UNIVERSIDAD CATÓLICA

DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRÍA EN DERECHO MENCIÓN DERECHO PROCESAL

TEMA:

La ausencia de normativa penal para reprimir el lavado de activos a través de criptomonedas

AUTOR:

Jaime Germán Silva Colcha

Previo a la obtención del grado académico de:

MAGISTER EN DERECHO MENCIÓN DERECHO PROCESAL

TUTOR:

Dr. Juan Carlos Vivar Álvarez Msc.

ECUADOR

ENERO DE 2023

UNIVERSIDAD CATÓLICA

DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRÍA EN DERECHO MENCIÓN DERECHO PROCESAL

CERTIFICACIÓN

Certificamos que el presente trabajo fue realizado en su totalidad por Jaime Germán Silva Colcha, como requerimiento parcial para la obtención del Grado Académico de Magister en Derecho Mención Derecho Procesal.

DIRECTOR DEL PROYECTO DE INVESTIGACIÓN

_____

Dr. Juan Carlos Vivar Álvarez, Msc.

REVISOR

Dra. Nuria Pérez Puig

_____

DIRECTOR DE LA MAESTRIA

_____

Dr. Miguel Hernández Terán

Guayaquil, 3 del mes de enero de 2023

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL
SISTEMA DE POSGRADO
MAESTRÍA EN DERECHO MENCIÓN DERECHO PROCESAL

Declaración de responsabilidad

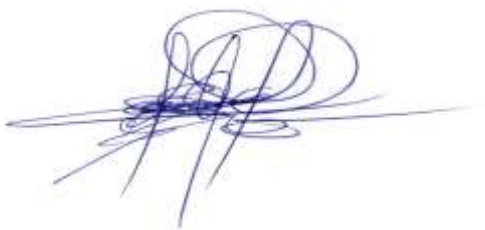
Jaime Germán Silva Colcha

TENGO A BIEN DECLARAR QUE:

El proyecto de investigación denominado "LA AUSENCIA DE NORMATIVA PENAL PARA REPRIMIR EL LAVADO DE ACTIVOS A TRAVÉS DE CRIPTOMONEDAS", requisito previo a la obtención del Grado Académico de Magister en Derecho mención Derecho Procesal, ha sido desarrollado en base a una investigación absoluta, holística e integral, con total respeto de los derechos de propiedad intelectual de terceros conforme a las citas que constan dentro del presente, las fuentes de consulta han sido incorporadas en la bibliografía, concluyendo que el trabajo corresponde a mi autoría.

En virtud de aquello me hago responsable de contenido, veracidad y alcance científico de la tesis de grado académico de Maestría en Derecho, mención Derecho Procesal.

Guayaquil, 3 de enero de 2023
EL AUTOR
Jaime Germán Silva Colcha



UNIVERSIDAD CATÓLICA

DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRÍA EN DERECHO MENCIÓN DERECHO PROCESAL

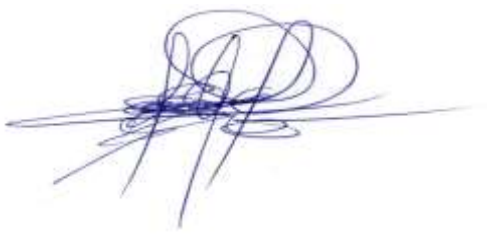
AUTORIZACIÓN

Jaime Germán Silva Colcha

Autorizo a la Universidad Católica de Santiago de Guayaquil, la publicación en la biblioteca de la institución, así como también en el repositorio digital de la misma, del proyecto de Investigación previo a la obtención del Grado académico de Magister en Derecho mención Derecho Procesal, que lleva como título "LA AUSENCIA DE NORMATIVA PENAL PARA REPRIMIR EL LAVADO DE ACTIVOS A TRAVÉS DE CRIPTOMONEDAS", cuyo contenido son de mi exclusiva autoría y me responsabilizo de todo lo redactado en el trabajo académico.

Guayaquil, a 3 de enero de 2023

EL AUTOR



Jaime Germán Silva Colcha

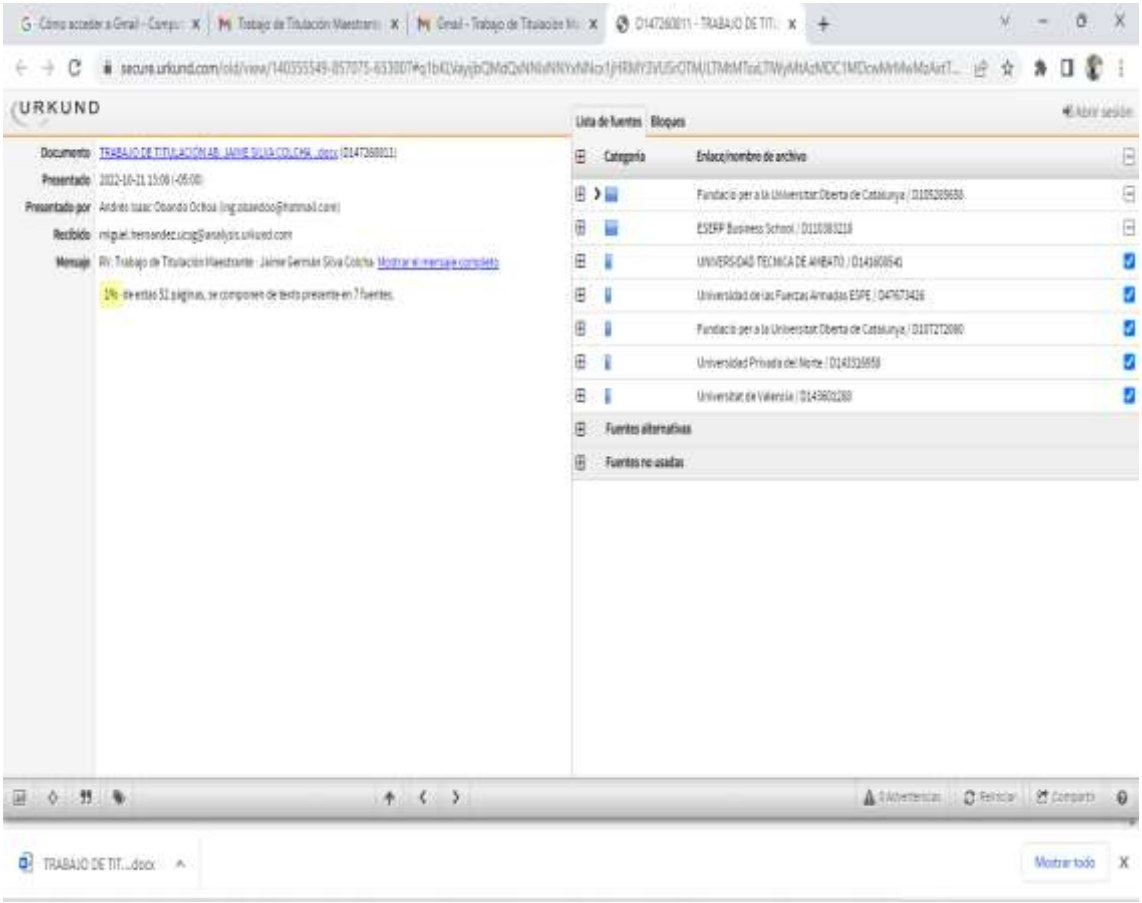
UNIVERSIDAD CATÓLICA

DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRÍA EN DERECHO MENCIÓN DERECHO PROCESAL

Informe de Urkund



Agradecimiento

Expreso un cordial agradecimiento en primera instancia a la institución que me ha formado durante este lapso; a la Universidad Católica Santiago de Guayaquil; así como a la Función Judicial del Ecuador por permitirme cursar esta importante Maestría ; sin desmerecer el infinito agradecimiento al tutor Dr. Juan Carlos Vivar Álvarez Msc. ; a todo el cuerpo docente de la Universidad y a mi fraterno amigo Ab. Kevin Cabezas Páez quienes me han guiado de manera desinteresada por el camino del conocimiento.

Jaime Germán Silva Colcha

Dedicatoria

El presente trabajo investigativo le dedico a mi señora madre Lic. Mélida Targelia Colcha Ramos, incondicional aliciente para la realización de ésta Maestría , sublime mujer que con su apoyo íntegro pretende únicamente que me desarrolle como un excelente ser humano y un distinguido profesional.

Jaime Germán Silva Colcha

ÍNDICE GENERAL

RESUMEN

Dentro del presente trabajo investigativo se aborda un tema de total relevancia jurídica como la ausencia de norma en el Ecuador para reprimir el lavado de activos que es cometido a través de criptomonedas, en un primer momento se estudia al lavado de activos o también conocido como blanqueo de capitales, se examinan las particularidades de las criptomonedas y su utilización a través de herramientas informáticas para darle la apariencia de un dinero legítimo y reinsertarlo al orden socioeconómico tanto nacional como extranjero. Se aplicó una metodología mixta tanto cualitativa como cuantitativa porque desde su complementación una a otra mejora el entendimiento del problema, optimando la creatividad y permite llegar a una mejor conclusión dentro del problema de investigación. Con las conclusiones a las que se han arribado se recomienda una reforma del Código Orgánico Integral Penal, en el sentido de tipificar la conducta de las criptomonedas en el delito de lavado de activos, debido a su facilidad de uso para delinquir, y a la vez capacitar y dotar de equipos tecnológicos a quienes realizan investigación de los delitos de acción pública como Fiscalía General del Estado y Policía Nacional.

Palabras clave: ausencia normativa, criptomoneda, lavado de activos, orden socioeconómico, reforma legal.

ABSTRACT

Within this investigative work, an issue of total legal relevance is addressed, such as the absence of a norm in Ecuador to repress money laundering that is committed through cryptocurrencies, at first, money laundering or also known as money laundering is studied of capitals, the particularities of cryptocurrencies and their use are examined through computer tools to give it the appearance of legitimate money and reinsert it into the national and foreign socio-economic order. A mixed qualitative and quantitative methodology was applied because from their complementation one to another improves the understanding of the problem, optimizing creativity and allows to reach a better conclusion within the research problem. With the conclusions reached, a reform of the Comprehensive Código Orgánico Integral Penal is recommended, in the sense of classifying the conduct of cryptocurrencies in the crime of money laundering, due to its ease of use to commit crimes, and at the same time train and to provide technological equipment to those who carry out investigations of crimes of public action such as the State Attorney General's Office and the National Police.

Keywords: regulatory absence, cryptocurrency, money laundering, socioeconomic order, legal reform.

INTRODUCCIÓN

El tema de las criptomonedas atrae cada vez más la atención de las autoridades internacionales, el motivo es sencillo de entender, la aparición de divisas paralelas a los circuitos tradicionales, fuera del control de los bancos centrales, plantea serias dudas en cuanto a estabilidad financiera, protección al usuario y también riesgos de blanqueo de capitales. En los tiempos este tema ha sido tratado en las reuniones del G20, elaborándose un documento al final del encuentro que hace referencia explícita a las criptomonedas, subrayando que hoy este fenómeno no representa una amenaza para la estabilidad financiera internacional aunque las autoridades permanezcan atentas a los riesgos de blanqueo de capitales, terrorismo y protección del inversor (Moreno, 2021).

