*
[109] *Id*.
[110] *Vid.* Weili Chein, Zibin Zheng, Jiahui Cui, Edith Ngai, Peilin Zheng, Yuren Zhou. *Detecting Ponzi Schemes on Ethereum: Towards Healthier Blockchain Technology.* Sun Yat-sen University Guanzhou, China (2018), p. 12. y; Tyler Moore, Jie Han y Richard Clayton. "The postmodern ponzi scheme: empirical analysis of high-yield investment programs". *Financial Cryptography and Data Security*. ed. Springer, Heidelberg (2012), pp. 37-41.; y; Jen Neisius y Richard Clayton. "Orchestrated crime: the high yield investment fraud ecosystem". *Financial Cryptography and Data Security*. ed. AL. Birmingham (2014), pp. 87-94.
[111] *Cfr*. Paul Allan Schott. *Guía de referencia para el antilavado de activos y la lucha contra el financiamiento del terrorismo*. Banco Mundial en coedición con Mayol, (2007), p. 3.
[112] *Ibíd*

Delincuencia Organizada Transnacional, también conocida como la Convención de Palermo. Dicho articulado decreta lo siguiente respecto al lavado de activos:

> Artículo 6. Penalización del blanqueo del producto del delito
> 1. Cada Estado Parte adoptará, de conformidad con los principios fundamentales de su derecho interno, las medidas legislativas y de otra índole que sean necesarias para tipificar como delito, cuando se cometan intencionalmente:
>   a. i) La conversión o la transferencia de bienes, a sabiendas de que esos bienes son producto del delito, con el propósito de ocultar o disimular el origen ilícito de los bienes o ayudar a cualquier persona involucrada en la comisión del delito determinante a eludir las consecuencias jurídicas de sus actos;
>   ii) La ocultación o disimulación de la verdadera naturaleza, origen, ubicación, disposición, movimiento o propiedad de bienes o del legítimo derecho a éstos, a sabiendas de que dichos bienes son producto del delito;
>   b. Con sujeción a los conceptos básicos de su ordenamiento jurídico:
>   i. La adquisición, posesión o utilización de bienes, a sabiendas, en el momento de su recepción, de que son producto del delito; […] [113]

El Ecuador regula el lavado de activos a través del Código Orgánico Integral Penal, la Ley Orgánica de Prevención, Detección, y Erradicación del Delito de Lavado de Activos y Del Financiamiento de Delitos[114] y su respectivo reglamento, el Reglamento de Contrataciones del Consejo Nacional Contra el Lavado de Activos y de la Unidad de Inteligencia Financiera[115], y las Normas de Prevención de Lavado de Activos Financiamiento del Terrorismo y otros Delitos[116]. Históricamente el lavado de activos se consideraba como una forma de encubrimiento, pero debido a su gravedad, organismos internacionales como el GAFI (Grupo de Acción Financiera Internacional), la Organización de las Naciones Unidas a través de su Oficina contra la Droga y el Delito (UNODC), o el Grupo Egmont de Unidades de Inteligencia Financiera, han emitido recomendaciones consideradas como estándares internacionales, los cuales exhortan a las naciones a tipificar el lavado de activo como delito autónomo[117]. Es decir que el carácter de delito autónomo que posee el lavado de activos se debe a una decisión de política criminal. El profesor Zambrano Pasquel explica que este ilícito es "un delito independiente o autónomo de los delitos de origen o conexos, sin que se requiera que los

[113] Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional (2000) Artículo 6.
[114] Ley Orgánica de Prevención, Detección, y Erradicación del Delito de Lavado de Activos y Del Financiamiento de Delitos. Registro Oficial Suplemento No. 802 de 21 de julio de 2016.
[115] Reglamento de Contrataciones del Consejo Nacional Contra el Lavado de Activos y de la Unidad de Inteligencia Financiera. Registro Oficial No. 58 de 5 de abril de 2007.
[116] Normas de Prevención de Lavado de Activos Financiamiento del Terrorismo y otros Delitos. Registro Oficial Suplemento No. 396 de 28 de diciembre de 2018.
[117] *Cfr.* Paul Allan Schott. *Guía de referencia para el antilavado de activos y la lucha contra el financiamiento del terrorismo*. *Óp. cit.*, p. 17.

otros delitos hayan sido juzgados para que proceda el procesamiento penal por *el lavado de activos* que tiene plena autonomía punitiva y procesal"[118].

El problema de lavado de activos en el Ecuador ha sido un tema de preocupación en los últimos años. Cabe recordar que el Ecuador entro en la famosa "lista negra" del GAFI en el 2010 por ser considerado un país con deficiencias estratégicas en los sistemas antilavado de activos y financiamiento del terrorismo; además, fue calificado como país no cooperante por el mismo organismo. El país logro salir de esta lista en el 2015[119]. El Ecuador, al poseer una economía dolarizada y al estar en el medio de dos naciones que se encuentran entre los mayores productores de droga a nivel mundial, es un país que ofrece muchos atractivos para que los criminales laven dinero en su territorio[120]. Estados Unidos a través de su Departamento de Estado (United States Deparment of State) emitió un reporte internacional en el 2016 sobre estrategias de control de narcóticos en el cuál situó al Ecuador como uno de los 88 países donde existe mayor actividad de blanqueo de capitales cuyo origen principalmente es el delito de narcotráfico[121]. En el plano internacional el lavado de activos representa un problema colosal ya que, según los reportes emitidos por la UNODC, las cifras de lavado de activo ascienden aproximadamente a 1.6 trillones de dólares a nivel mundial[122]. Este delito tiene carácter de ser transnacional ya que usualmente tiene incidencia en varias jurisdicciones.

El COIP prescribe el lavado de activos en el artículo 317 en los siguientes términos:

> **Art. 317**.- Lavado de activos. - La persona que en forma directa o indirecta:
>
> 1. Tenga, adquiera, transfiera, posea, administre, utilice, mantenga, resguarde, entregue, transporte, convierta o se beneficie de cualquier manera, de activos de origen ilícito.
> 2. Oculte, disimule o impida, la determinación real de la naturaleza, origen, procedencia o vinculación de activos de origen ilícito.
> 3. Preste su nombre o el de la sociedad o empresa, de la que sea socio o accionista, para la comisión de los delitos tipificados en este artículo.

---

[118] Alfonso Zambrano Pasquel. *Lavado de Activos: Aproximación desde la Imputación objetiva y la Autoría mediata.* Corporación de Estudios y Publicaciones (CEP): Quito, (2010), p. 39.
[119]Sara Ortiz. *El GAFI acompaño al Ecuador durante 5 años.* https://www.elcomercio.com/actualidad/gafi-ecuador-lavado-activos-sicariato.html (acceso: 27/02/2019).
[120] Galo Chiriboga Zambrano. *Lavado de Activos: Cifras del Lavado de Activos, Nuevas fuentes en el delito.* Revista Perfil Criminológico. Flacso Ecuador y Fiscalía General del Estado: Quito, (2015), p. 2.
[121] United States Department of State. Bureau of International Narcotics and Law Enforcement Affaris. *International Narcotics Control Strategy Report. Volume II. Money Laundering and Financial Crimes.* (2016), p. 112.
[122] Naciones Unidas Oficina contra la Droga y el Delito. *Recopilación de reglas y normas de las Naciones Unidas en la esfera de la prevención del delito y la justicia penal.* https://www.unodc.org/unodc/en/money-laundering/globalization.html (acceso: 27/02/2019)

4. Organice, gestione, asesore, participe o financie la comisión de los delitos tipificados en este artículo.
5. Realice, por sí mismo o por medio de terceros, operaciones y transacciones financieras o económicas, con el objetivo de dar apariencia de licitud a actividades de lavado de activos.
6. Ingrese o egrese dinero de procedencia ilícita por los pasos y puentes del país[123].

2.3.1 Análisis del tipo objetivo y subjetivo del delito de lavado de activos

Albán Gómez establece que "[l]os elementos objetivos con que se describe la conducta son elementos externos, que pueden ser apreciados fundamentalmente por los sentidos"[124]. Entre estos elementos objetivos se encuentra el núcleo o verbo rector, el cual en palabras del mismo autor este es "el elemento central de la tipicidad, el que determina y delimita el acto (acción u omisión) ejecutado por la persona"[125]. Este delito posee más de un núcleo o verbo rector, de la forma en la cual está tipificado en el COIP se pueden encontrar hasta 24 verbos rectores.

En cuanto al sujeto activo de este delito es un sujeto activo indeterminado ya que cualquier persona puede realizarlo, a diferencia de delitos con sujeto activo calificados tales como el peculado o enriquecimiento ilícito. El sujeto pasivo de este delito es la sociedad en sí y el Estado, ya que el bien jurídico que vulnera es el orden socio económico. La mayor parte de la doctrina considera que el lavado de activos es un delito pluriofensivo que vulnera varios bienes jurídicos, no solo el orden socio económico, aunque este ha sido considerado como el bien jurídico vulnerado primordial de este delito[126]. Los otros bienes jurídicos que se ven vulnerados con el lavado de activos son la salud pública, la administración de justicia, o la seguridad interior del Estado. Barriga Bedoya explica que "[e]l orden socioeconómico es […] bien jurídico protegido porque por cuanto el lavado de activos afecta la producción, distribución y consumo de bienes y servicios, la libre competencia del mercado; genera desconfianza en los sistemas financieros de los Estados"[127].

[123] Código Orgánico Integral Penal. Art. 317. Publicado en el Registro Oficial Suplemento No. 180 de 10 de febrero de 2014.
[124] Albán Gómez, Ernesto. *Manual de Derecho Penal Ecuatoriano. Parte Especial. Óp. cit.*, p. 146
[125] *Ibíd.*
[126] *Cfr.* Franklin Barriga Bedoya. *El lavado de activos en Iberoamérica y la necesidad de la armonización legislativa*. Instituto ecuatoriano de estudios para las relaciones internacionales: Quito, (2011), p. 49.
[127] *Ibíd*

El objeto material de este delito son los *activos*, que bien pueden estar constituidos por bienes, dinero, valores, etc[128]. Respecto al objeto material de este delito Zambrano Pasquel establece lo siguiente:

> Aparece igualmente como una exigencia del objeto material de la figura de blanqueo de capitales que los activos provengan o hayan sido obtenidos como consecuencia de la comisión de un delito […] allí está el *origen maculado* de los mismos. Entonces es cierto que *el vínculo entre el bien que se pretende legitimar y el delito previo es fundamental para la configuración del lavado* [129].

El tipo subjetivo de este delito es el dolo, ya que hay un claro designio de causar un daño por parte del sujeto activo. Cabe recalcar que este tipo de delito no puede poseer la modalidad de culpa ya que según lo prescrito por el Art. 27 del COIP la conducta culposa solo "es punible cuando se encuentra tipificada como infracción en este código"[130]. En la tipificación del lavado de activos no se puede encontrar indicio alguno que el legislador haya tipificado el elemento de culpa dentro de este tipo penal.

Este delito corresponde a un tipo penal abierto ya que el código detalla "sólo parte de las características de la conducta prohibida, reenviando al tribunal la tarea de completar las restantes"[131]. Es menester destacar que, a pesar de que el delito de lavado de activos es un delito autónomo, Fiscalía debe probar el origen ilícito de los activos los cuales provienen de una conducta criminal previa. En lo referente a los delitos subyacentes o conexos al lavado de activos Allan Schott establece que "[u]n delito subyacente al lavado de activos es la actividad delictiva que genera ganancias, las cuales una vez blanqueadas producen el delito de lavado de activos"[132]. El lavado de activos conlleva una problemática importante ya que cuando se logra blanquear activos de origen ilícito estos son frecuentemente utilizados por organizaciones criminales para financiar nuevos delitos. El GAFI estableció 20 categoría de delitos subyacentes en sus *cuarenta recomendaciones* las cuales son: 1. Participación en un grupo delictivo organizado y en asociaciones extorsivas, 2. Terrorismo, incluyendo el financiamiento de este, 3. Tráfico

---

[128] *Cfr*. Alfonso Zambrano Pasquel. *Lavado de Activos: Aproximación desde la Imputación objetiva y la Autoría mediata. Óp. cit.*, p. 46.
[129] *Ibíd*
[130] Código Orgánico Integral Penal. Art. 27. Publicado en el Registro Oficial Suplemento No. 180 de 10 de febrero de 2014.
[131] Liuver Camilo Momblanc. *Legalidad versus tipos penales abiertos en el Código Penal Cubano*. http://dx.doi.org/10.21503/lex.v11i11.12 (acceso: 27/2/2019), expresando las ideas principales de Francisco Muñoz Conde y Mercedes García Arán. *Derecho Penal. Parte General*. 2 da. edición. Revisada y puesta al día conforme al Código Penal de 1995. Editorial Tirant lo Blanch: Valencia, (1996).
[132] Paul Allan Schott. *Guía de referencia para el antilavado de activos y la lucha contra el financiamiento del terrorismo. Óp. cit.*, p. 57.

de seres humanos y tráfico ilícito de inmigrantes, 4. Explotación sexual, 5. Tráfico ilegal de estupefacientes y sustancias psicotrópicas, 6. Tráfico ilegal de armas, 7. Tráfico de mercancías robadas y otros bienes, 8. Corrupción y soborno, 9. Fraude, 10. Falsificación de dinero, 11. Falsificación y piratería de productos, 12. Delitos ambientales, 13. Homicidio, lesiones corporales graves, 14. Secuestro, privación ilegítima de la libertad y toma de rehenes, 15. Robo o hurto, 16. Contrabando, 17. Extorsión, 18. Falsificación, 19. Piratería, 20. Uso indebido de información confidencial o privilegiada y manipulación del mercado[133].