Tres puntos clave que se refieren a casos concretos surgidos en el pasado reciente. Los intercambios de criptomonedas tienen lugar en plataformas no reguladas y ha habido numerosos casos de robo sin que los usuarios puedan proteger sus derechos. En materia de blanqueo de capitales, la no trazabilidad de Bitcoins debido a su tecnología, ha permitido el movimiento de activos sospechosos que acabaron en la mira de las autoridades internacionales como Estados Unidos de Norteamérica y Unión Europea. El canal de intercambio permite eludir a los intermediarios financieros autorizados y de esta forma la opacidad en las transacciones es casi total lo cual brinda facilidades a los delincuentes que operan a través de plataformas informáticas dejando su autoría en anonimato, cometiendo los injustos de forma célere.

La necesidad de armonizar las regulaciones entre los distintos países también surgió del G20. Un punto clave. Dado que las criptomonedas se dividen sin fronteras, a menudo logran insinuarse en las diferentes disciplinas legislativas explotando las ineficiencias. Desde este punto de vista, los ministros de finanzas hicieron una referencia explícita al trabajo que está llevando a cabo el Grupo de acción financiera (Fatf), el organismo intergubernamental que durante mucho tiempo se encarga de organizar propuestas para la armonización de las reglas

para las criptomonedas. Las recomendaciones son particularmente importantes porque podrían terminar en el documento final del G-20 y, por lo tanto, ser implementadas progresivamente por los Estados que las adhieran.

El propósito de esta acción conjunta es llegar en un tiempo razonable al desarrollo de reglas vinculantes para los intercambios de criptomonedas (plataformas). En particular, entonces será importante comprender si los principios contra el blanqueo de capitales vigentes son suficientes para combatir el fenómeno a nivel internacional o si es necesario introducir formas de implementación para armonizar la lucha contra los delitos que se cometen con criptomonedas.

En el Ecuador tenemos por un lado a la normativa penal que en su Código Orgánico Integral Penal, recoge al lavado de activos o blanqueo de capitales en su artículo 317, en donde se tipifican diversas modalidades a través de sus elementos descriptivos del tipo y verbos rectores tales como la ocultación, transferencia, posesión utilización, conversión de activos de origen ilícito, si bien en esta disposición nos da una luz para la comprensión del verbo convertir, pero esta no es suficiente para su interpretación literal propia de la norma penal sustantiva, por ese motivo en el COIP y en las demás leyes que regulan y previenen el lavado de activos en el país es necesario tratar a las criptomonedas de una forma particular y específica para su prevención, sanción y regulación debido a su incidencia negativa en el orden socioeconómico.

CAPÍTULO I

Planteamiento del problema

A lo largo de la historia, la sucesión de innovaciones tecnológicas continuas y cíclicas ha cambiado la forma en que las personas viven, interactúan y organizan sus vidas. La economía también siempre ha estado influenciada por los descubrimientos en el campo científico y técnico: la revolución industrial, la electricidad, el petróleo, han provocado cambios en los métodos de producción y transporte, afectando profundamente el contexto socioeconómico. En particular, en los últimos años la historia del hombre se ha caracterizado por la transición de un tipo de sociedad industrial a un tipo de la denominada sociedad de la información, revolucionando profundamente el contexto social en el que vive el hombre.

Úbeda (2009) sostiene que, si en un pasado cercano era la producción industrial la que dominaba el escenario económico, ahora son los datos los que están en el centro de atención. La invención de la computadora, la World Wide Web, los teléfonos inteligentes y, más recientemente, el crecimiento del fenómeno de Internet de las cosas, han transformado cada vez más al individuo y la sociedad. Los ciudadanos de hoy viven en un mundo globalizado, interconectado y dominado tecnológicamente.

Al igual que las revoluciones anteriores de las artes y la tecnología, los descubrimientos tecnológicos más recientes también ofrecen numerosas oportunidades, pero esconden riesgos importantes como señala el autor Buscaglia (2015). La anulación de las fronteras nacionales, la interconexión de las personas y los dispositivos utilizados ponen en peligro los llamados activos legales nueva generación como la privacidad, la identidad digital, el derecho al olvido. El vórtice del cambio también envuelve al individuo, quien se ve obligado a desarrollar habilidades técnicas nuevas y específicas relacionadas con el uso de dispositivos de nueva generación; se trata de competencias cada vez más especializadas, en continua y rápida evolución (Health, 2020).

Una de las innovaciones tecnológicas que se ha estado afianzando en los últimos años es la cadena de bloques, todavía conocida generalmente como la tecnología detrás del funcionamiento de las criptomonedas. En realidad, no solo se utiliza como vehículo para el flujo de monedas virtuales, sino que cuenta con aplicaciones prácticas en contextos heterogéneos para la solución de diversos problemas. Dependiendo de las aplicaciones prácticas, la cadena de bloques puede plantear cuestiones relacionadas con su abuso, entendido como su uso con fines ilícitos. La historia de los descubrimientos científicos está llena de ejemplos de nuevas herramientas concebidas para la satisfacción de una necesidad específica explotada con fines delictivos (Lacarte, 2018). En el transcurso de los siguientes párrafos, se proporcionará una descripción general de la cadena de bloques, su posible uso y su marco legal en relación con los tipos de delitos configurables.

Hacia finales de 2008, Satoshi Nakamoto publicó el libro "Bitcoin: un sistema de efectivo electrónico de igual a igual" (Wright, 2020, p. 15), en el que los principios teóricos y operativos del protocolo Bitcoin se exponen en sólo nueve páginas. El objetivo declarado de su creación es crear un dinero electrónico basado en el modelo de *red peer-to-peer* que pueda utilizarse en ausencia de un organismo central (bancos o instituciones financieras) que garantice el correcto funcionamiento del sistema de pagos.

Según Lacarte (2018) el carácter innovador propuesto en el protocolo Bitcoin es la resolución del denominado "Problema de doble gasto" (que surge cuando un sujeto gasta la misma moneda digital varias veces, hecho posible por la fácil duplicación de datos informáticos), que consiste en el uso de prueba de trabajo y en particular de la cadena de bloques.

Esta última es probablemente la solución tecnológica más innovadora de los últimos años, que se presta a innumerables y aún inexploradas aplicaciones prácticas. Por tanto, no solo es la base del funcionamiento de todas las criptomonedas actualmente en circulación, sino que ha

visto crecer su uso y desarrollo con la creación de los denominados contratos inteligentes o *Smat Contracts*. Dado que siempre ha sido el derecho quien debe perseguir a la tecnología, como Aquiles y la tortuga, es necesario comprender a fondo el funcionamiento de las nuevas tecnologías para poder regular correcta e inequívocamente su uso y los consiguientes efectos en la vida de los ciudadanos. (Jansson, 2018).

Cuando el legislador se ve obligado a emitir normas que toman en cuenta los tecnicismos de las nuevas tecnologías, muy a menudo hay una producción legislativa imprecisa y contradictoria; o, se crean normas que en el momento de su entrada en vigor ya están obsoletas, en virtud de la gran diferencia en el ritmo del progreso científico con respecto a la máquina legislativa.

Por ello, en la primera parte del presente trabajo investigativo se analizará y examinará la tecnología blockchain, desde su funcionamiento hasta las diversas formas prácticas: no solo las criptomonedas (bitcoin y más) y los contratos inteligentes, sino también las nuevas formas de capital generalizado levantando, el ICO o *Initial Coin Offerings* (Lanuza & Olóndriz, 2019). También se examinarán las normativas actualmente vigentes (y continuamente actualizadas) en nuestro ordenamiento jurídico y no, procurando también identificar cuáles pueden ser las mejores vías a seguir a nivel legislativo, para evitar aprovechar la tecnología en declaraciones normativas con el efecto para cortar su desarrollo de raíz.

Todo ello, corroborado por la necesidad de proteger a las personas de los importantes abusos que pueden causar graves infracciones a los bienes jurídicos más importantes. En virtud de esta última consideración, en la segunda parte llegaremos al corazón del objeto de investigación de este trabajo, a saber, los perfiles criminales de las criptomonedas. Estos últimos se prestan a fines ilícitos diversos y polivalentes tanto por sus peculiaridades intrínsecas (fundamentalmente el anonimato), como por el hecho de que se utilizan, en la mayoría de los casos, para cometer delitos mediante sistemas informáticos o internet. (Arzuaga, 2018).

El análisis de delitos que pueden configurarse mediante criptomonedas a delitos contra la propiedad y financieros ha sido limitado. En particular, se abordará el delito de blanqueo de capitales, junto con el tema del ciber lavado, la nueva frontera de la limpieza del "dinero sucio" (Jiménez, 2015, p. 55). De hecho, las criptomonedas pero en general internet han dado lugar a nuevas formas de llevar a cabo los delitos de lavado de activos.

El legislador ha tomado medidas para emitir y actualizar la normativa vigente contra este injusto con el objetivo de involucrar también a los prestadores de servicios relacionados con las criptomonedas, especialmente los intercambios, sujetos virtualmente colocados en la aduana del mundo virtual y real. Además, se analizará la posibilidad de configurar los delitos relacionados con actividades bancarias y financieras ilegales, siendo el uso más extendido de las criptomonedas un medio alternativo al dinero, conductas que emulan las funciones y actividades de las instituciones bancarias y financieras. (Úbeda, 2009). Los activos sin la autorización necesaria podrían integrar los delitos previstos en los dos textos consolidados antes mencionados.

Es muy común comprar, vender o convertir criptomonedas en las llamadas plataformas intercambio, que, gracias a la alta volatilidad de los precios, puede generar enormes beneficios. Además, también es necesario considerar los ingresos de los distintos sujetos profesionales que prestan servicios relacionados con el uso de las criptomonedas, y valorar si contribuyen a determinar la renta imponible, cuya falta de declaración o pago podría constituir los delitos fiscales previstos en el Código Orgánico Integral Penal (Asamblea Nacional, 2014).

Con el objetivo de brindar una investigación completa de los perfiles criminales no solo desde un punto de vista sustantivo sino también puramente procesal, se abordarán las cuestiones de la prueba electrónica y las investigaciones informáticas. En concreto, también se rastrearán los problemas que surgen cuando el objeto de los medios probatorios de investigación son las criptomonedas (en particular en el contexto de la incautación), y las peculiaridades de las

llamadas análisis forense de bitcoins, es decir, técnicas de investigación e indagaciones relacionadas con las criptomonedas.

Por tanto, el objetivo de este trabajo es rastrear los perfiles de relevancia delictiva en los casos vigentes en la actualidad derivados del uso de criptomonedas, pero, en el transcurso de la discusión, se aprovechará la oportunidad para proponer nuevas soluciones legislativas y llevar a la atención del lector problemas que actualmente no son fáciles de resolver. Se verá, en particular, que en algunos casos un esfuerzo hermenéutico no es suficiente, también en virtud de la prohibición de la analogía *in malam partem* que caracteriza al derecho penal.

Antecedentes

El blockchain, a primera vista, no constituye una novedad en sus elementos esenciales en cuanto a la necesidad humana de registrar y contabilizar las transacciones. De hecho, no es más que un libro mayor distribuido y descentralizado donde todas las transacciones se reportan agrupadas en una cadena de “bloques” enlazados entre sí en sucesión cronológica. (Rigters, 2021).

Desde el nacimiento de las primeras empresas en la época de Mesopotamia, se sintió la necesidad de anotar las relaciones de crédito y débito de uno; posteriormente, se innovó el método de contabilidad, con la teorización de la doble entrada, explotada por las primeras instituciones bancarias a nivel mundial.

Con la llegada de las computadoras, internet y los servicios de almacenamiento en la nube, ha sido posible mantener los datos contables y computacionales en su dispositivo pero también "en la nube", evitando cualquier posible destrucción o alteración física de lo que antes era un papel de registro donde se realizaban las transacciones fueron notados. La forma en que los humanos transcriben y almacenan sus datos se ha revolucionado aún más. El blockchain ha renovado la forma de registrar transacciones y almacenar datos, transcribiéndolos en una cadena

de bloques concatenados. Si bien se trata de una tecnología profundamente innovadora, explota y aglutina diversas soluciones tecnológicas que ya existían antes de su concepción. (Bashir, 2019).

Una primera teorización del blockchain tuvo lugar en 1991 con la publicación del artículo "Cómo sellar un documento digital" de Stuart Haber y W. Scott Stornetta, en el que se teorizaron sistemas de certificación temporal de archivos digitales, anticipándose de hecho algunas soluciones tecnológicas adoptadas en blockchains que se utilizan en la actualidad. (Moreno, 2021).

En general, sin embargo, su nacimiento se remonta a la publicación del libro de Satoshi Nakamoto en 2008, donde se describe el innovador protocolo Bitcoin basado en la cadena de bloques. La verdadera innovación, sin embargo, está en haber combinado las tecnologías existentes con la teoría de juegos y un efectivo sistema de incentivos que conduzca a la solución de algunos problemas que han surgido anteriormente en cuanto a pagos entre varios sujetos interconectados en ausencia de un tercero que garantice la veracidad y ausencia de fraude por parte de los usuarios. Sin embargo, el Bitcoin también tiene orígenes teóricos y prácticos que se remontan a muchos años antes de su creación. En particular, en 1994 se concibió un sistema de pago virtual con Digicash, creado por D. Chaum, pero a diferencia del protocolo Bitcoin, aún contaba con un tercero que garantizaba la finalización exitosa de todas las transacciones. (Arzuaga, 2018).

En el mismo período, un movimiento de activistas llamado "Cypherpunk" nacido a fines de la década de los 80, publicó el "Manifiesto Cypherpunk" en 1993, cuyo contenido se centra en temas como la privacidad y el uso de cifrado para protegerla. Según el pensamiento del movimiento antes mencionado, la privacidad en una sociedad abierta requiere sistemas de transacciones anónimas, y el anonimato de la transacción no significa su secreto.

Para Jones (2019) el anonimato es fundamental para la verdadera esencia de la privacidad, ya que otorga a los usuarios el derecho a revelar su identidad cuando y solo si lo desean. Además, el movimiento promete defender y garantizar la privacidad con criptografía, firmas digitales y monedas electrónicas: todos elementos que serán tomados como base teórica diez años después por Satoshi Nakamoto para idear el protocolo Bitcoin.

En general, los principios fundacionales del movimiento criptoanarquista se centran en la oposición y el inevitable debilitamiento del poder y las instituciones estatales, sin tener en cuenta la existencia de leyes, salvo las expresadas y aplicadas por códigos informáticos. En 1998, Wei Dai dio a conocer B-money, un white paper (abiertamente inspirado en los principios del movimiento criptoanárquico) donde se propusieron dos modelos de sistemas de pago descentralizados con cifrado.

Lacarte (2018), indica en su estudio que el primer sistema de pago fue definido por el mismo autor como impráctico en virtud de la ausencia de resolución del problema del doble gasto el segundo, por otro lado, se basa en la "prueba de participación" que alienta a los usuarios a no incurrir en conductas fraudulentas amenazándoles con perder sus depósitos, promoviendo así la adopción de conductas no fraudulentas.

Finalmente, en 2004 Hal Finney teorizó, tomando como modelo el funcionamiento de Hashcash (sistema antispam propuesto por Adam Back en 1997) (Moreno, 2019), lo que para Smith (2018) constituye una de las piedras angulares del protocolo Bitcoin, la "prueba de trabajo". Por tanto, el que se acaba de ilustrar es el trasfondo histórico, teórico y tecnológico que llevó a Satoshi Nakamoto a la concepción del protocolo Bitcoin utilizando tecnología blockchain en 2008, y en 2009 a crear el primer bloque, (también conocido o llamado génesis) del encadenamiento de bloques (Jansson, 2018). Bitcoin.

De hecho, algunos autores como el conocido Arzuaga (2018) consideran al Bitcoin como la expresión práctica de la ideología del movimiento criptoanárquico, basada en la ausencia de

la necesidad de intermediación estatal en el contexto de los sistemas de pago digitales y transacciones privadas, así como de manera más general en el contexto de la emisión y gestión del mercado monetario.

Esta tecnología ha servido para crear nuevas criptomonedas, de hecho en la actualidad hay muchas, pueden desarrollarse diariamente, cotizan en bolsa como el mercado de Forex, y sirven como intermedio financiero para el comercio legal, compra y venta de bienes y servicios con total normalidad, en la actualidad la moneda virtual más conocida y usada es el Bitcoin, pero también hay otras como el Ethereum, Ripple, Cardano, Litecoin, etc., estas criptodivisas pueden intercambiarse entre sí por ejemplo el Bitcoin transformarse en Cardano, y también llegar a ser la transformación de Bitcoin a dólares, euros, libras, etc., y viceversa, la forma de almacenar este tipo de monedas es a través de monederos virtuales o e-wallet, entre los más conocidos tenemos a Copay, Electrum y Exodus, aunque existen muchas más opciones que ofrecen el servicio.

Formulación del problema

Abordar la temática del lavado de activos cometido a través de criptomonedas es uno de real y actual importancia que contiene muchas aristas y se lo fórmula para fines de esta indagación como el siguiente: ¿Existen vacíos normativos procesales en el Ecuador cuando se comete lavado de activos mediante criptomonedas?

Objetivo general

Analizar el delito de lavado de activos que se comete mediante criptomonedas como una nueva forma de delinquir, y la ausencia de norma procesal en el Ecuador.

Objetivos específicos

1.- Estudiar al delito de lavado de activos que es cometido mediante criptomonedas como una nueva forma de delinquir en el Ecuador.

2.- Identificar las normas procesales que regulan el lavado de activos y las criptomonedas en el Ecuador.

3.- Proponer una regulación especial a las criptomonedas para evitar el cometimiento de lavado de activos en el Ecuador.

Hipótesis

Existe ausencia de normativa penal para reprimir el lavado de activos a través de criptomonedas.

Justificación

El lavado de activos, también conocido como blanqueo de capitales, consiste en un conjunto de operaciones efectuadas para asegurar que el capital o activo de carácter ilícito pase a tener una apariencia legítima (Tondini, 2009). Este actuar delictual es un fenómeno que ocupa al derecho penal y trasciende a una índole social que cada vez y cuando está en constante evolución y generalizado a nivel mundial.

Para autores como Raskovsky & Linares (2019) el perfeccionamiento de este ilícito ha trascendido a fronteras internacionales y se han implementado nuevas formas de cometer este delito como es la utilización de criptomonedas que no tienen ningún tipo de dependencia de organismo ni gobierno, es decir Banco Central alguno; de tal modo que son cifradas por criptografía entre las más conocidas tenemos al Bitcoin, el Etherium, el Binance Coin, Cardano, Tether, etc.

Todos estos activos o criptomonedas que son lícitos porque cotizan en la bolsa de valores están a disposición de cualquier persona natural o jurídica, y la forma de comprar, comerciar, adquirir, retirar y convertir el dinero fiat (Ramsey, 2019) o dinero circulante fiduciario puede ser a través de depósitos a monederos virtuales como Binance, Skrill, Neteller, etc.

Continuando con la operación, para en lo posterior transferir el dinero a un bróker o portafolio de inversión de criptomonedas cualquiera, para que de esta manera se pueda comerciar con el dinero depositado, y la forma del retiro podrá ser en criptomonedas, esta es la operación en donde que no importa cuál sea el origen del dinero que se deposita, el bróker o los portafolios de inversión no cuestionan el origen del dinero, y a la vez prestan facilidades para que el dinero sea retirado en su totalidad con ganancias o pérdidas a través de la criptomonedas a elección, las más usadas para el retiro son Bitcoin y Etherium, entre otras.

De esta manera a nivel mundial se comete lavado de activos, el Ecuador no es la excepción ya que existe ausencia normativa para la regulación y prevención de este ilícito a través de criptomonedas, aparte del Art. 317 del Código Orgánico Integral Penal, que regula el delito como tal, en nuestro país el Estatuto Orgánico de Gestión Organizacional del Banco Central (Banco Central del Ecuador), hace mención a las operaciones de Forex, únicamente a reportar y registrar dichas operaciones, pero es totalmente lícito porque forma parte del control que realiza el Banco Central, como la anotación de mensajería Swift, operaciones de inversión, transferencias de carácter internacional, entre otras; por otro lado la regulación de estos activos criptográficos no existe en el país y esta ausencia normativa facilita a la delincuencia organizada para la realización de estos actos ilícitos, transgrediendo bienes jurídicos de relevancia social, en donde se disimula u oculta la procedencia de este dinero.

En el mundo algunos Estados han creado y ejecutado políticas públicas en contra del blanqueo de capitales, como la restricción hasta la prohibición de este tipo de divisas (Torres, 2019), el Ecuador es una de estas excepciones ya que no existe política pública, y normativa

alguna que regule cierta modalidad. Este injusto trasfronterizo se propaga significativamente, tanto en términos del número de casos como en las cantidades que los criminales intentan convertir un activo ilícito a lícito.

Para el autor Peláez (2019) el perjuicio, además del delito del que se origina del dinero sucio, también se origina cuando su producto se reintroduce en el ciclo del mercado financiero. De hecho, se suscitan una serie de efectos nocivos y distorsiones, tanto a nivel económico, político como social, los mismos que han sido objeto de disputa a nivel mundial. Por ello es un tema de tal relevancia que necesita ser estudiado para realizar en lo posterior una propuesta con el fin de ayudar a las autoridades a detectar, prevenir y sancionar esta modalidad delictual en el país.