2.3.2 Etapas del proceso de lavado de activos

La doctrina internacional ha determinado que el proceso por el cual los criminales lavan dinero producto de sus actividades criminales está dividido en tres etapas; las cuales son la colocación, la estratificación u ocultamiento y la integración. A continuación, se explicará los pormenores de estas tres etapas.

Colocación: es la primera etapa del proceso la cual consiste en incorporar el dinero de procedencia ilegal al sistema formal, el cual puede ser el sistema comercial o financiero principalmente. En esta etapa las grandes cantidades de dinero deben de ser separadas o desligadas del ilícito o ilícitos perpetrados de los cuales provienen. Marengo resalta que en esta etapa "el blanqueador encuentra su mayor vulnerabilidad en el proceso debido fundamentalmente a las exigencias de identificación y control de operaciones por sobre un determinado umbral económico"[134]. Existen numerosos métodos utilizados para efectuar esta primera etapa, las más empleadas son el *smurfing* o pitufeo (fraccionar los fondos de dinero de origen ilícito en porciones más pequeñas para eludir los controles de instituciones financieras u otras entidades de fiscalización, por ejemplo, introducir el dinero sucio en varias cuentas bancarias en cantidades muy pequeñas y aparentemente insignificantes para que el banco no reporte dichas transacciones bancarias como operaciones inusuales o injustificadas (ROII) a la Unidad de Análisis Financiero y Económico (UAFE)), la utilización de empresas fantasma, la compra de inmobiliaria o su construcción, la compra de billetes de lotería o pasajes de viaje, y la compra de locales con gran circulación de efectivo (discotecas, bares, prostíbulos) y permitan la

[133] Grupo de Acción Financiera. Estándares Internacionales sobre la Lucha contra el lavado de activos y el financiamiento del terrorismo y la proliferación: Las Recomendaciones del GAFI. 2012. p. 116
[134] Federico Marengo. "Aspectos generales del lavado de activos: El lavado de activos y la financiación del terrorismo. La problemática en el mercado de capitales". Revista Pensamiento Penal. Mayo, 2011. p. 7

tergiversación de los números de venta de productos o servicios, es decir muestran en la contabilidad que han vendido más de lo que en realidad han efectuado, entre otros métodos[135].

Estratificación: esta etapa, también conocida como *layering*, consiste en "ocultar los productos ilícitos mediante la realización de numerosas transacciones para dificultar el seguimiento y conocer el origen de aquellos"[136]. A grandes trazos consiste en mover el dinero varias veces para distanciarlo de su fuente original y dificultar la detección por parte de las autoridades. Marengo explica que la estratificación "[s]e trata, […] de desconectar y quebrar el nexo que vincula con la primera y más sospechosa operación, utilizada para ingresar el dinero en los cauces legales"[137]. Barriga Bedoya describe que "[e]ntre las técnicas empleadas en esta fase se encuentran: creación de un rastro documental falso para ocultar la verdadera fuente de propiedad, la conversión del metálico en instrumentos financieros, adquisición de bienes materiales con dinero en metálico y su posterior cambio o venta, transferencias electrónicas, […]"[138].

Integración: esta etapa consiste en la incorporación de los fondos productos del ilícito en la economía legal para engañar a las autoridades al hacerles creer que dichos fondos fueron obtenidos por medios legítimos. Mediante la culminación de las dos fases anteriores se les confiere a estos fondos una apariencia de legitimidad con el propósito de obstaculizar cualquier proceso de inspección o fiscalización. En esta etapa se hace muy complicado diferenciar las ganancias legales de las ilegales. Algunas técnicas comunes empleados en esta etapa son: compra de inmuebles, compra de artículos de lujo o metales preciosos, empresas fachada, utilización de organizaciones sin fines de lucro, etc[139].

---

[135] *Cfr.* Franklin Barriga Bedoya. *El lavado de activos en Iberoamérica y la necesidad de la armonización legislativa. Óp. cit.*, p. 50. y *Cfr* Paul Allan Schott. *Guía de referencia para el antilavado de activos y la lucha contra el financiamiento del terrorismo. Óp. cit.*, p. 10. y *Cfr.* Alfonso Zambrano Pasquel. *Lavado de Activos: Aproximación desde la Imputación objetiva y la Autoría mediata. Óp. cit.*, p. 47.

[136] Franklin Barriga Bedoya. *El lavado de activos en Iberoamérica y la necesidad de la armonización legislativa. Óp. cit.*, p. 50.

[137] Federico Marengo. "Aspectos generales del lavado de activos: El lavado de activos y la financiación del terrorismo. La problemática en el mercado de capitales". *Óp. cit.*, p. 8.

[138] Franklin Barriga Bedoya. *El lavado de activos en Iberoamérica y la necesidad de la armonización legislativa. Óp. cit.*, p. 51.

[139] *Cfr* Alfonso Zambrano Pasquel. *Lavado de Activos: Aproximación desde la Imputación objetiva y la Autoría mediata. Óp. cit.*, p. 45.

2.3.3 Empleo de las criptomonedas para la comisión de lavado de activos

Existen numerosos métodos de lavar activos con criptomonedas, demasiados para ser analizados de forma detallada en la presente tesis. Por tal motivo, se ha escogido dos de los incontables métodos. Dichos métodos son los siguientes:

2.3.3.1 Empleo de cajeros automáticos de criptomonedas

Dado la creciente popularidad de las criptomonedas muchas empresas han montado negocios de cajeros automáticos para criptodivisas. En Ecuador hay por el momento dos cajeros automáticos de criptomonedas en la ciudad de Quito, ubicados en la oficina No. 410 del edificio Metropolitan. Estos cajeros ofrecen la compra y venta de criptomonedas como Bitcoin, Dash o Pura por dinero en efectivo[140]. El surgimiento de estos nuevos tipos de servicios para el criptomercado ha suscitado una creciente preocupación por parte de las autoridades al ver a los cajeros automáticos de criptomonedas como medios idóneos para que criminales laven dinero. Hay que recalcar que, al no existir regulaciones ni leyes claras a nivel global sobre el tratamiento que se le debe dar a las criptomonedas ni los servicios relacionados a estas, estos cajeros automáticos no cumplen con las regulaciones de KYC[141] o AML[142], ni con las normas establecidas en la Codificación de Resoluciones de la Superintendencia de Bancos y Seguros y de la Junta Bancaria que establecen las medidas de seguridad y debida diligencia que deben emplear las instituciones financieras para operar efectivamente[143].

El autor Hyman expone un ejemplo de como un criminal puede utilizar los cajeros automáticos de criptomonedas para blanquear los activos producto de sus actividades delictivas. Dicho autor pone el ejemplo de un narcotraficante que crea varias cuentas de Bitcoin, y ya que el único requisito para abrir una cuenta de Bitcoin es proporcionar un correo electrónico, este narcotraficante crea un correo electrónico que no corresponde con su verdadera identidad por cada cuenta de Bitcoin. A raíz de esto exige a sus compradores que paguen las transacciones en bitcoins a diferentes cuentas en montos pequeños (esto

[140] Carelin García. *Ecuador ya tiene su primer cajero automático de múltiples criptomonedas.* https://www.criptonoticias.com/mercados/ecuador-tiene-primer-cajero-automatic (acceso: 28/2/2019).
[141] Know Your Costumer/ Conozca Su Cliente
[142] Anti-Money Laundering/ Anti Lavado de Activos
[143] Codificación de Resoluciones de la Superintendencia de Bancos y Seguros y de la Junta Bancaria. Artículo 40. Suplemento del Registro Oficial No. 369 del 24 de enero de 2011.

para no levantar sospechas). A continuación, el narcotraficante utiliza una red de "mulas" que van a sacar poco a poco dinero en efectivo de las diversas cuentas de Bitcoin que posee. Adicionalmente puede hasta convertir sus ganancias en bitcoin en otras criptomonedas para encubrir aún más sus operaciones delictivas[144].

Los defensores acérrimos de las criptomonedas argumentan que un cajero automático tradicional también puede ser utilizado para lavar dinero; sin embargo, los cajeros automáticos regulares están sujetos a mayores controles, poseen un marco de regulación bien definido, y están atados a cuentas en bancos que poseen extensa información de los usuarios de dichas cuentas y las instituciones bancarias que manejan estas cuentas están sujetas a la fiscalización de órganos reguladores y de control. Las cuentas de criptomonedas no están atadas a nada ya que cabe recordar que unas de las principales características de las criptomonedas son la descentralización y el anonimato.

2.3.3.2 Empleo de *Mixers* o mezcladores de criptomonedas

Héctor Ruilova proporciona una explicación concisa y concreta sobre el funcionamiento y características de los mezcladores de criptomonedas. Dicha explicación es la siguiente:

> Un mezclador de criptomonedas es una herramienta que sirve para mejorar el anonimato de las transacciones. El algoritmo es bastante simple: un usuario envía sus criptomonedas a la dirección de un mezclador, el cual es registrado individualmente para cada usuario. Las monedas se mezclan con transacciones de otras personas o se distribuyen entre cientos de miles de carteras que pertenecen a un mezclador. Una vez que se completa el proceso, bitcoins "limpios" se transfieren a un almacenamiento preestablecido, ya sea de vuelta al remitente o al nuevo propietario.
>
> La distribución de fondos entre numerosas billeteras hace que sea imposible establecer un vínculo entre un emisor y un receptor. Un usuario también puede dividir la entrada de la transacción en denominaciones para ocultar la cantidad real[145].

La empresa CipherTrace Cryptocurrency Intelligence público un reporte sobre el panorama del lavado de dinero y la industria de las criptomonedas en las cuales indicaba que los mezcladores de criptomoneda represaban el mayor riesgo contra las regulaciones de antilavado de activos por la forma en la cual operan y su acceso se da de forma casi

[144] Mitchell Hyman. "Bitcoin ATM: A criminal´s laundromat for cleaning money". St. Thomas Law Review, Volume 296, (2015), p. 293.
[145] Hectór Ruilova. *Cómo funciona los mezcladores de criptomonedas y las billeteras anónimas.* https://www.academiablockchain.com/2018/04/04/como-funcionan-los-mezcladores-de-criptomonedas-y-las-billeteras-anonimas/ (acceso: 28/2/2019).

exclusiva a través de la deep web[146]. Los paralelismos con lo ocurrido con la red Silk Road son muy notorios. Esta empresa de inteligencia ha descubierto que algunos mezcladores de criptomonedas han llegado a implementar técnicas muy avanzadas para dificultar el rastreo de las criptomonedas lavadas. Tal es el caso de la mezcladora *BestMixer* que desarrollo un *spam* malicioso que operaba de la siguiente manera:

> Los usuarios de Bitcoin comenzaron a recibir cantidades mínimas de BTC de BestMixer junto con un mensaje que promocionaba el servicio de la compañía, este mensaje declaraba que BestMixer permite a los usuarios mezclar Bitcoin, Litecoin y Bitcoin Cash. Estas pequeñas transacciones esencialmente representaban una campaña de publicidad masiva, es decir, spam de cadena de bloques. Pero no se trataba simplemente de publicidad spam: al enviar Bitcoin a las direcciones BTC principales, BestMixer estaba contaminando efectivamente a estos usuarios al obligarlos a realizar transacciones con un mezclador a través de estas pequeñas transacciones. Al *desempolvar* cada dirección con fondos de un mezclador, la campaña tuvo el efecto de ensuciar la reputación de los usuarios. La razón para desempolvar tantas direcciones fue un intento de confundir las herramientas de análisis de blockchain para evitar las regulaciones AML. CipherTrace emitió una alerta en esta campaña, calificándola como "polvo criptográfico".[147]

Es decir, que para encubrir la red de usuarios que efectivamente estaban utilizando la mezcladora BestMixer, está mezcladora lanzó un *spam* que provoco que cientos de cuentas de usuarios Bitcoins que nunca habían utilizado estos servicios pareciera que, si lo habían utilizado, de esta forma intentaron engañar a las autoridades para que no puedan identificar cuáles eran las cuentas que si estaban lavando dinero a través de BestMixer.