Resumen del capitulo

La criptomoneda o criptomoneda se define como una moneda generada e intercambiada exclusivamente de forma electrónica, caracterizada por la criptografía, la no centralidad de la emisión y ausencia de valor legal, pero representa un medio de pago voluntario entre usuarios, dentro de sus características relevantes tenemos a la desaparición de una autoridad monetaria central ya que su existencia y vigencia están probadas por el sistema distribuido, este controla tanto las criptomonedas como sus propiedades; se pueden crear nuevas unidades de criptomonedas y, de ser así, define su origen y cómo determinar su propietario; las propiedades de la criptomoneda solo pueden probarse mediante criptografía; se permite el intercambio de unidades criptográficas y la confirmación de la transacción solo puede ser emitida por aquellos que puedan acreditar la propiedad de las criptomonedas involucradas en la transacción.

Ahora al referirnos a la realización de blanqueo de capitales se produce en el caso clásico, o sea la eliminación de cualquier posible conexión con la infracción anterior (conducta sustitutiva); en el movimiento, a través de herramientas de negociación, de bienes de origen

ilícito (realización de transferencia); en la realización de otras operaciones encaminadas a obstaculizar la identificación del origen delictivo de los bienes, considerada como cláusula de cierre enfocada a perseguir conductas no identificables previamente por el legislador y que son fruto de la "creatividad" con la que trabajan los grupos delictivos para blanquear el dinero de origen ilícito.

Está claro que las características de las criptomonedas en total anonimato y sin el control de una autoridad centralizada representan una formidable oportunidad para el blanqueo de capitales y, en general, para la reinversión de capitales de origen ilícito, es por tal motivo relevante en que existan normativas propias para prevenir el delito, ya que encontramos ausencia de norma para reprimir el lavado de activos a través de criptomonedas.

CAPITULO II

MARCO TEÓRICO

2.1.- El lavado de activos como fenómeno global

El interés por el fenómeno del lavado de activos tiene orígenes relativamente recientes. De repente, pasó a ser el centro de atención en los Estados Unidos en la década de 1970, tras el escándalo de Watergate, por las operaciones de pista falsa llevadas a cabo por la administración del presidente Nixon con el fin de financiar sus operaciones secretas (Peláez, 2019). Sin embargo, se señaló que ciertamente el lavado de activos no puede considerarse nacido en ese momento, sino que debe enmarcarse correctamente como inherente a la necesidad de que cualquier malhechor esconda los frutos adquiridos ilegalmente a través de actividades delictuosas. (Terradillos, 2011).

A juicio de Palencia & Pierre, sobre este delito en la actualidad afirmaron lo siguiente:

> "En actividades contra el orden socioeconómico de un Estado, la intervención del Derecho Penal se haya justificada ante aquellas conductas que conlleven un daño social trascendente, creándose tipos penales a la par del desarrollo económico y de la escala de velocidades con que se vaya dando la globalización". (Palencia & Pierre, 2016, p. 241).

El escándalo de Watergate fue sin duda un episodio importante, pero la apuesta por la lucha contra el blanqueo de dinero nació sobre todo gracias a otros factores: la lucha contra el narcotráfico, en primer lugar, con la llamada guerra contra las drogas emprendida por el gobierno de Estados Unidos para paralizar la actividad de los narcotraficantes bloqueando su capacidad de gasto. El término blanqueo de capitales, así como el término "lavado" (Peláez, 2019, p. 19), adoptado en la legislación extranjera constituye el resurgimiento en el contexto legislativo de una metáfora: "el dinero sucio (contaminado por el delito) debe ser lavado en el

circuitos financieros de varios tipos, antes de que pueda ser devuelto limpio al mercado de origen". (Náquira, 2018, p. 143).

Acerca de la corrupción, la misma "no es una desviación contingente de muchos de los sistemas políticos imperantes en Latinoamérica, sino parte de su funcionamiento esencial" (Palencia & Pierre, 2016, p. 245). Los operadores económicos y las estructuras en connivencia con la delincuencia crean una profunda distorsión de los mecanismos del mercado y la competencia, así como una desaceleración del crecimiento económico y el socavamiento de la reputación de intermediarios individuales o de sistemas financieros completos. Además, al estar necesariamente relacionados con la búsqueda de métodos de inversión más propensos a ocultar el rastro de papel, los movimientos de capital pueden ir en direcciones absolutamente irrazonables en comparación con las esperadas de un inversor que opera con capital legítimo.

El objetivo del reciclador o persona que efectúa el lavado de capitales, por tanto, independientemente de la complejidad de la operación en la que se realiza el reciclaje, es alterar la información que constituye el "código genético" (Fernández, 2019, p. 67), de los flujos financieros. Esta información es fundamental para reconstruir el rastro documental y rastrear el delito y, por lo tanto, hasta el autor del injusto. Por tanto, si la diferencia entre la riqueza generada por la actividad delictiva y la generada por el empresario legal está en su origen, es precisamente esta connotación la que debe verse afectada. Considerar este fenómeno, entonces, limitado a los billetes, aunque el control del efectivo es fundamental, es realmente anacrónico e ingenuo (Mallada, 2012).

El lavado de dinero tiene un fuerte arraigo internacional, que se manifiesta en dos vertientes: la internacionalización del crimen organizado (por ejemplo en el ámbito del narcotráfico, de seres humanos o de armas) y la caracterización económica de las actividades delictivas que a menudo adoptan esquemas típicos de emprendimiento (incluida la función financiera, también con recurso a sistemas extranjeros los llamados paraísos fiscales utilizados

tanto para el blanqueo como para la captación y depósito de capitales ilícitos). (Fernández & Bacigalupo, 2009).

A nivel mundial, no solo en Estados Unidos o Europa, sino en todo el planeta, la lucha contra el lavado de activos está fuertemente ligada a la presencia de organizaciones criminales de tipo mafiosas, que utilizan el lavado de capitales para infiltrarse en la economía legal e incluso crear empresas conjuntas con particulares. Un importante punto de inflexión señalado por Peláez (2019) en la lucha contra el lavado de activos tuvo lugar en 1988, con la Convención de Viena de las Naciones Unidas. Los Estados participantes se comprometieron a introducir en los ordenamientos jurídicos nacionales causas penales ad hoc, con el objetivo de combatir el blanqueo de dinero vinculado al narcotráfico. Este acuerdo ha dado lugar a la multiplicación de la normativa contra el delito en mención.

La Convención antes mencionada fue seguida por la Convención de Estrasburgo, pero sobre todo por la Directiva 1991/308/CE, que exigía a los Estados miembros que reprimieran la conducta de blanqueo del producto del tráfico de drogas, según lo dispuesto por la Convención de Viena, y exhortó a los Estados a luchar contra el lavado de activos en una gama más amplia de delitos, según lo dispuesto en el Convenio de Estrasburgo. Cabe destacar que, con motivo del G7 en París en 1989, el establecimiento del GAFI (Grupo de Acción Financiera), organismo intergubernamental cuyo propósito es la elaboración y desarrollo de estrategias para combatir el blanqueo de capitales de origen ilícito, mediante el perfeccionamiento de estándares para batallar las actividades financieras ilícitas, la evaluación y seguimiento de los sistemas internacionales y la identificación de países con problemas estratégicos en sus sistemas de prevención y lucha contra este tipo penal.

Referirse al lavado de activos para Náquira (2018), ya no se refiere a un numerus clausus de delitos, sino a una generalidad. La actividad legislativa de esos años se movió sobre la base de la constatación de que la lucha contra las ganancias del crimen organizado debía seguir dos

pautas: por un lado, era necesario prevenir el dinero acumulado ilícitamente, el llamado "dinero sucio" se transformó en dinero "limpio". A continuación, el legislador europeo prosiguió con su actividad de reforma sobre el tema mediante la introducción de la II Directiva contra el blanqueo de capitales (97/2001 / CE).

Este último solicitó la tipificación del mismo, vinculado no solo al narcotráfico, sino también a todas las actividades del crimen organizado, así como la extensión de las obligaciones contra el blanqueo de capitales a actividades y profesiones no financieras, como contable y forense. A esto le siguió la III Directiva (2005/60 / CE) "para la prevención del blanqueo de dinero y la financiación del terrorismo", que estableció un mecanismo regulador confirmado también por la IV y V Directiva de la UE contra el lavado de activos inspirado en el deber de conocer a los clientes o intermediarios financieros con enfoque basado en riesgos.

La misma directiva estableció un conjunto articulado de obligaciones para las instituciones de crédito y financieras, así como para otros sujetos privados, por su proximidad a la realización de operaciones que puedan constituir actividades de lavado de dinero. El texto normativo revisado, entre otras novedades, anticipó el contenido de la V Directiva Anti-Blanqueo de Capitales (2018/843 / UE), introduciendo la noción de "moneda virtual", así como ampliando las obligaciones bajo la normativa anti-blanqueo de capitales a "proveedores de servicios relacionados con el uso de moneda virtual'. Con este decreto, las obligaciones contra el delito también se extendieron a los "proveedores de servicios de billetera digital", los llamados *wallet provider*.(Robinhood, 2021).

2.2.- ¿Qué es una criptomoneda?: conceptos fundamentales, cuestiones críticas y la tecnología Blockchain

Una criptomoneda o dinero criptográfico es un medio de pago digital que generalmente se basa en tecnología *blockchain* y procedimientos criptográficos como funciones *hash* y firmas

digitales. A diferencia de las monedas clásicas, las criptomonedas no involucran monedas ni billetes, ya que todas las unidades de pago son exclusivamente digitales. Estas unidades monetarias usualmente con cifrado asimétrico se generan colectivamente en todo el sistema y, en la mayoría de los casos, cuando se lanza una criptomoneda, se establece un número definido de unidades. El concepto de "minería" para el proceso de generación de unidades se ha generalizado y esto explica por qué a menudo oímos hablar de "minería de criptomonedas" o *mining*. (Luna, 2020).

Las características principales de una criptodivisa: Tras la hiperinflación del Bolívar Fuerte, el 20 de agosto de 2018, Venezuela no solo introdujo la nueva moneda Bolívar Soberano, sino que también la vinculó al criptosistema Petro. Si bien el gobierno venezolano habla de la "primera criptomoneda estatal", Petro carece de las características decisivas de una moneda, como la descentralización del sistema o la igualdad de derechos entre todos los participantes, precisamente por la regulación estatal. Igualmente controvertidos son los sistemas gestionados de forma privada como *Ripple* (Lanuza & Olóndriz, 2019).

Mirando más precisamente a los tres componentes elementales de una criptomoneda, está claro que los sistemas administrados por empresas privadas y el Estado satisfacen el aspecto cripto pero no tienen mucho que ver con el principio clásico de Bitcoin cifrado (Smith, 2018). La criptografía no solo da el nombre, también es la disciplina decisiva para la seguridad de las criptomonedas. Detrás del concepto de criptografía se encuentra la ciencia que se ocupa del cifrado y la protección general de datos e información. Ambos son indispensables para un sistema de pago sin efectivo y completamente digital, que básicamente debería funcionar sin un organismo central y regulador. En las criptomonedas se utilizan principalmente dos procedimientos criptográficos: funciones hash, y firmas digitales.