Los profesores van Wegberg, Oerlemans y van Deventer de la universidad holandesa de Delft publicaron en el 2018 un estudio en el cuál se analizaba la efectividad de utilizar criptomonedas para lavar activos a través de estas plataformas de mezcladoras de cripto-divisas. Estos investigadores lograron encontrar más de 25.000 sitios web que ofrecían estos servicios. Los resultados de este estudio fueron alarmantes ya que pudieron comprobar que los servicios de las mezcladoras eran altamente eficientes y no dejaban ningún rastro de las transacciones realizadas por este equipo de investigadores[148].

---

[146] Ciphertrace Cryptocurrency Intelligence. *Cryptocurrency Anti-Money Laundering Report, 2018 Q4.* p.11.
[147] *Ibíd*
[148] Rolf van Wegberg, Jan-Jaap Oerlemans, y Oskar van Deventer. "Bitcoin money laundering: mixed results?: An explorative study on money laundering of cybercrime proceeds using bitcoin." Jou*rnal of Financial Crime*, Vol 25 (2018), pp. 419-435.

3 CAPÍTULO III: PANORAMA NORMATIVO INTERNACIONAL Y POSIBLES REGULACIONES APLICABLES AL ECUADOR

Este capítulo examina cuales han sido las diferentes posturas que los países alrededor del mundo han tomado a la hora de regular las criptomonedas. Se explicará que hay tres aproximaciones que se han dado al dilema de las criptomonedas: la inacción, la prohibición y la regulación. Se explicará qué países han tomado determinada postura y cuál de las diferentes aproximaciones al problema es la única que cumple con el objetivo de prevenir el uso delictivo de las criptomonedas. Posteriormente se dilucidará los mecanismos regulatorios que las naciones de Malta y Estados Unidos han implementado para reglar los negocios relacionados con las criptomonedas y sus tecnologías conexas. Finalmente se expondrá las medidas que el Ecuador debe tomar para prevenir los usos ilícitos de las criptodivisas.

3.1 Posturas de diferentes países en cuanto a la regulación de las criptomonedas

Una vez demostrado que las criptomonedas pueden ser utilizadas para la comisión de ilícitos es menester iniciar el análisis del segundo problema que esta tesis plantea. Dicho problema consiste en la siguiente interrogante; ¿qué disposiciones o mecanismos se deben poner en práctica para aplacar la utilización de las criptodivisas como herramientas auxiliares de la ejecución de delitos? Frente a esta interrogante los países han tomado diferentes posturas que se pueden agrupar en tres maneras diferentes de aproximarse al problema de las criptomonedas: la inacción, la prohibición y la regulación.

3.1.1 Inacción

Actualmente no existe un conceso a nivel internacional de cómo deben ser reguladas las criptomonedas. La mayoría de naciones no han elaborado normativa que reglamente los usos de las criptomonedas ya que aún resulta un desafío comprender todas las aristas que abarca esta nueva tecnología. Un gran número de países permiten el uso de las criptomonedas, pero no cuentan con un cuerpo legal normativo, ni con organismos de control que supervisen a las industrias que brindan servicios relacionados con estas. Algunos países incluso han manifestado que no consideran necesario regular las criptomonedas, tal es el caso de Finlandia, que en su momento declaró, a través de su Banco Central, lo siguiente:

> Bitcoin es un monopolio dirigido por un protocolo, lo que previene los aspectos negativos de los monopolios tradicionales, como el abuso del poder y la manipulación de precios para beneficio individual […] No hay necesidad de regularlo porque como sistema está comprometido al protocolo tal como es, y las tasas de transacción que le carga al usuario son determinados por los usuarios independientemente del esfuerzo de los mineros.[149]

A medida que transcurre el tiempo las naciones están comenzando a comprender el impacto, tanto positivo como negativo, de las criptomonedas. Por tal razón, cada vez se ve con más frecuencia países que abandonan su postura de inacción y ahora se enfocan en buscar soluciones a los desafíos de esta nueva tecnología. La postura de inacción no es la adecuada para resolver los efectos problemáticos de las criptomonedas ya que la falta de regulación provoca que las prácticas nocivas de las criptomonedas prosperen y no otorga la seguridad jurídica necesaria para que la industria crezca. El mercado actual busca que haya regulación clara y precisa sobre los usos permitidos de las criptomonedas y cómo los derechos de los usuarios estarán protegidos frente a esta nueva tecnología; al mismo tiempo el mercado busca que dichas regulaciones sean lo suficientemente flexibles para que no coarten el progreso y la innovación tecnológica.

3.1.2 Prohibición

La página web Coin Dance publicó un listado del estatus legal de Bitcoin en todos los países del mundo. Dicho informe detalla los países en los cuales Bitcoin y otras criptomonedas son consideradas ilegales, estos son: Bolivia, Argelia, Nepal, Bangladesh, Vietnam, Macedonia, Afganistán, Kirguistán, Qatar, y Vanuatu[150]. De todos estos países solo Bangladesh ha establecido sanciones para las personas que realicen transacciones con criptomonedas con penas de hasta 12 años de privación de la libertad[151].

La reacción normal cuando surge una tecnología disruptiva, en especial una que tiene usos potencialmente nocivos, es contemplarla con escepticismo e incluso temor. Es comprensible que las naciones tengan cautela a la hora de tratar con las criptomonedas u otras monedas virtuales considerando los antecedentes con Liberty Reserve o Silk Road. Sin embargo, las medidas prohibitivas que han tomado los países antes mencionados son cuanto menos cuestionables. Castigar con penas privativas de libertad el uso de las

[149] Carlos González. *Banco Central de Finlandia afirma que no es necesario regular Bitcoin.* https://www.criptonoticias.com/banca-seguros/banco-central-finlandia-afirma-no-necesario-regular-bitcoin/ (acceso: 26/5/2019).
[150]Coin Dance. *Bitcoin Legality by Country Summary*. https://coin.dance/poli/legality (acceso: 6/3/2019).
[151] *Ibíd*

criptomonedas es una violación a los principios fundamentales del Derecho Penal. Hay que recordar que el Derecho Penal es de mínima intervención, es decir que la aplicación de una ley penal debe ser de *ultima ratio*, solo ser aplicado en casos de gravedad extrema con el fin de salvaguardar bienes jurídicos protegidos. No todos los usos de las criptomonedas violentan bienes jurídicos, por lo tanto, sancionar estos usos de forma indiscriminada atenta contra los derechos de las personas. En palabras de Pérez Pinzón "La seguridad y la libertad de los ciudadanos no son amenazadas únicamente por los delitos, sino también, y generalmente en mayor medida, por penas excesivas y despóticas […]"[152]. Lo citado anteriormente describe a la perfección la situación de Bangladesh, ya que la imposición de penas de hasta 12 años de privación de la libertad es una medida de violencia estatal excesiva y desproporcionada.

También hay que recalcar que, pese a sus posibles usos delictivos, la tecnología de las criptomonedas ofrece una cantidad de ventajas y beneficios que no pueden ser ignorados. Esta tecnología no solo está generando un impacto en el sector financiero sino en sectores como servicios de salud, almacenamiento y distribución de datos, mejoramiento de procesos electorales, catastros y muchos más[153]. Estas naciones tienen que darse cuenta de que sus políticas de prohibición dirigidas a esta tecnología son inútiles ya que es imposible cerrar de forma definitiva el sistema Bitcoin de la misma forma que es imposible hacer lo mismo con el internet[154]. La mayoría de naciones que han prohibido Bitcoin son países de economías precarias que bien podrían utilizar esta tecnología como una nueva forma de impulsar sus ingresos, lo que mejoraría el poder adquisitivo de la población además de ser una nueva fuente de empleo para miles de personas. Si los criptoactivos y el *blockchain* llegan a convertirse en la nueva revolución tecnológica, de forma similar como sucedió con el internet, el prohibir su uso y no desarrollar una legislación que incentive su incorporación en el mercado implicará una gran desventaja

[152] Alvaro Orlando Pérez Pinzón. "Principios Fundamentales del Derecho Penal". *Revista de Derecho Penal y Criminología* (1989), p. 17.

[153] Serenity Gibbons. *10 ways cryptocurrency will make the world a better place.* https://due.com/blog/cryptocurrency-will-make-world-a-better-place/ (acceso: 6/3/2019); Andrew Gazdecki. *Five ways blockchain could change the world.* https://www.forbes.com/sites/forbestechcouncil/2018/09/07/five-ways-blockchain-couldchange-the-world/#5052df3873d7 (acceso: 6/3/2019); Anca Faget. *Here´s how blockchain will change the world.* https://coindoo.com/heres-how-blockchain-will-change-the-world/ (acceso: 6/3/2019); y Javier Saavedra. *Las criptomonedas cambiarán el mundo.* https://okdiario.com/opinion/criptomonedas-cambiaran-mundo-893608 (acceso: 6/3/2019).

[154] Bitcoinist. *11 countries where Bitcoin is still illegal.* https://bitcoinist.com/11-countries-bitcoin-still-illegal/ (acceso: 6/3/2019).

para estos países, los cuales tendrán una batalla cuesta arriba contra el resto de naciones que si fueron receptivas a las criptomonedas[155]. Para contrastar, muchos de las naciones más ricas del mundo (Suiza, Japón, Singapur) están en una competencia para convertirse en el centro del mundo *cripto*[156].

Algunos países han cambiado su postura inicial frente al Bitcoin ya que se han dado cuenta de la prohibición no era una opción viable. Alemania, Estonia y Colombia fueron países que hace algunos años se pronunciaron en contra de las criptomonedas y ahora están buscando la forma de implementarlas en sus sistemas financieros y de regularlas en cuerpos normativos[157]. El Banco de la República de Colombia se manifestó en 2014, a través de la Superintendencia Financiera, que rechazaba el Bitcoin ya que el peso colombiano es la única moneda dc curso legal autorizada por el gobierno[158]. Para septiembre de 2018 la misma entidad convoco un grupo de expertos para comenzar a redactar un proyecto de ley de regulación de criptoactivos[159].

En lo referente a la legalidad de las criptomonedas, Ecuador se presenta como un caso muy particular, ya que, de forma similar a Colombia, el Banco Central del Ecuador se pronunció mediante un comunicado enunciando que el uso del Bitcoin no está autorizado en el país al no ser moneda de curso legal[160]. Pero a diferencia de Colombia, Ecuador tenía un motivo ulterior para "prohibir" el Bitcoin, la iniciativa de crear su propia moneda electrónica[161]. Los detalles sobre esta coyuntura se detallarán más adelante.

---

[155] *Ibíd*
[156] *Ibíd*
[157] Coin Dance. *Bitcoin Legality by Country Summary*. *Óp. cit.*
[158] Semana. *¿El bitcoin es legal en Colombia?* https://www.semana.com/economia/articulo/bitcoin-legalidad-de-la-divisa-en-colombia/475730 (acceso: 7/3/2019).
[159] El Tiempo. *Los seis desafíos que impone regular a los criptoactivos en el país.* https://www.eltiempo.com/economia/sector-financiero/regulacion-de-las-criptomonedas-en-colombia-269694 (acceso: 7/3/2019).
[160] Banco Central del Ecuador. *Comunicado oficial sobre el uso del bitcoin*. https://www.bce.fin.ec/index.php/boletines-de-prensa-archivo/item/1028-comunicado-oficial-sobre-el-uso-del-bitcoin (acceso:7/3/2019).
[161] El Comercio. *Ecuador prohíbe bitcoin para crear su propia moneda digital.* https://elcomercio.pe/tecnologia/actualidad/ecuador-prohibe-bitcoin-crear-propia-moneda-digital-380017 (acceso: 7/3/2019).

3.1.3 Regulación

3.1.4 Naciones con regulaciones específicas para criptoactivos

A la presente fecha, Malta y Estados Unidos destacan por ser los países de mayor producción de legislación orientada hacia la regulación de las criptomonedas[162]. Sin embargo, la aproximación que tienen estos dos países a la hora de regular las criptomonedas es muy diferente. Por un lado, Malta ha creado legislación integral y especializada para las criptomonedas. Por su parte Estados Unidos no ha creado leyes especiales para la regulación de las criptomonedas, sino que ha buscado integrar las criptomonedas a sus leyes vigentes. A continuación, se revisará las particularidades de las legislaciones de Malta y Estados Unidos con el fin de identificar qué medidas normativas se han implementado para aminorar los riesgos asociados a las estafas y el lavado de activos, y cuál es la mejor aproximación regulatoria que se debe dar a las criptomonedas.

Malta: es mundialmente conocida como la *isla blockchain* entre los entusiastas de las criptomonedas ya que esta nación se ha destacado por ser muy receptiva a emprendimientos de tecnologías innovadoras y proveer muchas facilidades para que los negocios de criptomonedas prosperen. Malta ha sido el primer país del mundo en aprobar una legislación integral para las criptomonedas y la tecnología *blockchain.* En noviembre de 2018 entraron en vigencia la Ley de Activos Financieros Virtuales[163], Ley de Acuerdos y Servicios en Tecnología Innovadora[164], y Ley de Autoridad de Innovación Digital[165].

Su ley de Ley de Activos Financieros Virtuales está diseñada con el propósito de regular las ICO´s (la ley maltesa las agrupa en una categoría más amplia bajo el nombre de *Virtual Financial Asset Offerings* (*VFA Offerings*)). Está ley regula los VFA´s y ICO´s de forma muy similar a las Ofertas Públicas Primarias (IPO´s)[166]. La práctica común de cómo las legislaciones han regulado las IPO´s es solicitar a las empresas que van a realizar la oferta en el mercado bursátil que presenten un prospecto. El prospecto es un documento que su principal función es detallar información pertinente sobre la compañía como el nombre, razón social y nombre comercial del emisor, domicilio, calificación del riesgo,

[162] Ciphertrace Cryptocurrency Intelligence. *Cryptocurrency Anti-Money Laundering Report, 2018 Q4. Óp. cit.,* p. 14.
[163] *Initial Virtual Financial Asset Offerings and Virtual Financial Assets Act.*
[164] *Innovative Technology Arrangments and Services Act.*
[165] *Digital Innovation Authority Act.*
[166] Initial Public Offerings (IPO´s).

capital suscrito, monto y tipo de valores a emitir, etcétera[167]. En el caso de las ICO´s el equivalente al prospecto es un *white paper*, que cumple prácticamente las mismas funciones que un prospecto[168]. Las instituciones del mercado de valores usualmente son las encargadas de tratar con compañías que buscan hacer una IPO en el mercado bursátil.

Lo que ha hecho Malta mediante la implementación de estas leyes es crear una especie de mercado bursátil para criptoactivos con una entidad que regula todos los aspectos de dicho mercado. Esto lo ha realizado mediante la Ley de Autoridad de Innovación Digital, la cual ha creado la MDIA[169], un organismo autónomo el cual es la máxima autoridad de regulación de este nuevo mercado de criptoactivos. De esta forma las ICO´s son registradas en el registro virtual del MDIA y este organismo analiza los *whitepapers* de dichas ICO´s y les asigna una calificación de riesgo[170]. Está calificación sirve para que los inversores tengan una noción sobre la capacidad de cumplimiento de las ICO´s y el riesgo de invertir en estas empresas. De esta manera se reduce considerablemente el riesgo de ICO´s fraudulentas. Pero la MDIA no solo va a regular a las ICO´s sino que es la encargada de emitir licencias de operación de cualquier tipo de empresa que quieran efectuar transacciones con criptomonedas; esto incluye a los *exchanges*, los mineros y otros proveedores de servicios con criptomonedas[171].

Malta al ser parte de la Unión Europea tiene que cumplir con las directivas que la Unión expide sobre lucha contra lavado de activos y financiamiento del terrorismo ALD/CFT[172]. La Directiva 5 de la Unión Europea de lucha anti-lavado de activos (5AMLD) estableció una serie de guías para la implementación de un régimen ALD/CFT efectivo en lo que respecta a las criptomonedas. Malta ha tomado medidas que van incluso más allá de lo requerido por la Directiva 5 de la Unión Europea[173]. El registro virtual de la MDIA estará vinculado con la Unidad de Inteligencia Financiera Maltense, de esta

[167] Melissa Gabriela León Cárdenas y Miguel Ángel Pinto Caballero. *La Oferta Pública Inicial como Herramienta Alternativa para el Financiamiento de PYMES familiares en la Ciudad de Guayaquil*. Trabajo de titulación previo a la obtención del grado de Ingeniero en Comercio y Finanzas Internacionales. Universidad Católica de Santiago de Guayaquil. Guayaquil, (2016), p. 42.
[168] Joao dos Santos y Stefano Vranca. *Blockchain technology and Cryptocurrencies: Emerging Trends. Óp. cit.,* p. 106.
[169] Malta Digital Innovation Authority
[170] *Digital Innovation Authority Act.* Art. 4 y *Initial Virtual Financial Asset Offerings and Virtual Financial Assets Act.* Art. 3.
[171] *Digital Innovation Authority Act.* Art. 6.
[172] Regulaciones Anti Lavado de Dinero/Contra el Financiamiento del Terrorismo
[173] Jonathan Galea. *The effect of Bitcoin on money laundering law.* Tesis doctoral. Universidad de Malta. Malta, (2019), p. 27.

forma se planea tener un registro efectivo de las empresas que operan servicios relacionados con criptomonedas y se podrá dar un mejor seguimiento a las transacciones de criptodivisas. La MDIA también solicita a todas las empresas que desean operar servicios relacionados con criptomonedas que implementen controles ALD/CFT, es decir políticas de KYC[174], incluir a las empresas de servicios de criptomonedas como sujetos obligados a reportar operaciones sospechosas a la Unidad de Inteligencia Financiera, y otras medidas adicionales. Jonathan Galea, CEO de BitMalta y autor de "*The Effect of Bitcoin on Money Laundering Law",* estableció que parte de las mejoras que implementó Malta a los requerimientos de la 5AMLD fueron los siguientes:

> Parte del plan para un régimen de ALA / CFT más estricto incluye una regulación estricta de lo siguiente:
> • Servicios *exchanges* entre diferentes criptoactivos, para evitar la "estratificación" anónima de fondos para enmascarar su origen.
> • Plataformas que facilitan el intercambio de criptoactivos de igual a igual, lo que podría permitir transferencias anónimas de fondos entre individuos
> • Cajeros automáticos de criptoactivos, que podrían utilizarse de forma anónima para comprar criptomonedas[175].

La legislación de Malta en lo referente a criptomonedas es vista como el cuerpo normativo más completo que hay en la actualidad en cuanto a la regulación de esta nueva tecnología. Estos cuerpos normativos integrales regulan a los servicios de criptomonedas desde varias áreas del derecho tales como propiedad intelectual, competencia, contractual, penal, etcétera[176].

Sin embargo, la reputación de Malta está en entredicho ya que durante los últimos años ha sido objeto de investigaciones de lavado de activos por parte del Parlamento de la Unión Europea[177]. Cabe recordar que Malta también es una jurisdicción considerada como paraíso fiscal o régimen fiscal preferente por muchas de las legislaciones del mundo[178]. Pese a estos sucesos, el Informe del Índice de Anti Lavado de Activos de Basilea, el cuál mide el riesgo de lavado de activos y financiamiento del terrorismo, ubicó

[174] Know Your Costumer/ conoce a tu cliente
[175] Jonathan Galea. *The effect of Bitcoin on money laundering law. Ópt. cit.*, p. 122.
[176] Iván Gómez. *Malta se convierte en el primer país con una legislación integral para criptomonedas y contabilidad distribuida.* https://www.criptonoticias.com/regulacion/malta-convierte-primer-pais-legislacion-integral-criptomonedas-contabilidad-distribuida/ (acceso: 8/3/2019).
[177] Sobre la relación de Malta con el lavado de activos, *vid.* Reuters. *La EU revisará las medidas llevadas a cabo en Malta contra el blanqueo de dinero.* https://es.reuters.com/article/topNews/idESKBN1HU1ZA-OESTP (acceso: 8/3/2019); y Lyubov Pronina. *EU tells Malta to step up crackdown on Money Laundering by Banks.* https://www.bloomberg.com/news/articles/2018-11-08/eu-tells-malta-to-step-up-crackdown-on-money-laundering-by-banks (acceso: 8/3/2019).
[178] Ejemplo Resolución SRI No. NAC-DGERCGC 15-0000052 Paraísos y Regímenes fiscales preferentes Art. 2.

a Malta en el puesto 132 de 149 países evaluados. Esto quiere decir que Malta se encuentra entre el 11% por ciento de países con menor riesgo de lavado de activos[179].

Estados Unidos: fue el primer país del mundo en establecer una regulación específica para las criptomonedas a través de la BitLicense. En 2014 el Departamento de Servicios Financieros del Estado de Nueva York de los Estados Unidos emitió el reglamento para empresas que realicen actividades con criptomonedas o cualquier moneda virtual[180]. La BitLicense establece que todos los negocios que entren en la categoría de *Virtual Currency Business Activity* (VCBA) están sujetos a las regulaciones establecidas por la BitLicense y necesitan de un permiso operativo para poder llevar a cabo sus funciones económicas[181]. Davis Polk explica los requerimientos que establece la BitLicense a las empresas de VCBA son los siguientes:

1) Evaluación de riesgos: a. Evaluación de riesgos inicial y anual considerando los riesgos legales, de *compliance*, financieros y de reputación. b. El programa ALA/CFT debe reflejar la evaluación de riesgos.	**2. Función del *Compliance:*** a. Sistema de controles internos, políticas y procedimientos para garantizar el cumplimiento continuo de todas las leyes, normas y reglamentos ALA. b. Designar oficial(es) de cumplimiento ALA c. La junta general de directos debe revisar/aprobar las políticas generales de ALA. d. La NYDFS[182] considerará si el solicitante ha cumplido con las leyes contra el lavado de activos y con otras regulaciones pertinentes, como un factor en su determinación de si se debe otorgar una solicitud.
3. Función de auditoría: a. Evaluaciones anuales independientes para el cumplimiento y la efectividad del programa ALA por parte de personal calificado. Se incentiva que varias evaluaciones sean realizadas anualmente. b. El personal interno responsable del diseño, instalación, mantenimiento u operación del programa ALA, o las políticas y procedimientos que guían su operación, están	**4. Prohibiciones:** a. No estructuración/asistencia en la estructuración de transacciones para evadir los requisitos de informes. b. No permitir/facilitar la ofuscación o el ocultamiento de la identidad del cliente o contraparte. Ej.: i) Ej.- tumblers/mixers ii) Monedas virtuales creadas para ofuscar la identidad de las partes (Zcash, Monero)