Las funciones hash según Arzuaga (2018) son la pieza básica del rompecabezas para verificar la integridad de los datos y codificar las direcciones de cuenta y las operaciones de los

participantes. Además, forman la base de blockchain y block mining. Las firmas digitales le permiten comprobar el estado de la información cifrada sin exponerla. Esta posibilidad también se utiliza para proteger el contenido de los correos electrónicos. En criptomonedas, esta tecnología es ideal para firmar transacciones y comunicar la aprobación de una operación a la red.

Acerca de la tecnología Blockchain: Según afirma Rigters (2021) la cadena de bloques es el libro mayor descentralizado de una criptomoneda, donde todas las transacciones se enumeran en forma de bloques. El registro de los bloques individuales se realiza sin lagunas y en orden cronológico de modo que, con el tiempo, se obtiene un registro verificable, mayoritariamente abierto y duradero. La administración está a cargo de los participantes de la red básica *peer-to-peer*, quienes siguen un protocolo definido para validar nuevas operaciones.

En consecuencia, todos los nodos descargan automáticamente una copia integral de la cadena de bloques, lo que hace que una instancia central sea superflua para ver las operaciones que han tenido lugar. Un registro de datos basado en la tecnología blockchain no se puede cambiar sin la aprobación de los otros miembros. (Bashir, 2019).

Dado que la cadena de bloques y el protocolo Bitcoin se caracterizan por un sistema descentralizado, no existe un organismo central que certifique y garantice la veracidad y consistencia de las transacciones. Por tanto, el blockchain utiliza un sistema de consenso distribuido basado en la confianza mutua de los participantes de la red, de tal manera que se resuelven problemas comunes a los sistemas de pago descentralizados como el tema del doble gasto y el llamado "Problema de los Generales Bizantinos" (Rigters, 2021).

Además, la aplicación de la teoría de juegos al funcionamiento del Bitcoin, sostiene Bashir (2019) que permite incentivar a los usuarios a que pongan a disposición sus recursos para el correcto y eficaz funcionamiento del sistema, contribuyendo a su preservación, continuidad y desarrollo. Partiendo del análisis del principio de consentimiento distribuido, es

de fundamental importancia ya que es solo gracias al principio antes mencionado que Blockchain es capaz de garantizar su transparencia operativa.

De hecho, dado que no existe una autoridad central en la que los usuarios depositen su confianza (como bancos, organismos estatales, etc.), es necesario que los usuarios dependan unos de otros. Así, el mecanismo de consentimiento basado en prueba de trabajo previene conductas fraudulentas que pueden llevarse a cabo en un doble gasto de los mismos bitcoins o en un acuerdo entre múltiples usuarios para defraudar al sistema.

Este último, el problema de los generales bizantinos, teorizado en 1982 por Shostak, es presentado por el mismo autor a través de un ejemplo práctico: hay generales bizantinos que, después de haber rodeado una ciudad, deben decidir cuándo atacar o retirarse por necesariamente actuando al unísono; si hay generales "traidores", comprometerán la acción coordinada que conducirá a la derrota de los bizantinos. Allí la solución al problema permite llegar a un acuerdo incluso en presencia de información contradictoria (atacar o retirar) de los generales fraudulentos.

Esta metáfora describe esencialmente los problemas que pueden surgir en contextos de redes *peer to peer*, donde existen múltiples nodos que intercambian información entre ellos y es posible que algunos nodos intenten registrar transacciones que nunca ocurrieron o fueron falsas como en el caso de los generales bizantinos, que comprometen el asedio difundiendo órdenes distorsionadas de tal manera que socaven la simultaneidad del ataque.

En el protocolo Bitcoin para asegurar que un minero no agregue bloques fraudulentos, se usa prueba de trabajo: cada nodo en la red sabrá que el bloque válido será solo el bloque agregado por el minero que ha tomado una cantidad considerable de energía computacional para resolver el acertijo criptográfico. (Reyes, 2021). De esta forma, todos los demás nodos que verificarán la resolución de la prueba de trabajo, validarán el bloque y todas las transacciones presentes en él en virtud del principio de consentimiento distribuido.

El blockchain también resuelve el problema del doble gasto, es decir, gastar las mismas monedas dos veces, reenviando el mismo pago varias veces a diferentes destinatarios. En el sistema bancario, son precisamente las entidades de crédito las que garantizan la no ocurrencia del doble gasto. Pero en la virtualización de la moneda y en ausencia de un garante central, la criptografía permite "identificar cada moneda" para que todos los nodos sepan que ciertos bitcoins han sido enviados a una determinada dirección y que posteriormente no pueden ser enviados a otro sujeto.

Cuando se reciben bitcoins, no es posible gastarlos inmediatamente, porque es necesario esperar al menos seis confirmaciones de tantos nodos. Las confirmaciones se fundamentan en los bloques posteriores que se añaden sucesivamente a aquel en el que se ingresó la transacción a validar; por lo tanto, después de aproximadamente seis bloques encadenados, la transacción puede considerarse válida e insertada permanentemente en la cadena de bloques, ya que su modificación se vuelve muy poco probable. (Cossey, 2019).

Morales (2020), manifiesta que puede suceder que en un período de tiempo limitado se agreguen dos bloques a la cadena, ambos conteniendo las mismas transacciones o solo algunos de ellos dando lugar a un llamado tenedor (un tenedor en la cadena del bloque). La solución a este inconveniente está garantizada por el principio según el cual la confianza de los usuarios se coloca en la cadena más larga, es decir, la cadena de bloques en la que se gastó la mayor cantidad de energía (prueba de trabajo).

De esta manera, los mineros agregarán los nuevos bloques a la rama más larga de la cadena, y las transacciones contenidas en el llamado bloque de los denominados huérfanos, se pondrán en cola para ser agregados a los siguientes bloques pertenecientes a la cadena más larga. Moreno (2021) identifica otro aspecto innovador de la cadena de bloques del protocolo Bitcoin es el sistema de incentivos que garantiza la continuidad del funcionamiento de todo el sistema. De hecho, el blockchain además de utilizar tecnologías ya existentes y solucionar el

problema de los generales bizantinos y el doble gasto, explota la teoría de los juegos, un modelo matemático para el estudio de las "situaciones competitivas" (p. 157).

En base a ello, Satoshi Nakamoto, citado por Wright (2020), ha ideado un sistema mediante el cual cada nodo que participa en la red, mediante el uso de sus propios recursos computacionales (electricidad), recibe una determinada cantidad de bitcoins como recompensa además del monto de comisiones. Este sistema se introdujo porque en el protocolo bitcoin no existe un organismo central que imprima y distribuya la moneda. Por tanto, los nodos que dedican sus recursos a la minería son los que acuñan los bitcoins y ponen en circulación la nueva moneda minada.

El sistema así articulado garantiza el éxito del sistema Bitcoin, ya que se incentiva a los usuarios a actuar de acuerdo con las reglas y no en contra de ellas, ya que una actuación deshonesta no conlleva ventajas como para preferirla a una conducta honesta.

Finalmente, la esperanza de Nakamoto es que cuando se coloquen en la red el número total de bitcoins (21 millones), el incentivo consista exclusivamente en comisiones. De esta manera, un minero deshonesto debe elegir entre la posibilidad de realizar transacciones inexistentes o participar en la formación de los nuevos bloques con honestidad, ganando con los costos de transacción: de esta manera, actuar con honestidad será considerablemente más rentable que actuar de manera deshonesta. (Wright, 2020).

2.2.1.- Principales características de las criptomonedas y principales actores de la comunidad virtual

La moneda virtual ha sido definida por el Banco Central Europeo (2017) en los siguientes términos:

> "(…) Es una forma de valor digital que no es emitida por un organismo público ni está imperiosamente conexa a una divisa oficial, pero que es admitida por la sociedad como medio de pago y se puede transferir, acumular o comerciar de forma electrónica" (p. 45).

Para destacar los posibles riesgos derivados del uso de criptomonedas, los estudiosos del tema como Jansson (2018) identifican sus principales características:

Son creados por una emisora privada de acuerdo con sus propias reglas a las que los miembros de la comunidad eligen adherirse; no están en manos del usuario, que posee una billetera electrónica o e-wallet a la que se puede acceder mediante una contraseña; estas carteras son, de hecho, software desarrollado por partes calificadas, como proveedores de carteras. Posteriormente es posible, en algunos casos, convertir la moneda digital en dinero legal y viceversa a través de plataformas de intercambio; los titulares de billeteras electrónicas permanecen en el anonimato; las transacciones que implican la transferencia de dinero virtual son técnicamente irreversibles, por lo que nunca es posible solicitar la cancelación; la criptomoneda no es de curso legal, se puede utilizar para la compra de bienes y servicios solo si el *accipiens* o persona que lo recibe está disponible para aceptarla.

Es inevitable que estas características conlleven riesgos de forma inherente. El hecho de que cada usuario, en base a sus propias reglas, pueda crear una nueva moneda virtual deja espacio para una competencia desenfrenada, pero sobre todo un juego sin reglas puede engañar fácilmente a aquellos inversores que no dominen la criptomoneda. Además, al ser un sistema completamente virtual, el riesgo de entregar toda nuestra billetera en manos de posibles piratas informáticos es crucial.

Es por eso que nunca debe invertir más de lo que puede permitirse perder como bien señala Muñoz (2017). Sin embargo, un aspecto aún más crítico radica en el anonimato de las transacciones, característica que sin duda llama la atención de las organizaciones criminales. También es posible dividir las monedas virtuales en tres tipos macro, en función de su

interacción con la moneda de curso legal en concordancia con lo establecido por Antonopoulos (2017):

1. Moneda virtual no adquirible, "no convertible" o "cerrada", porque no prevé la posibilidad de convertirse en moneda de curso legal y, por lo tanto, utilizable solo dentro de los límites de la comunidad virtual;

2. Moneda de "convertibilidad limitada", que se puede comprar con moneda tradicional, pero que a su vez no se puede convertir a moneda de curso legal;

3. Moneda "totalmente convertible", que se puede comprar y revender a cambio de moneda tradicional.

Específicamente para el autor Antonopoulos (2017) la diferencia entre la criptomoneda y la moneda tradicional radica en la incapacidad de la moneda virtual para cumplir las tres funciones de una moneda oficial: unidad de cuenta, medio de pago y depósito de valor. La función de unidad de cuenta de la criptomoneda es intuitivamente menor cuando los precios de la misma están sujetos a grandes fluctuaciones, incluso dentro del mismo día.

La falta de moneda de curso legal tampoco permite considerar la moneda virtual como un medio de pago útil. Finalmente, en lo que respecta a la función de depósito de valor, hay que tener en cuenta que la cantidad de unidades de criptomonedas que se pueden producir es limitada, por lo que cuantas más transacciones liquidadas en criptomonedas, mayor es su valor. Como resultado, es poco probable que las monedas virtuales se utilicen como reserva de valor.