[179] Índice ALA de Basilea. Instituto de Basilea sobre la Gobernanza. *Informe del Índice de ALA de Basilea 2016.* p. 5.
[180] Davis Polk. *New York´s Final "BitLicense" Rule: Overview and Changes from July 2014 Proposal.* https://www.davispolk.com/files/new_yorks_final_bitlicense_rule_overview_changes_july_2014_proposal.pdf (acceso 8/3/2019).
[181] Richard Levina, Aaron O`Birenb y Madiha Zuberic. *Real Regulation of Virtual Currencies.* Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data, (2015), p. 327.
[182] New York State Department of Financial Services/ Departamento de Servicios Financieros del Estado de Nueva York de los Estados Unidos

descalificados para realizar la función de auditoría. c. El informe de auditoría debe ser enviado a la NYDFS.	
5. Registros: a. Se debe mantener registros detallados durante al menos 7 años, los registros deben incluir la siguiente información: identidad y dirección física de los clientes/ titulares de cuentas, y, en la medida de lo posible, cualquier otra parte de la transacción; el monto o valor de la transacción (incluyendo la denominación, fecha de cuando la transacción fue iniciada y completada, descripción de la transacción y forma de pago)	**6. Informes:** a. Notificación obligatoria a la NYDFS dentro de 24 horas de la emisión de transacciones/ series de monedas virtuales que exceda los $10,000 en valor en un día. Informes CTR´s. b. Reporte de Operaciones Sospechosas (SAR) deben ser presentados dentro de los 30 días si el titular de la licencia no está sujeto a los requisitos federales de presentación de SAR.
7. Compliance de la OFAC (Office of Foreign Asset Control): a. Los clientes deben ser verificados en la lista de *Specially Designated Nationals* (SDN) mantenida por la OFAC. b. Políticas, procedimientos y prácticas basadas en el riesgo para garantizar el cumplimiento de las regulaciones de la OFAC "en la mayor medida posible".	**8. Programa de identificación del cliente:** a. identificación/ verificación de la identidad del cliente, incluido el nombre y la dirección física, cuando un cliente abre una cuenta o el titular de la licencia establece una relación de servicio con el cliente b. Políticas, procedimientos y controles de debida diligencia mejorados para los licenciatarios que no pertenecen a los extranjeros y para las cuentas de personas extranjeras. c. Verificación de la identidad de los titulares de cuentas que inicien transacciones de un valor superior a los $3.000

(Fuente Polk, 2015)[183]

Los requerimientos que establece la BitLicense en cuanto al cumplimiento de las políticas ALA/CFT están sujetas a las sanciones del *Bank Secrecy Act* el cuál es la ley sobre lavado de activos de Estados Unidos. La Red de Control de Delitos Financieros (FinCEN) está encargada de regular los negocios de servicios de dinero[184] (MSB´s) y prevenir y detectar el lavado de activos, el fraude, las estafas y otras prácticas ilegales. FinCEN emitió una guía sobre criptomonedas en 2015 en la cual agrupa a los servicios de criptomonedas como MSB´s por lo tanto todo negocio de servicios de criptomoneda tiene que registrarse con FinCEN como sujeto obligado. Las medidas que FinCEN solicita a las MSB´s son las mismas que están establecidas en la BitLicense.

[183] Davis Polk. *New York´s Final "BitLicense" Rule: Overview and Changes from July 2014 Proposal*. *Óp. cit.*
[184] Money services and business

3.2 Posible medidas y mecanismos para la regulación de las criptomonedas en el Ecuador

En junio de 2014 el Banco Central emitió un comunicado advirtiendo que el uso del Bitcoin en Ecuador no está autorizado debido a que el Bitcoin no es moneda de curso legal. La Junta de Política y Regulación Monetaria y Financiera comunicó a los medios que debido a disposición expresa del inciso 3 Art. 98 del Código Orgánico Monetario y Financiero el Bitcoin está prohibido en el país. Dicho artículo está prescrito de la siguiente manera:

> Art. 98. Prohibiciones. Se prohíbe de forma general: […]
> 3. La circulación y recepción de moneda y dinero no autorizados por la Junta de Política y Regulación Monetaria y Financiera[185].

En aquella ocasión el gobierno ecuatoriano, a través del Banco Central y la Junta de Política y Regulación Monetaria y Financiera, buscaba implementar la creación de dinero electrónico a través de la Resolución Administrativa No. BCE-037-2014. Las posteriores manifestaciones del Banco Central y de la Junta Monetaria se deben a que consideraban al Bitcoin como la competencia del dinero electrónico, entonces buscaron las formas de desincentivar el uso entre la población de esta criptomoneda[186]. El dinero electrónico del Ecuador no fue un proyecto exitoso debido a que nunca gozó de la confianza de la población ya que muchos expertos apuntaban que el gobierno podría aumentar la emisión del dinero electrónico indiscriminadamente y esto podría provocar inflación en la economía[187].

Posteriormente el lunes 8 de enero de 2018 el Banco Central a través de un comunicado oficial manifestó que, aunque el Bitcoin no es un medio de pago autorizado en el país, su compra y venta no está prohibida. Recalcó que el Bitcoin no está autorizado para el pago de bienes y servicios en el Ecuador[188]. Por lo tanto, se puede concluir que el uso de las criptomonedas en el Ecuador está restringido, pero no es ilegal.

---

[185] Código Orgánico Monetario y Financiero. Artículo 98. Suplemento del Registro Oficial No. 332 del 12 de septiembre de 2014.

[186] Mariano Puigvert. *¿Qué ha sido de la moneda digital de Ecuador?* https://www.criptonoticias.com/adopcion/que-ha-sido-de-la-moneda-digital-de-ecuador/ (acceso: 9/3/2019).

[187] María Laura Patiño. *El dinero electrónico, una apuesta peligrosa.* https://www.eluniverso.com/opinion/2016/06/01/nota/5610315/dinero-electronico-apuesta-peligrosa (acceso: 9/3/2019).

[188] Banco Central del Ecuador. *Comunicado oficial sobre el uso del bitcoin*. https://www.criptonoticias.com/adopcion/que-ha-sido-de-la-moneda-digital-de-ecuador/ (acceso: 9/3/2019).

Ahora bien, la implementación de las criptomonedas dentro de la economía ecuatoriana merece ser analizada con detenimiento. Si bien es cierto que las criptomonedas poseen usos potencialmente nocivos, también es cierto que albergan muchas virtudes que pueden impulsar la economía del país. El Ecuador posee una ventaja respecto a la mayoría de naciones latinoamericanas en cuanto a una posible adopción de las criptomonedas, ya que el Ecuador utiliza el dólar estadounidense como moneda de curso legal. La mayoría de los *exchanges* utilizan el dólar como tipo de cambio, por lo tanto, si el Ecuador incorporara negocios de criptomonedas a su mercado las transacciones y operaciones comerciales en el Ecuador serían mucho más rápidas y eficaces frente a la mayoría de países de Latinoamérica. La inversión extranjera estaría mucho más interesada en invertir en Ecuador que en otros países de la región. Por otro lado, los posibles riesgos que presentan las criptomonedas en cuestión de delitos son factores a considerar, ya que el Ecuador hasta el 2015 estaba en la lista de negra de GAFI y está en el medio de dos países con grandes producciones de narcotráfico. Si el Ecuador implementara negocios de criptoactivos en su economía estos negocios podrían ser empleados como mecanismos eficaces para que el narcotráfico lave su dinero. La solución a esta difícil problemática es implementar regulación y medidas efectivas que no coarten la innovación tecnológica pero que tengan pautas claras para prevenir, detectar y suprimir los riesgos delictivos asociados con las criptomonedas. A continuación, se proporcionará una serie de posibles medidas que se pueden poner en funcionamiento que cumplan con los dos propósitos antes mencionados.

3.2.1 Fiscalía Especializada contra la Ciberdelincuencia

Actualmente el Ecuador no posee un Fiscalía Especializada contra la Ciberdelincuencia ni ninguna unidad especializada dentro de las fiscalías existentes para la persecución de los delitos cibernéticos[189]. Países como Argentina, Paraguay, España, Alemania, Australia, Chile, entre otros ya han incorporado fiscalías especializadas en delitos informáticos y estas han demostrado ser útiles en la prevención, investigación y persecución de los ciberdelitos[190].

[189] Fiscalía General del Estado. Reglamento de las Nuevas Unidades de Gestión de Causas. Art.14. Registro Oficial Edición Especial 36 del 28 de abril de 2010.
[190] Amit Wadhwa y Neerja Arora. "A Review on Cyber Crime: Major Threats and Solutions". *International Journal of Advanced Research in Computer Science.* Vol. 5 No.8 (2017), pp. 4- 6.

La implementación de una Fiscalía Especializada contra la Ciberdelincuencia no solo ayudará a prevenir el uso delictivo de las criptomonedas, sino que contribuiría en la lucha contra todo tipo de delitos informáticos. La indagación y persecución de los ciberdelitos en el Ecuador se da principalmente a través de tres fiscalías especializadas: la Fiscalía Especializada en Soluciones Rápidas, la cual investiga delitos cibernéticos simples, tales como el hackeo de información de perfiles de redes sociales; la Fiscalía Especializada en Patrimonio Ciudadano la cual indaga sobre la apropiación ilícita de bienes ajenos mediante la utilización medios tecnológicos u otros semejantes, y; la Fiscalía Especializada en Delincuencia Organizada, la cuál uno de sus objetivos es la investigación y persecución de delitos cometidos por las cibermafias y organizaciones criminales que utilizan la red para ejecutar sus operaciones[191].

Las dificultades que poseen las instituciones obligadas a la persecución de estos delitos son varias. La primera de ellas es la insuficiente formación y entrenamiento que reciben los agentes llamados a la investigación y dirección de los procesos sobre delitos cibernéticos, esto incluye a los fiscales, secretarios, asistentes, peritos y la Policía Judicial que es el órgano auxiliar en la realización de la indagación delictiva. La segunda dificultad es la ausencia de infraestructura tales como centros de vigilancia computarizada y la falta de herramientas tecnológicas capacitadas para la detección de delitos informáticos[192]. La tercera problemática es la falta de cooperación y coordinación internacional con unidades de inteligencia, fiscalías y fuerza policial de otros Estados. Hay que recordar que los delitos cibernéticos tienen una naturaleza transfronteriza, por lo tanto, la ausencia de convenios internacionales de cooperación con otros países afecta negativamente al Ecuador. Actualmente la cooperación internacional existente se da a través de asistencias mutuas en materia penal, sin embargo, la asistencia entre países puede tardar meses[193]. La cooperación internacional se tratará más adelante a detalle como otra propuesta de medidas a implementarse para la prevención del uso delictivo de las criptomonedas.

---

[191] Fiscalía General del Estado. Reglamento de las Nuevas Unidades de Gestión de Causas. Art. 14- 23. Registro Oficial Edición Especial 36 del 28 de abril de 2010., y Sara Ortiz. *El rastreo de "hackers" en el Ecuador es limitado*. https://www.elcomercio.com/actualidad/rastreo-hackers-ecuador-limitado-ataque.html. (acceso: 28/5/2019).

[192] Santiago Acurio del Pino. *Derecho Penal Informático.* Corporación de Estudios y Publicaciones: Quito, (2015), p. 166-167.

[193] Fiscalía General del Estado. *Los Delitos Informáticos van desde el Fraude hasta el Espionaje.* https://www.fiscalia.gob.ec/los-delitos-informaticos-van-desde-el-fraude-hasta-el-espionaje/ (acceso: 28/5/2019).

La nueva Fiscalía Especializada sobre Ciberdelincuencia deberá poseer el personal adecuado que pueda: (a) comprender todos los pormenores que abarca la tecnología correspondiente a las criptomonedas, estar a la vanguardia de los cambios tecnológicos que surgen continuamente en el mundo de las divisas virtuales y estar preparados a adaptar sus actuaciones en conformidad con estos nuevos avances, (b) identificar los métodos y técnicas empleados por los ciberdelincuentes que se sirven de las criptodivisas, (c) conocer cuáles son los estándares internacionales que organismos como el GAFI solicitan implementar para combatir delitos beneficiados por la tecnología de los criptoactivos, y (d) poseer las herramientas, apoyo logístico y tecnología necesaria para la identificación, prevención y persecución de estos delitos. La capacitación de fiscales, asistentes, peritos y miembros de la policía judicial debe ser una prioridad. No deben estar capacitados únicamente en derecho penal o criminología, sino también poseer conocimientos de economía, mercado de valores, tecnología y otras ciencias complementarias y útiles para enfrentar todo lo relacionado a delitos cibernéticos. Asimismo, es importante recalcar que la capacitación sobre delitos informáticos y criptomonedas y su tecnología adyacente debe ser también proporcionada a Jueces.

Además de la implementación de una fiscalía especializada, la Fiscalía General del Estado debe comprender que la cooperación interinstitucional es un factor clave que no puede ser descuidada y no solo debe darse con otras instituciones públicas sino también con Universidades, Fundaciones, Institutos, etc[194]. Por añadidura se puede solicitar la asistencia de empresas de inteligencia especializadas en criptomonedas para la detección de los usos delictivos de estas. Por ejemplo, Malta, a través de su Oficina de Autoridad Servicios Financieros, se ha asociado con la empresa de seguridad e inteligencia criptográfica CipherTrace con el fin de monitorear toda actividad sospechosa en lo referente a criptomonedas[195]. Ecuador puede implementar medidas similares y beneficiarse de la industria privada en la prevención de usos delictivos de criptoactivos.

[194]Fiscalía General del Estado. *Dirección de Escuela de Fiscales*. https://www.fiscalia.gob.ec/direccion-de-escuela-de-fiscales/ (acceso: 28/5/2019).
[195] Business Wire. *Malta Financial Services Authority Partners with CipherTrace for Virtual Asset Business Compliance.* https://www.businesswire.com/news/home/20190311005582/en/Malta-Financial-Services-Authority-Partners-CipherTrace-Virtual (acceso: 28/5/2019)

3.2.2 Cooperación Internacional

El Convenio de Budapest sobre la Ciberdelincuencia de 2001 es el primer tratado internacional que pretende enfrentar la amenaza de la ciberdelincuencia a través de la cooperación internacional, el desarrollo de prácticas y técnicas de análisis e investigación, y el fomento de la armonización legislativa entre los países signatarios del convenio. Ecuador no ha ratificado el Convenio de Budapest[196].

Ecuador ha firmado instrumentos bilaterales, convenios, acuerdos y otros documentos de cooperación con Suiza, Paraguay, Colombia, Italia, Cuba[197]. Por su parte la República del Ecuador ha ratificado los siguientes instrumentos multilaterales sobre cooperación penal: 1. Convención Interamericana sobre asistencia mutua en materia penal de Nassau de 1992, 2. Convención de las Naciones Unidas contra la delincuencia organizada transnacional de Palermo de 2000, 3. Convención de las Naciones Unidas contra el tráfico ilícito de estupefacientes y sustancias psicotrópicas de Viena de 1988, 4. Convención Interamericana contra la corrupción, 5. Convención de las Naciones Unidas contra la Corrupción de 2003. Como se puede observar de lo expuesto anteriormente, el Ecuador no ha suscrito convenios directos de cooperación internacional con un gran número de países y según la Unión Internacional de Telecomunicaciones, el Ecuador ha sido uno de los países que menos pasos ha dado para la implementación de procesos efectivos dirigidos a la lucha contra el cibercrimen en Sudamérica[198]. Es por esta razón, que una de las medidas que se debe implementar para la prevención y persecución de delitos relacionados con las criptomonedas es que el Ecuador firme una mayor cantidad de tratados internacionales con otros países y ratifique el Convenio de Budapest sobre la Ciberdelincuencia. Al hacer esto el Ecuador establecería una red de cooperación internacional que pueda funcionar con mayor efectividad y celeridad.

Los procesos investigativos en lo referente a la ciberdelincuencia están condicionados a la obtención de evidencia digital. La evidencia digital, por sus características de intangibilidad y volatilidad, es extremadamente proclive a ser destruida o modificada en cuestión de segundos. Por lo tanto, las investigaciones que comprenden

[196] Convenio sobre la Ciberdelincuencia (2001).
[197] Fiscalía General del Estado. *Instructivo de cooperación penal internacional*. Dirección de Asuntos Internacionales de la Fiscalía General del Estado. Quito (2013), pp. 19-21.
[198] International Telecommunication Union. *Understanding Cybercrime: phenomena,challenges and legal response. September 2012.* pp. 186- 190.

delitos cibernéticos deben ser lo más diligentes, rigurosas y ágiles para que se pueda conservar dichas evidencias de una forma segura. Para tal efecto uno de los sistemas que mejor resultados ha proporcionado ha sido la implementación de canales o puntos de contactos 24x7 y redes de información y transferencia de datos digitales entre países[199]. Dado que el lugar de origen de los ciberdelitos y el lugar de ejecución de los mismos suele suceder en distintos Estados es esencial que haya mecanismos efectivos de cooperación internacional ágiles y que se acuerde con otras naciones los criterios específicos sobre la jurisdicción concurrente y competencia penal cuando estén involucrados dos o más países[200].

3.2.3 Medidas para evitar delitos de estafa y lavado de activos perpetrados por medio de las criptomonedas

En relación a la prevención de los delitos de lavado de activos y estafa, los cuales son el tema central de la presente tesis, el organismo encargado de la recopilación de información, realización de reportes, ejecución de políticas y estrategias nacionales de prevención y erradicación de estos delitos y otros delitos conexos es la Unidad de Análisis Financiero y Económico (UAFE)[201]. Si se llega poner en práctica negocios de criptomonedas en el Ecuador la UAFE tiene la potestad de declararlos como sujetos obligados según lo prescrito en el inciso c del Artículo 12 de la Ley de Prevención de Lavado de Activos. La UAFE debería requerir que todas las organizaciones que brinden servicios de criptomonedas u otras monedas virtuales obtengan una licencia de operación para poder llevar a cabo sus actividades económicas. Sería necesario crear un sistema similar al SISLAFT[202] para llevar un registro de las empresas y negocios que operan con criptomonedas. Los sujetos obligados estarían en el deber de emitir reportes RESU[203] y ROII[204] de las operaciones y transferencias que realizan sus clientes o proveedores. La UAFE también debería exigir a los negocios de criptomonedas que designen un oficial de cumplimiento dentro de su organigrama institucional que vele por el buen desempeño

[199] Cristos Velasco San Martín. *Jurisdicción y competencia penal en relación al acceso transfronterizo en materia de ciberdelitos.* Tirant Lo Blanch: Valencia, (2016) pp.382 -383.
[200] *Id*. p. 387.
[201] Ley Orgánica de Prevención, Detección y Erradicación del Delito de Lavado de Activos y del Financiamiento de Delitos. Artículo 12. Registro Oficial Suplemento 802 del 21 de julio de 2016.
[202] Sistema para la prevención de Lavado de Activos y Financiamiento del Terrorismo.
[203] Reporte Operaciones y Transacciones Sobre el Umbral.
[204] Reporte de Operaciones y Transacciones Inusuales e Injustificadas.

de las políticas y procedimientos para la prevención de lavado de activos.[205] Negocios tales como los *exchanges,* los mineros, y empresas que empleen cajeros automáticos de criptomonedas deberían estar obligados a obtener licencias de operación y emitir reportes a la UAFE. Los requisitos que se imponían en la BitLicense a las distintas empresas de criptomonedas que mencionamos anteriormente deberían también aplicarse en el Ecuador. El único servicio de criptomonedas que no puede ser permitido son los *mixers* ya que estos tienen como único propósito el aumentar el anonimato de las transacciones.

En el capítulo dos se estableció que en el delito de estafa los elementos objetivos del engaño y error son indispensables para que la conducta sea punible por el ordenamiento penal. Debido a la ignorancia que existe sobre el tema de las criptomonedas y el hecho que algunas personas que ven a las criptomonedas como medios idóneos para volverse ricos hacen que estás sean muy susceptibles a ser víctimas de estafas. Para evitar esto la transmisión transparente de información fidedigna por parte de las autoridades es crucial. Entre más educado esté el público sobre el tema de las criptomonedas más difícil será que sean víctimas de estafas, independientemente de que los estafadores intenten cometer sus objetivos a través de *smart contracts* o *Initial Coin Offerings*.

En cuanto al tema de la ICO´s la legislación maltesa es un buen referente sobre las medidas que se deben implementar para prevenir el uso ilícito de estas. Ecuador puede hacer igual que Malta y regular las ICO´s de forma similar a las Ofertas Públicas Primarias con todas las exigencias y requisitos que poseen las últimas, con especial énfasis en la calificación de riesgo que se debe asignar a cada ICO´s con el fin de que los inversionistas tengan una mayor certeza sobre los riesgos y beneficios que estas representan. A sí mismo, al igual que las Casas de Valor, los *exchanges* estarán obligados a proveer información a sus clientes sobre las contingencias que se pueden presentar en las operaciones, el valor volátil de las criptomonedas y otros *tokens*, y el resto de riesgos tecnológicos asociados a las criptodivisas. Para solucionar el problema que pueden representar los *smart contracts* fraudulentos la única solución por el momento es contar con una Fiscalía Especializada en Ciberdelincuencia que posea los mecanismos y herramientas adecuadas para la detección de estos programas informáticos perversos. Los estudios publicados por profesores de la Universidad de Cagliari, profesores e

[205] Manual Genérico UAFE. p.7

investigadores de la Universidad de Sun Yat-sen en China y otros centros de investigación, han demostrado que existe mecanismos y la tecnología adecuada para poder detectar *smart contracts* fraudulentos. Debido a que las criptomonedas y otras tecnologías contiguas representan ciertos riesgos a la seguridad, han surgido empresas de inteligencia tales como CipherTrace, Chainanlysis, Dark Trace, entre otras. De hecho, estas empresas de seguridad han comenzado a desarrollar Inteligencia Artificial capaz de detectar fraudes con criptomonedas[206]. La Fiscalía de Ciberdelincuencia puede apoyarse de los avances tecnológicos y servicios que estas empresas han desarrollado para la prevención de ilícitos cometidos mediante el uso de criptoactivos y otros delitos informáticos.

3.2.4 Otras medidas

Una ley especializada sobre criptomonedas y tecnologías similares es también un imperativo que se debe realizar. Dicha ley tendría que establecer los lineamientos sobre cuál es la naturaleza jurídica de las criptomonedas, cómo van han operar las empresas que comercian con esta tecnología y a que órganos de control deben de reportar sus actividades comerciales. Esta ley debe de especificar las diferentes regulaciones que se deben implementar a las distintas empresas y actividades comerciales que han surgido a raíz de la irrupción de las criptomonedas; esto es los *exchanges*, los mineros, las ICO´s, plataformas de *smart contracts*, etc. Dicha ley debería de cubrir los aspectos relevantes sobre derecho mercantil, societario, contractual, competencia, y demás ramas del derecho que sean aplicables en lo referente a criptomonedas. No es necesario una reforma de carácter sustantivo sobre delitos en la ley penal porque los tipos penales ya existen. Si toda la industria de las criptomonedas se encuentra regulada, se eliminaría la inseguridad que está relacionada con esta tecnología y esto provocaría una menor incidencia de delitos con criptoactivos.

[206] InfoCoin. *Desarrollan Inteligencia Artificial que puede detectar fraudes con criptomonedas.* http://infocoin.net/2019/01/08/desarrollan-inteligencia-artificial-que-puede-detectar-fraudes-con criptomonedas/ (acceso: 28/5/2019).

4 CAPÍTULO IV: CONCLUSIONES Y RECOMENDACIONES

1. Las criptomonedas fueron diseñadas para operar por un sistema de pagos descentralizados que emplea el método P2P. Las criptomonedas ofrecen un medio de transferencia de valor entre dos usuarios sin la participación de un intermediario, no poseen reconocimiento de moneda de curso legal y funcionan sin la intervención de ninguna autoridad gubernamental o entidad financiera. Toda la información personal de las transferencias está encriptada, lo que las hace anónimas, sin embargo, los datos de las transferencias son públicos en un libro contable *blockchain* que a su vez se encuentra distribuido en todos los nodos de la red. Es decir, las características básicas de las criptomonedas son: la descentralización, el anonimato, la transferencia de valor instantáneo y la desintermediación. Estas características las convierten en instrumentos ideales para la comisión de delitos.

2. De todos los delitos que han proliferado en los últimos años facilitados por las criptomonedas hay primordialmente dos delitos que han causado la alerta de las autoridades, estos delitos son el lavado de activos y la estafa.

3. Los criminales han utilizado principalmente dos métodos para la ejecución del delito de estafa usando la tecnología de las criptomonedas. Estos métodos son el empleo de ICO´s fraudulentas y la utilización de *smart contracts* fraudulentos. Los delincuentes utilizan las ICO´s y los *smart contracts* como esquemas Ponzi en orden de defraudar a los inversionistas. Los esquemas Ponzi, o estafas piramidales funcionan captando de forma constante a nuevos inversionistas para que con el capital aportado por los últimos se les paga a los primeros inversores.