Después de subrayar los aspectos que distinguen a la criptomoneda de la moneda oficial, se debe tener cuidado de no confundirla con dinero electrónico como bien sostiene Preukschat (2017). Los requisitos de estos últimos son la puesta en marcha, funcionamiento y supervisión prudencial de la actividad de las entidades de dinero electrónico. Se define como un valor monetario representado por una cuenta por cobrar del emisor que es:

1.- Almacenado en un dispositivo electrónico;

2.- Emitidos al recibir fondos cuyo valor no sea inferior al valor monetario emitido;

3.- Aceptado como medio de pago por empresas distintas del emisor.

En conclusión, parece más correcto clasificar las monedas virtuales como un bien, es decir, cualquier cosa, sea material o inmaterial, capaz de satisfacer una utilidad o necesidad humana, o incluso como la posibilidad de sufrir expropiación y limitación y que, como tal, representa el objeto de los derechos (White, 2019).

Acerca de los actores claves de la comunidad virtual:

Un segundo y más profundo análisis realizado por el Banco Central Europeo distingue los diferentes servicios prestados por los principales actores de la comunidad virtual en función de su naturaleza. Los inventores, con identidad conocida o en algunos casos desconocida, son quienes crean la nueva moneda virtual y desarrollan la parte técnica de la red, orientada a mantener y mejorar las características técnicas de la moneda, incluido cualquier algoritmo (Walker, 2018).

Los mineros trabajan, a menudo en grupos, para validar las transacciones para que el nuevo bloque formado se agregue a la cadena de bloques, mediante la resolución de complejos cálculos matemáticos. Su aporte es fundamental para mantener activa la cadena, y para ello reciben, por cada bloque generado, una recompensa en criptomoneda, por un monto que se reduce a la mitad cada cuatro años.

Las monedas recibidas se pueden vender en el mercado (Jones, 2019). En ausencia de la figura de los mineros, no serían raras las operaciones con intenciones fraudulentas, dobles gastos o unidades falsas. En virtud de su valiosa contribución, se les permite cobrar una tarifa de transacción a quienes decidan iniciarla.

Según el autor Jones (2019) los usuarios se incorporan a la comunidad virtual con el objetivo de obtener criptomonedas útiles para la compra de bienes y servicios reales o virtuales de comerciantes dispuestos a aceptarlas, útiles para realizar pagos persona a persona o con fines

de inversión. El usuario obtiene unidades de moneda virtual a través de: la compra; participación en actividades recompensadas con unidades de moneda virtual (por ejemplo, participación en actividades promocionales); autogeneración de dinero, o "minería" (en este caso el usuario es un minero); venta de bienes y servicios virtuales y reales contra pago en moneda virtual; Reciba criptomonedas como donación.

Los proveedores de billeteras virtuales, según Smith (2018) inician y proporcionan a los usuarios una billetera digital en la que almacenar claves criptográficas de moneda virtual y códigos de autenticación de transacciones, ordenados cronológicamente. Los intercambiadores o *exchangers* son aquellos que cotizan los tipos de cambio a los que comprar y vender moneda virtual frente a las principales monedas fiduciarias y frente a otras monedas virtuales. Además, están autorizados a proporcionar estadísticas, billeteras y servicios de conversión a los comerciantes que aceptan criptomonedas como medio de pago.

Las plataformas de negociación representan según Lacarte (2018) el *alter ego* de los mercados oficiales, conectando compradores y vendedores de criptomonedas, sin embargo, actuar como una herramienta intermediaria. Las plataformas, a diferencia de los intercambiadores, no compran y/o venden por sí mismas y en algunos casos solo ofrecen la posibilidad de identificar potenciales contrapartes y luego realizar el intercambio en persona.

2.3.- Fases y técnicas de lavado de activos mediante criptomonedas

Los delincuentes que poseen, reciben pagos o convierten de dinero fiat en criptomonedas deben convertirlas en dinero de curso legal para reintroducir el producto económico del delito en el ciclo del mercado normal, un proceso que requiere ofuscar el origen de los fondos (Lombardero, 2009). Desafortunadamente, varios servicios y herramientas sofisticados ayudan a los delincuentes a hacer esto. Después de todo, si los malos no tuvieran forma de sacar provecho de las criptomonedas recibidas a través de canales ilegales, los incentivos para

cometer delitos serían mucho menores (Heath, 2020). A continuación, se muestra un ejemplo del proceso de blanqueo de capitales, tal como sostiene Fernández, (2019):

1.- Introducción: movimiento de dinero desde su fuente. El dinero circula dentro del sistema monetario existente a través de ciertos intermediarios, como instituciones financieras, casinos, tiendas o casas de cambio. Ejemplos de estas actividades incluyen el contrabando de efectivo fuera de un país, la complicidad de un banco, el cambio de moneda, la compra de activos, etc.

2.- Estratificación: En la segunda fase, el objetivo es dificultar la revelación de la actividad de reciclaje. Para ello, los delincuentes deben estratificar el gasto y ocultar el rastro del dinero sucio. Esto generalmente se hace convirtiendo el dinero en instrumentos monetarios o comprando activos con fondos ilícitos para revenderlos.

3.- Integración: Esta es la etapa final del blanqueo de capitales, en la que el dinero blanqueado reingresa a la economía a través del sistema bancario y, en consecuencia, se considera "limpio". Los métodos utilizados en esta fase incluyen, entre otros, la venta de inmuebles, empresas fachada, bancos extranjeros y facturas falsas.

Dada su naturaleza digital y características intrínsecas, Bitcoin parece ser un medio adecuado para las fases de introducción y estratificación. Comenzando con la introducción, Bitcoin podría ser una herramienta útil para intercambiar moneda fiduciaria con bitcoin o BTC, y luego cambiar de criptomoneda a otra moneda fiduciaria, moviendo así dinero de un país a otro. Sin embargo, dado que muchos delincuentes utilizan Bitcoin para recibir dinero, el principal problema es la integración, es decir, reintroducir fondos ilícitos en la economía para ocultar sus actividades ilegales (Arzuaga, 2018).

En la fase de integración, de acuerdo con el *Informe sobre criptomonedas de Chainalysis 2020*, muchos delincuentes lavan criptomonedas con la ayuda de corredores de venta libre. Los corredores *Over-the-Counter* u OTC son comerciantes o empresas que facilitan las

transacciones entre compradores y vendedores que no quieren o no pueden comerciar en un intercambio de criptomonedas (Smith, 2019). Los corredores OTC son populares entre los comerciantes y mineros que desean vender grandes cantidades de activos criptográficos a un precio negociado, ya que el uso de un intercambio regular para vender grandes volúmenes podría afectar los precios del mercado.

La mayoría de los comerciantes OTC se asocian con los intercambios, pero muchos de ellos ofrecen medidas *Know Your Customer* o KYC mucho más bajas que los intercambios en los que operan. Muchos aprovechan esta oportunidad y se especializan en servicios de lavado de dinero para delincuentes. De cualquier manera, los intercambios siguen siendo el medio preferido para limpiar Bitcoins sucios. En el transcurso de 2019, entidades criminales enviaron más de $ 2.8 mil millones en Bitcoin a plataformas de intercambio, y el 52% de estos se destinó a dos de los intercambios más grandes, Binance y Huobi (Wright, 2020).

Bitcoin parece ser más práctico para la segunda etapa del lavado de dinero: capas. Es una moneda digital que se puede utilizar para comprar en la red sin las limitaciones de los límites físicos. Prestando suficiente atención (y utilizando técnicas para preservar la privacidad como las que vamos a explorar), es posible gastar Bitcoin para comprar activos o cobrarlo a través de comerciantes OTC.

Por ejemplo, alguien podría comprar un bien de alto valor como un reloj Rolex o cualquier otro, en un mercado secundario y revenderlo por dinero fiduciario. Sin embargo, será bastante difícil para los delincuentes comprar activos monetarios, ya que la mayoría solo son accesibles a través de intermediarios que aplican las medidas de KYC o *conozca a su cliente*; sin embargo, es importante señalar que, a diferencia del efectivo, las criptomonedas son intrínsecamente transparentes, ya que todas las transacciones se registran en un libro mayor público. Como señala el informe Chainalysis, todos estos fondos ilícitos dejan huellas. Al

acumular la información necesaria, es posible identificar quién se esconde detrás de la dirección de Bitcoin utilizada para lavar dinero (Kreher & Langlois, 2020).

Debido a sus características inherentes, todas las transacciones en una cadena de bloques se comparten entre los participantes, cuyo consentimiento se requiere para validar su historial, el CEO de CoinRoutes, Dave Weisberger (2019), explicó:

> "El objetivo del lavado de dinero es crear una cadena de transacciones que no se pueda rastrear, y dado que la cadena de bloques de Bitcoin está diseñada para tener un registro público indeleble de todas las transacciones, el lavado se vuelve mucho más difícil" (p. 161).

Los mixers o los mezcladores:

Si el pseudoanonimato no ofrece suficiente privacidad, se pueden utilizar los llamados *mezcladores*, software o servicios que permiten a los usuarios realizar transacciones mezclando monedas con otros usuarios para preservar la privacidad. Esto permite a los usuarios ocultar salidas y direcciones y, en consecuencia, sus verdaderas identidades.

Los mezcladores de criptomonedas terminaron en el centro de atención de las noticias en 2019, con informes de cierres de servicios por parte de las autoridades europeas. Sin embargo, según el informe de Chainalysis, los mezcladores parecen usarse mucho más para la privacidad que para actividades ilegales. Solo el 8.1% de todas las monedas mixtas fueron robadas, y solo el 2.7% de las monedas mixtas se usaron anteriormente en los mercados de la darknet (Raskovsky & Linares, 2019).

Los mezcladores no son exactamente fáciles de usar y aun así no pueden proporcionar el mismo nivel de seguridad asociado con los "métodos tradicionales" para el lavado de dinero. El uso de un mezclador podría ser sospechoso, pero estas herramientas pueden ocultar transacciones de manera efectiva solo si se mezcla una masa crítica de Bitcoin. Además, las

autoridades tienen disponibles contramedidas más avanzadas, como el análisis de blockchain, que puede vincular incluso Bitcoins mixtos a las direcciones correctas.

A diferencia del efectivo, cada transacción de criptomonedas se documenta en un libro mayor visible públicamente. Con las herramientas adecuadas, es posible investigar qué operaciones de criptomonedas están asociadas con actividades ilegales, recopilar información sobre sus técnicas de ofuscación y compartir hallazgos con las fuerzas del orden para evitar que los delincuentes abusen del sistema.

Estas empresas han ayudado a los legisladores al proporcionar información valiosa para ayudar a resolver casos penales. Uno de ellos es la participación reciente de Chainalysis en el cierre del sitio web Welcome to Video, que está acusado de permitir que los visitantes publiquen, compartan y descarguen videos de menores en una red de pedófilos (Rigters, 2021). El efectivo sigue siendo la forma más sencilla y segura de blanquear dinero. La Oficina de las Naciones Unidas para el Control de Drogas y Prevención del Delito y Chainalysis estima que por cada dólar en Bitcoin gastado en la web oscura, se blanquean al menos $ 800 en efectivo (Moreno, 2021).