4. Los criminales han utilizado principalmente dos métodos para la comisión del delito de lavado de activos empleando la tecnología de las criptomonedas como medio auxiliar. En cuanto al lavado de activos existen numerosos métodos para cometer este delito con criptomonedas. El primero de ellos es la utilización de cajeros automáticos de criptomonedas ya que estos carecen de regulación o leyes aplicables y por lo tanto no cumplen con requisitos de seguridad apropiados. El segundo método empleado para la comisión de este ilícito es utilizar mezcladoras de criptoactivos llamadas *mixers*. Los *mixers* son herramientas que sirven para aumentar el nivel de anonimato de una transacción con criptomonedas. La forma por la cual opera un *mixer* es mezclando las monedas de una transacción con otras transacciones de otras personas o distribuir entre cientos de carteras de criptomonedas que pertenecen a este *mixer*.

5. Los riesgos que suponen las criptomonedas al poseer características que facilitan la comisión de ilícitos ha llevado a los países a tomar tres posturas diferentes en cuanto al regulación de las criptomonedas. Estas tres posturas son: inacción, prohibición, y regulación. De todas estas posturas la única que puede llegar a cumplir con el objetivo de prevenir el uso delictivo de las criptomonedas es la regulación.

6. La prohibición de las criptomonedas, acompañada de la implementación de sanciones que no distinguen de un uso legítimo o delictivo de ellas, atenta contra el principio de mínima intervención del derecho penal ya que no todos los usos de las criptomonedas constituyen un ataque contra bienes jurídicos protegidos.

7. Existen dos naciones con regulaciones extensas y específicas sobre criptomonedas las cuales son Malta y Estados Unidos. Malta ha creado legislación integral sobre las criptomonedas y está posee la virtud de regular en los criptoactivos en todos los campos del derecho. La principal novedad de la legislación maltesa es la regulación de las ICO´s de forma análoga a las Ofertas Públicas Primarias. Estados Unidos por el otro lado ha desarrollado la BitLicense, la cual obliga a las empresas que van a operar con criptomonedas a cumplir restrictos de control tales como programas de identificación del cliente, evaluación de riesgos. Si el Ecuador decide incorporar las criptomonedas a la economía nacional las regulaciones implementadas por Malta y Estados Unidos pueden servir como un marco de referencia útil para la integración de las monedas virtuales en el Ecuador.

8. Las medidas que debe implementar el Ecuador para la adopción de las criptomonedas y la prevención del uso delictivo de estas son: 1. La creación de la Fiscalía Especializada contra la Ciberdelincuencia la cual no solo será útil para mitigar los delitos relacionados con las criptodivisas sino también será beneficioso en el combate de la ciberdelincuencia. Dicha fiscalía debe contar con el personal adecuado para el combate de los ciberdelitos, esto es tener fiscales, secretarios, asistentes, peritos capacitados sobre el tema y que cuenten con herramientas necesarias y adecuadas para perseguir este tipo de ilícitos; la capacitación de jueces también es crucial para cumplir los objetivos antes establecidos, 2. El Ecuador debe mejorar sus sistemas de cooperación internacional en materia penal, esto implica firmar el Convenio de Budapest sobre las Ciberdelincuencia del 2001 y establecer instrumentos bilaterales con más países, 3. La UAFE tiene que declarar como sujetos obligados a las industrias y organismos que negocien con criptomonedas y así poner requisitos de operación, la emisión de reportes dirigidos a la UAFE tales como el RESU o ROII y que cumplan con las normas ALA/CFT.

9. Todas las medidas implementadas tienen que ir a la par de proporcionar más información al público sobre las criptomonedas, de esta forma el delito de estafa mediante criptomonedas podría ser prevenido. La estafa cuenta con los elementos objetivos del engaño y el error, por lo tanto, entre más conocimiento posea una persona menos probabilidades hay de que está pueda llegar a ser víctima de una estafa.

10. Por último, una medida adicional que es un imperativo para la incorporación de las criptodivisas en el país es la implementación de una ley especializada sobre esta tecnología que establezca parámetros claros sobre la naturaleza jurídica de las criptomonedas, las regulaciones que deben ser implementadas por las empresas que van a proveer servicios relacionados con los criptoactivos, y regular las diferentes industrias de esta tecnología tales como los *exchanges,* las plataformas de smart contracts, los mineros, las ICO´s, etc.

5 BIBLIOGRAFÍA

Acevedo Eliana, y Rodríguez, Raíza. *Análisis del Bitcoin como técnica usada para el blanqueo de capitales en el sistema de Panamá*. III Congreso Investigación, Desarrollo e Innovación de la Universidad Internacional de Ciencia y Tecnología, (2018), pp. 231-253.

Act No. XXXI of 2018, Establishment of the Malta Digital Innovation Authority. Government Gazzete of Malta. No. 72,454- 20,7, 2018. Art. 4.

Act No. XXX of 2018, Initial Virtual Financial Asset Offerings and Virtual Financial Assets. Government Gazzete of Malta. No. 73,454-20,7,2018. Art. 3.

Acurio del Pino, Santiago. *Derecho Penal Informático.* Corporación de Estudios y Publicaciones: Quito, (2015), p. 166-167.

Albán Gómez, Ernesto. *Manual de Derecho Penal Ecuatoriano. Parte Especial. Tomo I.* 1era. Ed. Quito: Ediciones Legales EDLE S.A, 2018.

Albán Gómez, Ernesto. *Manual de Derecho Penal Ecuatoriano. Parte General.* 3era. Ed. Quito: Ediciones Legales EDLE S.A, 2018.

Asner, Matthew y Mitter, Alex. A White-Collar Lawyer's Guide to Virtual Currency. White Collar Crime Report, 09 WCR 158, 03/07/2014. http://www.bna.com

Assange, Julian, Appelbaum, Jacob, Muller-Maguhn, Andy y Zimmermann, Jeremie. *Cypherpunks: La libertad y el Futuro de Internet.* 1era. Ed. Barcelona: Deusto, 2012.

Banco Central del Ecuador. Comunicado oficial sobre el uso del bitcoin. https://www.bce.fin.ec/index.php/boletines-de-prensa-archivo/item/1028-comunicado-oficial-sobre-el-uso-del-bitcoin

Barriga Bedoya, Franklin. *Lavado de activos en Iberoamérica y la necesidad de la armonización legislativa.* Ed. Quito: Instituto Ecuatoriano de Estudios Para Las Relaciones Internacionales, 2011.

Bartoletti, Massimo, Carta, Salvatore, Cimoli, Tiziana y Saia, Roberto. *Dissecting Ponzi Schemes on Ethereum: Identification, analysis, and impact.* Dipartimento di Matematica e Informatica- Università di Cagliari. Cagliari, (2017), pp. 2-35.

BBVA. Qué es un "token" y para qué sirve. https://www.bbva.com/es/que-es-un-token-y-para-que-sirve/

Bitcoin Foundation. FAQ. https://bitcoin.org/es/faq#seguridad

Bitcoinist. 11 countries where Bitcoin is still illegal. https://bitcoinist.com/11-countries-bitcoin-still-illegal/

Bit2Me. ¿Por qué el Bitcoin tiende a la deflación? https://academy.bit2me.com/deflacion-en-bitcoin/

Blockchain Technologies. Smart Contracts Explained. https://www.blockchaintechnologies.com/smart-contracts/

Brill, Allan y Keene, Lonnie. "Cryptocurrencies: The Next Generation of Terrorist Financing?". *Defence Against Terrorism Review*. Vol 6. No. 1, Spring & Fall (2014), pp. 7- 30.

Castillo, María Angelina y Maisanche, Fabián. Indígenas del país denuncian estafa masiva con "criptomonedas".

https://www.elcomercio.com/actualidad/indigenas-denuncian-estafa-criptomonedas-bitcoin.html

Cawrey, Daniel. Charlie Shrem Indicted on Federal Charges for Money Laundering. https://www.coindesk.com/charlie-shrem-indicted-federal-charges-money-laundering

Ciphertrace Cryptocurrency Intelligence. *Cryptocurrency Anti-Money Laundering Report, 2018 Q4.*

Chainalysis. *Crypto Crime Report: Decoding increasingly sophisticated hacks, darknet markets, and scams, January 2019.* pp. 3- 29.

Chein, Weili, Zheng, Zibin, Cui, Jiahui, Ngai, Edith, Zheng, Peilin, Zhou, Yuren. *Detecting Ponzi Schemes on Ethereum: Towards Healthier Blockchain Technology.* Sun Yat-sen University Guanzhou, China, (2018), pp. 12-65.

Chiriboga Zambrano, Galo. "Lavado de Activos: Cifras del Lavado de Activos, Nuevas fuentes en el delito". *Revista Perfil Criminológico* No. 14 (2015), pp. 2-16.

Codificación de Resoluciones de la Superintendencia de Bancos y Seguros y de la Junta Bancaria. Artículo 40. Suplemento del Registro Oficial No. 369 del 24 de enero de 2011.

Código Orgánico Integral Penal. Registro Oficia No. 180 de 10 de febrero de 2014.

Código Orgánico Monetario y Financiero. Artículo 98. Suplemento del Registro Oficial No. 332 del 12 de septiembre de 2014.

Código Penal Español. Ley Orgánica 1&2/2015. Boletín Oficial del Estado, 10 de agosto 2015, núm. 243, pp. 89411 a 89530.

Coin Dance. Bitcoin Legality by Country Summary. https://coin.dance/poli/legality

Coindesk. Bitcoin Price (BTC). https://www.coindesk.com/price/bitcoin

Coindesk. Ethereum Price Index. https://www.coindesk.com/price/ethereum

Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional (2000) Artículo 6.

Corte Nacional de Justicia. Primera Sala de lo Penal. Juicio No. 014-2010. Registro Oficial Suplemento 26, 22 de Julio del 2013.

Davis Polk. New York´s Final "BitLicense" Rule: Overview and Changes from July 2014 Proposal. https://www.davispolk.com/files/new_yorks_final_bitlicense_rule_overview_changes_july_2014_proposal.pdf

Díaz, Genny. *Qué son los tokens y cómo se diferencian de las criptomonedas.* https://www.criptonoticias.com/colecciones/que-son-tokens-como-diferencian-criptomonedas

Donna, Edgardo Alberto. *Derecho Penal: Parte Especial Tomo II-B.* 2nda Ed. Buenos Aires: Rubinzal- Culzoni, 2007.

dos Santos, Joao y Vranca, Stefano. "Blockchain technology and Cryptocurrencies: Emerging Trends". *Expert Witnesses*. Vol 14, No. 2, (2018), pp. 104-147.

Dowlat, Sherwin. Cryptoasset Market Coverage Initiation Valuation. https://research.bloomberg.com/pub/res/d37g1Q1hEhBkiRCu_

Dragon Coin. Token Sale. https://tokensale.drgtoken.io

El Comercio. Ecuador prohíbe bitcoin para crear su propia moneda digital. https://elcomercio.pe/tecnologia/actualidad/ecuador-prohibe-bitcoin-crear-propia-moneda-digital-380017

El Tiempo. Los seis desafíos que impone regular a los criptoactivos en el país. https://www.eltiempo.com/economia/sector-financiero/regulacion-de-las criptomonedas-en-colombia-269694

Faget, Anca. Here´s how blockchain will change the world. https://coindoo.com/heres-how-blockchain-will-change-the-world/

Fernández Esteban, Cristina. Por qué sube y baja el precio del Bitcoin. https://www.ticbeat.com/innovacion/fintech/por-que-sube-y-baja-el-precio-del-bitcoin/

Fiscalía General del Estado. Dirección de Escuela de Fiscales. https://www.fiscalia.gob.ec/direccion-de-escuela-de-fiscales/

Fiscalía General del Estado. Instructivo de cooperación penal internacional. Dirección de Asuntos Internacionales de la Fiscalía General del Estado. Quito (2013), pp. 19-21

Fiscalía General del Estado. Los Delitos Informáticos van desde el Fraude hasta el Espionaje. https://www.fiscalia.gob.ec/los-delitos-informaticos-van-desde-el-fraude-hasta-el-espionaje/

Fiscalía General del Estado. Reglamento de las Nuevas Unidades de Gestión de Causas. Registro Oficial Edición Especial 36 del 28 de abril de 2010.

Fontán Balestra, Carlos. *Tratado de Derecho Penal. Tomo VI: Parte Especial*. La Ley: 1er Ed. Buenos Aires: Abeledo Perrot, 2013.

Galea, Jonathan. *The effect of Bitcoin on money laundering law.* Tesis doctoral. Universidad de Malta. Malta, 2019.