Los datos presentados sugieren que Bitcoin puede ser una herramienta adicional disponible para los delincuentes para el lavado de dinero. Por ejemplo, pueden usar direcciones desechables y técnicas de mezcla como precauciones para garantizar que estén protegidas por un nivel adecuado de privacidad. Sin embargo, las identidades pseudo-anónimas, las transacciones públicas y las complejidades del sistema requeridas para usar Bitcoin no brindan actualmente una alternativa más eficiente o efectiva al lavado de dinero.

Como se destaca en el informe Chainalysis, los delincuentes no quieren que se publique y comparta abiertamente un registro permanente de sus actividades ilícitas. Además, Bitcoin no puede manejar el enorme volumen de dinero necesario para las actividades de lavado de dinero. De hecho, la red Bitcoin tiene un volumen diario bastante bajo en comparación con otras clases

de activos: alrededor de 25 mil millones de dólares. Mover tal cantidad de dinero haría sonar la alarma de inmediato para las empresas de análisis de blockchain y requeriría intermediarios adicionales e intercambios centralizados (Preukschat, 2017).

En 2017 y 2018, Lazarus Group, un grupo de hackers asociado con Corea del Norte, cobró la mayoría de sus fondos a través de intercambios con medidas mínimas de KYC. En 2019, sin embargo, las técnicas del grupo se volvieron más sofisticadas. La mitad de los fondos se limpiaron a través de la billetera CoinJoin (mezclador), mientras que la otra mitad aún permanece en sus billeteras (Moreno, 2019).

Las fuerzas del orden y los reguladores deben convertirse en expertos en blockchain para mejorar sus habilidades para prevenir y reaccionar ante diversas formas de criptodelitos. Los intercambios también deben llevar a cabo procedimientos de diligencia debida en profundidad sobre los usuarios, las transacciones OTC y cualquier otro tercero que opere en su plataforma, que sigue siendo el destino preferido para que los delincuentes envíen criptomonedas ilícitas.

Las regulaciones no se formularon para el estado actual de las cosas. Se necesita una mayor colaboración y supervisión internacional para permitir la libertad de movimiento de fondos y dinero. Desafortunadamente, las legislaciones no han podido seguir el ritmo de los rápidos avances tecnológicos. Como alternativa a nuestros sistemas bancarios tradicionales, se necesitan nuevas reglas y regulaciones para garantizar una gobernanza adecuada a nivel mundial.(Antonopoulos, 2017).

2.3.1.- ¿Quién es un cybercriminal?: aspectos de carácter criminológico

La comisión de delitos mediante el uso de criptomonedas se ve facilitada no solo por las características objetivas de los medios tecnológicos, que en sí mismos revelan un carácter criminógeno particularmente pronunciado, sino también por el hecho de que la conducta no es

material. Un delito cometido en línea no es criminológicamente comparable a los delitos cometidos completamente fuera de línea.

Son varios los elementos que desde el punto de vista criminológico caracterizan los ciberdelitos, como el anonimato percibido, la falta de contacto físico o al menos visual con las víctimas, la cancelación de fronteras geográficas, y también las distintas normas legales en las distintas jurisdicciones como bien señala Almenar (2018).

El anonimato percibido lleva al sujeto actuante a la convicción de que su identidad será muy difícil de descubrir, y esto socava la función preventiva y disuasoria de las leyes penales. El individuo en la red se esconde detrás de diferentes alter egos con una máscara, o mejor dicho, varias máscaras a las que corresponden comportamientos diferenciados. La sanción penal incorporada en el precepto normativo no puede cumplir eficazmente su función si el individuo está convencido de que no está descubierto en Tiempos rápidos, para no ser sometido a juicio y sufrir la pena.

Desde otro punto de vista, la despersonalización de las víctimas, en cambio, significa que el delincuente, al no entrar en contacto directo con la víctima, no se da cuenta realmente del daño causado a la misma. De esta forma, la desvalorización social de la propia conducta se siente en mucha menor medida que un delito cometido fuera de línea, y todo ello hace que la comisión de actos ilícitos se facilite precisamente por la ausencia de escrúpulos morales. Igualmente relevante es el carácter transnacional de los delitos cometidos en línea (Ferro, 2020).

La conciencia de actuar en perjuicio de las víctimas ubicadas a miles de kilómetros aumenta la despersonalización de las víctimas y también induce al delincuente a sentirse inmune a cualquier forma de represión, especialmente si actúa en países donde las fiscalías son escasas o nulas. Se puede argumentar que una característica peculiar del ciberdelito es la desproporción entre los costos de los ataques y el daño causado y las ganancias acumuladas, lo

que determina una mayor palatabilidad que las mismas conductas que el individuo podría cometer de manera análoga (Agelán, 2018).

Esto significa que la comisión de un delito en línea es muy conveniente para Ortiz (2013), respaldada por el anonimato y la difícil trazabilidad. La transnacionalidad también causa dificultades en la cooperación judicial en los casos en que los países que no desean cooperar lanzan ataques y, en cualquier caso, los retrasos burocráticos de las órdenes de detención o la circulación de pruebas benefician a los criminales**.**

También debemos tener en cuenta como bien sostienen Martínez & Fernández (2020) las dificultades que existirían en los juicios contra los ciberdelincuentes al demostrar más allá de toda duda razonable su culpabilidad. Suponiendo que uno está ubicado e identificado, por ejemplo, después de determinar la dirección IP desde la que comenzó el ataque, no hay certeza suficiente para afirmar la culpabilidad de la persona conectada a esa dirección IP en particular.

En resumen, en virtud de las peculiaridades de los delitos cometidos a través de Internet, son igualmente singulares las cuestiones criminológicas que determinan una comisión más fácil de los delitos especialmente por parte de personas insospechadas, que no cometerían ningún delito en la "vida offline"; en el mundo virtual, sin embargo, los individuos antes mencionados tienen más probabilidades de incurrir en conductas delictivas en virtud de las razones examinadas anteriormente.

2.3.2.-¿Qué son los Criminal Smart Contracts?

Para obtener una imagen más completa, es necesario considerar la existencia de formas particulares de cometer delitos utilizando blockchain. En particular, el estallido del fenómeno de los llamados "Contratos inteligentes criminales". Como todas las nuevas soluciones tecnológicas, los contratos inteligentes también se prestan a ser utilizados con fines ilícitos; Sin embargo, el foco de atención se centrará en particular en la plataforma Ethereum y no en el

protocolo Bitcoin. De hecho, esto último ha llevado a la propagación de ransomware, ciberlavado y mercados oscuros, pero Ethereum ofrece nuevas características, a saber, la implementación de contratos inteligentes en la cadena de bloques (Kreher & Langlois, 2020).

La posibilidad de cometer delitos a través de contratos inteligentes no es una cuestión obvia, pero es importante comprobar primero si pueden utilizarse como medio para cometer actos ilegales. Hay dos cuestiones a considerar: si el uso del contrato inteligente garantiza tanto la comisión del delito como un pago a su autor; si los contratos inteligentes son prácticos, es decir, si no es necesario ejecutar una cantidad considerable de energía computacional que puede hacer que su uso no sea conveniente.

Para Sztandarowski (2019), los actos ilícitos que se pueden implementar a través de un contrato inteligente son la divulgación y venta de documentos secretos, el robo de claves privadas (por ejemplo, de una billetera de moneda virtual) y el llamado "Delitos con tarjeta de llamada" (Sztandarowski, 2019, p. 124), que se caracterizan por el hecho de que su ejecución se efectúa en la realidad offline.

Los contratos inteligentes le permiten intercambiar monedas virtuales automáticamente, eliminando así el riesgo de que una parte del contrato se retire y cancele el pago. Además, implican una interacción mínima entre las partes evitando así el riesgo de ser rastreados o monitoreados por terceros. Finalmente, le permiten utilizar fuentes externas al sistema de contrato inteligente, como informes meteorológicos o listas de precios de acciones oficiales como entrada al contrato. Sin embargo, estas características pueden facilitar la comisión de delitos, como en el caso de la escasa interacción de las partes que dificulta aún más a las autoridades competentes el seguimiento de conductas sospechosas.

El uso de datos externos como input para contratos inteligentes, por otro lado, conlleva la posibilidad de extender su radio de acción no solo a la realidad virtual online sino también a la realidad material de la comisión de otros delitos pagaderos a través de esta forma.

Los contratos inteligentes delictivos que se utilizan para revelar información secreta dan vida a mercados reales de información confidencial relativa, por ejemplo, a secretos diseños gubernamentales o industriales (Agelán, 2018). Los contratos inteligentes están programados de tal manera que una vez que se paga el precio, la información confidencial se descifra automáticamente durante un cierto período de tiempo.

Otros tipos de contratos inteligentes similares, por otro lado, están programados para descifrar públicamente solo una parte de la información después de un pago modesto, y todo el mensaje se descifra solo si el contenido es interesante para los usuarios; de lo contrario, se reembolsa la contribución inicial. Este tipo de contratos inteligentes, por tanto, permite la divulgación efectiva de información confidencial, dando a los titulares de la misma la posibilidad de monetizar la divulgación en el más completo anonimato y sencillez.

Para Ferro (2020) el llamado "Contrato inteligente criminal de compromiso de clave" (p. 102), está programado de tal manera que transfiera automáticamente una cantidad predeterminada de criptomonedas al autor del robo después de la entrega de la clave privada a un sujeto específico. De hecho, es un contrato que solicita y encarga el robo de claves privadas. Un aspecto crítico de este contrato inteligente es que la víctima o el objetivo del robo es visible públicamente, por lo que es posible tomar contramedidas efectivas para neutralizar sus efectos.

Finalmente, los llamados delitos con tarjetas telefónicas que utilizan contratos inteligentes se encuentran probablemente entre los más alarmantes, ya que su uso puede dar lugar a la comisión de delitos particularmente graves, como asesinatos por comisión. Su funcionamiento se basa en la publicación de contratos inteligentes por el asesinato de un individuo en particular por ejemplo.

El aspirante a autor intelectual o mediato del asesinato ingresa los detalles del homicidio como entrada (fecha, hora y lugar) y la ejecución automática del contrato (y el consecuente

pago de la remuneración pactada) se llevará a cabo solo después de verificar en base a un feed de datos que el sujeto fue asesinado en la forma ingresada por el asesino como entrada.

Es interesante notar que después de la publicación del contrato, no se produce interacción entre el (futuro) asesino y quien lo encargó; esto hace que sea extremadamente difícil rastrear a los dos sujetos sobre la base de su tráfico de datos (en este caso inexistente) (Almenar, 2018). Otras posibles aplicaciones de este tipo de contratos inteligentes incluyen la comisión de asaltos, secuestros, sabotajes y ataques cibernéticos o terroristas; Prácticamente todo lo que se puede verificar y contener en una fuente de datos puede designarse como el objetivo del contrato inteligente.