García, Carelin. Ecuador ya tiene su primer cajero automático de múltiples criptomonedas. https://www.criptonoticias.com/mercados/ecuador-tiene-primer-cajero-automatic

Gazdecki, Andrew. Five ways blockchain could change the world. https://www.forbes.com/sites/forbestechcouncil/2018/09/07/five-ways-blockchain-couldchange-the-world/#5052df3873d7

Gibbons, Serenity. 10 ways cryptocurrency will make the world a better place. https://due.com/blog/cryptocurrency-will-make-world-a-better-place/

Gómez, Iván. Malta se convierte en el primer país con una legislación integral para criptomonedas y contabilidad distribuida. https://www.criptonoticias.com/regulacion/malta-convierte-primer-pais-legislacion-integral-criptomonedas-contabilidad-distribuida/

González, Carlos. Banco Central de Finlandia afirma que no es necesario regular Bitcoin. https://www.criptonoticias.com/banca-seguros/banco-central-finlandia-afirma-no-necesario-regular-bitcoin/

Greenberg, Andrew. Silk Road 2.0 Launches, Promising A Resurrected Black Market Fort the Dark Web. https://www.forbes.com/sites/andygreenberg/2013/11/06/silk-road-2-0launches-%20promising-a-resurrected-black-market-for-the-dark-web/#68835cf42ed8

Grupo BTC. *El Bitcoin.*

Grupo de Acción Financiera. Estándares Internacionales sobre la Lucha contra el lavado de activos y el financiamiento del terrorismo y la proliferación: Las Recomendaciones del GAFI. 2012.

Gutiérrez Zarza, María Ángeles. "Investigación y enjuiciamiento de los "delitos de cuello blanco" en el sistema judicial norteamericano". *Anuario de Derecho Penal, Vol.L,* (1997), pp.579-653

Hyman, Mitchell. "Bitcoin ATM: A criminal´s laundromat for cleaning money". *St. Thomas Law Review*, Volume 296, (2015), pp. 287- 308.

InfoCoin. Desarrollan Inteligencia Artificial que puede detectar fraudes con criptomonedas. http://infocoin.net/2019/01/08/desarrollan-inteligencia-artificial-que-puede-detectar -fraudes-con-criptomonedas/

Instituto de Basilea sobre la Gobernanza. Informe del Índice de ALA de Basilea 2016.

Instituto Nacional de Tecnologías de la Comunicación. Bitcoin una moneda Criptográfica. https://www.incibecert.es/sites/default/files/contenidos/estudios/doc/int_bitcoin.pdf

International Telecommunication Union. *Understanding Cybercrime: phenomena, challenges and legal response. September 2012.* pp. 1- 366.

Kaplanov, Nikolei. "Nerdy Money: Bitcoin, The Private Digital Currency, and the Case Against its Regulation" *Loyola Consumer Law Review* Vol.25 (2012), pp.12-58.

Lara Lara, John Alexander y Muñoz Agudelo, Manuel Alejandro. "Análisis de los Principales Elementos del Bitcoin como Criptomoneda y Producto Commodity en el Comercio Nacional". Bogotá: Universidad de La Salle, 2017.

León Cárdenas, Melissa Gabriela y Pinto Caballero, Miguel Ángel. *La Oferta Pública Inicial como Herramienta Alternativa para el Financiamiento de PYMES familiares en la Ciudad de Guayaquil*. Tesis de grado. Universidad Católica de Santiago de Guayaquil. Guayaquil, 2016.

Levina, Richard, O`Birenb, Aaron y Zuberic, Madiha. *Real Regulation of Virtual Currencies. Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data*, 1era Ed. Nueva York: Elsevier, 2015.

Ley Orgánica de Prevención, Detección, y Erradicación del Delito de Lavado de Activos y Del Financiamiento de Delitos. Registro Oficial Suplemento No. 802 de 21 de julio de 2016.

López Alejandro. (2015). *Implicaciones jurídicas del uso del bitcoin en Colombia. Validez del contrato de compraventa comercial con bitcoins.* Universidad de Nariño.

Maisanche, Fabián. Los indígenas de Cotopaxi denuncian una estafa masiva y captación ilegal de dinero en plataformas digitales. https://www.elcomercio.com/actualidad/indigenas-cotopaxi-denuncian-estafa-criptomoneda.html

Mann, Joseph. El Desafío de Llegar a la Población no Bancarizada. http://latintrade.com/es/el-desafio-de-llegar-a-la-poblacion-no-bancarizada/

Marengo, Federico. “Aspectos generales del lavado de activos: El lavado de activos y la financiación del terrorismo. La problemática en el mercado de capitales”. *Revista Pensamiento Penal*. Mayo, 2011.

Marian, Omri. “Are Cryptocurrencies 'Super' Tax Havens?”. *Michigan Law Review*, Vol 112, (2013), pp. 38-48.

Maya Arroyo, Bernardo. *Delimitación entre el delito de estafa y el dolo civil como vicio del consentimiento.* Tesis pregrado. Universidad San Francisco de Quito. Quito, 2014.

Momblanc, Liuver Camilo. Legalidad versus tipos penales abiertos en el Código Penal Cubano. http://dx.doi.org/10.21503/lex.v11i11.12

Moore, Tyler, Han, Jie y Clayton, Richard. “The postmodern ponzi scheme: empirical analysis of high-yield investment programs”. *Financial Cryptography and Data Security*. ed. Springer, Heidelberg (2012), pp. 18-48.

Murphy, Austin. An Analysis of the Financial Crisis of 2008: Causes and Solutions. http://dx.doi.org/10.2139/ssrn.1295344

Naciones Unidas Oficina contra la Droga y el Delito. Recopilación de reglas y normas de las Naciones Unidas en la esfera de la prevención del delito y la justicia penal. https://www.unodc.org/unodc/en/money-laundering/globalization.html

Nakamoto, Satoshi. Bitcoin: A Peer-to Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf

Nava Garcés, Enrique Alberto. *Análisis de los Delitos Informáticos*. 1era Ed. Ciudad de México: Porrúa, 2005.

Neisius, Jen y Clayton, Richard. “Orchestrated crime: the high yield investment fraud ecosystem”. *Financial Cryptography and Data Security.* ed. AL. Birmingham (2014), pp. 87-94.

Normas de Prevención de Lavado de Activos Financiamiento del Terrorismo y otros Delitos. Registro Oficial Suplemento No. 396 de 28 de diciembre de 2018.

Ortiz, Sara. El GAFI acompaño al Ecuador durante 5 años. https://www.elcomercio.com/actualidad/gafi-ecuador-lavado-activos-sicariato.html

Ortiz, Sara. El rastreo de “hackers” en el Ecuador es limitado. https://www.elcomercio.com/actualidad/rastreo-hackers-ecuador-limitado-ataque.html (acceso 28/5/2019).

Pandacoin. Pandacoin. https://digitalpandacoin.org

Patiño, María Laura. El dinero electrónico, una apuesta peligrosa. https://www.eluniverso.com/opinion/2016/06/01/nota/5610315/dinero-electronico-apuesta-peligrosa

Pastor Muñoz, Nuria y Coca Vila, Ivó. *Lecciones de Derecho Penal. Parte Especial*. 4ta Ed. Barcelona: Atelier, 2015.

Pérez Pinzón, Álvaro Orlando. “Principios Fundamentales del Derecho Penal”. *Revista de Derecho Penal y Criminología* (1989), p. 17.

Pérez López, Xesús. “Las Criptomonedas: consideraciones generales y empleo de las criptomonedas como instrumento de blanqueo de capitales en la Unión Europea y en España”. *Revista de Derecho Penal y Criminología* 3/18 (2017), pp.141-187.

Pitta, Julie. Requiem for a Bright Idea. https://www.forbes.com/forbes/1999/1101/6411390a.html#436b692715f6

Pronina, Lyubov. EU tells Malta to step up crackdown on Money Laundering by Banks. https://www.bloomberg.com/news/articles/2018-11-08/eu-tells-malta-to-step-up-crackdown-on-money-laundering-by-banks

Puigvert, Mariano. ¿Qué ha sido de la moneda digital de Ecuador? https://www.criptonoticias.com/adopcion/que-ha-sido-de-la-moneda-digital-de-ecuador/

RCN noticias. Mercados Financieros caen tras inesperada elección de Trump como presidente de EE.UU. https://noticias.canalrcn.com/internacional-economia/mercados-financieros-caentrasinesperada-eleccion-trump-presidente-eeuu

Reglamento de Contrataciones del Consejo Nacional Contra el Lavado de Activos y de la Unidad de Inteligencia Financiera. Registro Oficial No. 58 de 5 de abril de 2007.

Resolución SRI No. NAC-DGERCGC 15-0000052 Paraísos y Regímenes fiscales preferentes Art. 2.

Reuters. La EU revisará las medidas llevadas a cabo en Malta contra el blanqueo de dinero. https://es.reuters.com/article/topNews/idESKBN1HU1ZA-OESTP

Rimkus, Ron. The Financial Crisis of 2008. https://www.econcrises.org/2016/08/17/the-financial-crisis-of-2008/

Ruilova, Hectór. Cómo funciona los mezcladores de criptomonedas y las billeteras anónimas. https://www.academiablockchain.com/2018/04/04/como-funcionan-los-mezcladores-de-criptomonedas-y-las-billeteras-anonimas/

Saavedra, Javier. Las criptomonedas cambiarán el mundo. https://okdiario.com/opinion/criptomonedas-cambiaran-mundo-893608

San Martín, Cristos Velasco. *Jurisdicción y competencia penal en relación al acceso transfronterizo en materia de ciberdelitos.* Tirant Lo Blanch: Valencia, (2016) pp.382 -383.

Santora, Marc y Rashbaum, William, y Perlroth, Nicole. Online Currency Exchange Accused of Laundering $6 Billion. https://www.nytimes.com/2013/05/29/nyregion/liberty-reserve-operators-accused-of-money-laundering.html

Schott, Paul Allan. *Guía de referencia para el antilavado de activos y la lucha contra el financiamiento del terrorismo*. 2da Ed. Bogotá: Mayol Ediciones S.A., 2007.

Semana. ¿El bitcoin es legal en Colombia? https://www.semana.com/economia/articulo/bitcoin-legalidad-de-la-divisa-en-colombia/475730

Small, Stephen. "Bitcoin: The Napster or Currency". *37 Hous. J. Int'l L*. 581 (2015) pp. 5-28.

Sutherland, Edwin. *El delito de cuello blanco.* 1era Ed. Buenos Aires: B de F, 2009.

UAFE. Manual Genérico UAFE. http://www.seps.gob.ec/documents/20181/727687/MODELO+DEL+MANUAL+DE+PREVENCIÓN+DE+LAVADO+DE+ACTIVOS+Y+FINANCIAMIENT

O+DE+DELITOS++PARA+SEGMENTOS+1+2+3.pdf/752321a1-6d09-4b70-8357-6b53f828cac9

Unión Internacional de Telecomunicaciones. Guía de Ciberseguridad para los Países en Desarrollo. http://www.itu.int/ITU-D/cyb/publications/2007/cgdc-2007-s.pdf

United States Department of State. Bureau of International Narcotics and Law Enforcement Affaris. *International Narcotics Control Strategy Report. Volume II. Money Laundering and Financial Crimes.* (2017), pp. 5-203.

United States District Court/ Southern Disctrict of New York. *United States of America v. Ross William Ulbricht.* Legal Information Institute, Cornell University, Law School.

van Wegberg, Rolf, Oerlemans, Jan-Jaap, y van Deventer, Oskar. "Bitcoin money laundering: mixed results?: An explorative study on money laundering of cybercrime proceeds using bitcoin." Jou*rnal of Financial Crime,* Vol 25 (2018), pp. 419-435.

Vigna, Paul y Casey, Michael. *The Age of Cryptocurrency: How Bitcoin and Digital Money are Challenging the Global Economic Order*. 1era Ed. Nueva York: St Martin´s Press, 2015.

Wadhwa, Amit y Arora, Neerja. "A Review on Cyber Crime: Major Threats and Solutions". *International Journal of Advanced Research in Computer Science.* Vol. 5 No.8, 2017.

Zambrano Pasquel, Alfonso. *Lavado de Activos: Aproximación desde la Imputación objetiva y la Autoría mediata.* 1era Ed. Quito: Corporación de Estudios y Publicaciones (CEP), 2010.