Una contramedida que puede contrarrestar eficazmente el funcionamiento automático de este software es alterar los datos contenidos en la alimentación de datos de tal manera que provoque la ejecución automática del contrato sin que el evento ocurra realmente. Además, a diferencia de las transacciones simples en la cadena de bloques que no revelan nada en sí mismo ilegal, los delitos relacionados con las tarjetas telefónicas son, de hecho, autoinculpatorios y, para ser efectivos, deben publicitarse adecuadamente y llamarse la atención.

Por lo tanto, se plantea la hipótesis de crear comunidades destinadas a monitorear la naturaleza de los contratos inteligentes publicados y que fueran eliminados de la red. O bien, se ha propuesto encomendar a los mineros la tarea de omitir transacciones cuando se ha informado que estas se derivan de contratos ilícitos. De hecho, en el caso de que el minero tuviera pleno conocimiento de los contenidos y finalidades de los contratos inteligentes ingresados por él en el blockchain, se podrían configurar hipótesis de participación en el delito ajeno, en forma de facilitación o cooperación.

La posibilidad de establecer que una determinada autoridad o un número suficiente de usuarios tiene la facultad discrecional de remover un contrato inteligente específico de la cadena de bloques. Esta solución es la más problemática, ya que puede que los usuarios que participan

en la red blockchain no la acepten pacíficamente como la idea básica de la cadena de bloques y el principio de consenso es que no existe un organismo superior, sino que la confianza se deposita en los propios usuarios.

Hay que considerar, para una discusión más completa, no solo los casos en los que se programan contratos inteligentes con la finalidad explícita de cometer o facilitar delitos, sino también los casos en los que, después de haber elaborado un contrato inteligente sin intención de cometer ningún delito, un delito se comete realmente como resultado de un error de programación o de resultados inesperados. De hecho, los contratos inteligentes son autoejecutables, por lo que una vez activados ya no existe la discreción humana sobre la ejecución del contrato. En estos casos, las cuestiones sobre la predicción del evento y la incidencia de mala conducta intencional en cualquier forma serán particularmente relevantes.

En conclusión, incluso los contratos inteligentes permiten la comisión de actividades ilícitas que pueden configurar delitos extremadamente graves, y el uso de criptomonedas para el intercambio de reservas de valor permite actuar en total anonimato y facilitar su ejecución frente a los métodos tradicionales de pago en moneda de uso legal y circulante como la moneda fiat.

2.3.3.- El lavado de activos mediante criptomonedas y las problemáticas del derecho penal

Las revoluciones tecnológicas determinan la necesidad del derecho de adaptarse constantemente a las nuevas y diferentes manifestaciones fenomenológicas de los delitos, esto ocurre a través de extensas interpretaciones de reglas existentes, la creación de nuevas reglas o la modificación de las existentes.

Las ideologías que subyacen a las revoluciones tecnológicas a menudo se inspiran en el deseo de crear realidades sin derechos y sin control estatal, todo con total libertad y confidencialidad; Los principios inspiradores del protocolo Bitcoin derivan, de hecho, de

movimientos cryptoanarquistas que sitúan la privacidad y la ausencia de interferencia del poder estatal en el centro de atención para evitar el control (Robinhood, 2021).

Para seguir brindando el mínimo nivel de protección a las personas y los activos legales protegidos, es necesario que la ley evolucione y se mantenga al día con la rápida evolución de las herramientas tecnológicas y el comportamiento humano relacionado. Un enfoque conservador que pretende elevar la realidad tecnológica flexible a las categorías dogmáticas y existentes del derecho penal corre el riesgo de ser limitante e impreciso. De hecho, en general los delitos cometidos mediante el uso de sistemas informáticos tienen peculiaridades en sus elementos objetivos que los diferencian claramente de los delitos tal y como estamos acostumbrados a teorizarlos e interpretarlos.

En primer lugar, en lo que respecta a la estructura del delito y, en particular, a la noción de “actos”, “acción” y “hecho”, es necesario resaltar sus características en relación a los delitos cometidos en el ciberespacio. La acción en el ciberespacio se superpone y se fusiona con el hecho, que siempre ha sido considerado por la doctrina como un "resultado externo, claramente distinto del accionar del delincuente y definible independientemente de él" (Martínez & Fernández, 2020, p. 76), como el individuo con su acción que establece en movimiento un proceso articulado en varias acciones cuyo resultado es apenas perceptible naturalísimamente.

Resulta para Ortíz (2013) difícil calificar la acción humana como una actividad externa, ya que tiene efectos perceptibles en el sentido lógico-informático (en forma de código binario). La acción del individuo en la mayoría de los casos no es la descrita por el hecho del delito, sino que será la ejecución automática por el sistema informático lo que será relevante para la naturaleza típica de la norma incriminatoria. Esto también determina que el hecho del delito pierda su connotación material, entendido como una modificación de la realidad externa, fundiéndose con el hecho.

Además, surgen problemas adicionales en relación con la aplicación espacial del derecho penal y el *tempus commissi delicti*. En cuanto a la primera pregunta, su solución es relevante para la determinación de jurisdicción y competencia. Ahora no hay duda de que el ciberespacio no obedece a la lógica territorial de las fronteras nacionales, a diferencia de los sistemas estatales que requieren un "espacio sobre el cual ejercer la soberanía exclusiva" (Almenar, 2018, p. 139).

Además, la red permite la desterritorialización del individuo, que puede actuar y estar presente en varias localizaciones informáticas, así como la destemporalización de acciones, es decir, programar y automatizar operaciones complejas sin el necesario y simultáneo contacto físico entre hombre y el sistema; piénsese en la implementación de contratos inteligentes criminales donde es posible planificar el software en sentido ascendente, cuya ejecución causará el evento relevante para la regla incriminatoria solo posteriormente y cuando ocurran ciertas condiciones previamente establecidas y ejecutadas automáticamente.

Las disposiciones pertinentes del Código Orgánico Integral Penal (Asamblea Nacional, 2014) en este caso sobre la competencia y obligatoriedad del derecho penal y los delitos cometidos en el territorio del Estado; Por tanto, es fundamental determinar cuándo se considera que un delito cometido mediante el uso de Internet se ha cometido en el territorio ecuatoriano y cuándo, a la luz del código, el autor se considera presente dentro de las fronteras nacionales. Es bastante difícil poder responder a estas preguntas con certeza, especialmente teniendo en cuenta la estructura descentralizada de blockchains.

Existen varias soluciones posibles, ya que el registro donde se guardan las transacciones no se guarda en un solo lugar, sino que cada copia se guarda en cada uno de los nodos de la red, esparcidos por todo el planeta. Dado que el registro de blockchain es ubicuo y está representado en múltiples copias, probablemente el único elemento que distingue a un bloque de los demás es el minero que permitió su concatenación.

Una solución podría ser considerar una transacción que tuvo lugar en el lugar donde el minero resolvió el acertijo criptográfico y enganchó el bloque a la cadena de bloques. Sin embargo, esta solución daría lugar a una incertidumbre permanente en cuanto a dónde se agregó la transacción al libro mayor. Además, también hay que recordar que para que una transacción se considere insertada de forma permanente en un bloque válido, es necesario que posteriormente se le agreguen más bloques, aproximadamente seis; de hecho, en el caso de una bifurcación, se agrega una transacción en un bloque que luego, en virtud del principio de la cadena más larga, se convierte en un bloque huérfano con la consiguiente confluencia de las transacciones en la cola que se agregará a los nuevos bloques (Preukschat, 2017) que se agregarán a la rama de la cadena más larga. Por lo tanto, puede suceder que incluso si una transacción se inserta en un bloque válido extraído por un minero ubicado en un país en particular, se considerará como insertada permanentemente en la cadena de bloques cuando otro minero agregue el sexto bloque siguiente.

Además, en todo esto hay un período de tiempo (aproximadamente cada 10 minutos se agrega un nuevo bloque), lo que crea una desconexión temporal entre el momento en que el agente realmente ha transmitido la transacción y el momento en que se considera que ha ocurrido. Evidentemente, es impensable que un delito cometido que luego se cancele se considere con cuidado, incluso cuando es posible afirmar que una transacción ha sido efectivamente concluida.

Un obstáculo para verificar la ubicación geográfica del individuo que transmite la transacción al minero es, como se explicó en los párrafos anteriores, el uso de VPN y navegadores con encriptación estratificada. Desde un punto de vista informático, incluso si el agente actúa físicamente desde una computadora ubicada en el país, estará conectado a servidores ubicados en otros países, creando así dificultades considerables también desde el punto de vista de la prueba y la aplicación efectiva de la jurisdicción ecuatoriana.

En cuanto al locus y el *tempus comissi delicti* del delito de blanqueo de capitales, considerando que se trata de un delito instantáneo, la solución preferible sería considerar el lugar y hora en que el sujeto transmite la transacción, ya que, aunque difícil de determinar por en virtud de las razones anteriores, al menos no queda a merced de la ubicuidad del sistema minero con todas sus incertidumbres inherentes sobre dónde y cuándo ingresará a la transacción en un bloque. Además, esta solución debería ser la más eficaz en términos de persecución del delito, ya que la competencia quedaría confiada al Estado en el que opera y actúa el sujeto que actúa físicamente (Martínez & Fernández, 2020).

2.3.4.- Perfiles procesales de los *cybercrimes* : forense digital y pruebas informáticas (relacionadas a la temática).

A criterio del profesor de Escamilla (2019) La difusión de los delitos cometidos con el uso de computadoras e Internet plantea cuestiones que no solo son relevantes para el derecho penal sustantivo, sino también de tipo puramente procesal. Si antes del advenimiento de las recientes revoluciones tecnológicas la conducta material de los individuos tenía lugar en el mundo offline, ahora las acciones y hechos relevantes para el derecho penal se caracterizan por su pertenencia al mundo virtual, desprovisto de una materialidad naturalista. La ley siempre ha tenido en cuenta los bienes corporales y los objetos tangibles que caracterizaban exclusivamente el entorno en el que trabajaba el individuo, pero actualmente no es así, ya que el progreso tecnológico ha llevado a una continua desmaterialización de la vida de los asociados.

Cambia la forma de interactuar, comunicar y percibir lo real. Lo que siempre ha estado dotado de su propia entidad material perceptible por los sentidos, ahora se digitaliza en forma de datos, es decir, bits simples. Las necesidades del individuo que en otros tiempos requerían tiempo y enormes recursos para ser satisfechas, ahora se pueden satisfacer con un mínimo esfuerzo a través de unos simples clics.

Todo esto significa para Barrios (2018) que incluso la forma en que se cometen los delitos ha sido revolucionada por el advenimiento de las herramientas electrónicas e Internet (solo piénsese en las estafas en línea, la difamación y el lavado de dinero, solo por nombrar algunos). Tal como se destacó en el capítulo anterior cómo las técnicas de blanqueo de capitales configuran el delito a través de conductas y acciones materiales que se diferencian claramente del reciclaje tradicional (mediante el uso de efectivo).

Habida cuenta de estas consideraciones, el proceso penal también debe adaptarse a las nuevas formas de cometer delitos. De hecho, las pruebas perderán su connotación material y consistirán en datos informáticos; cada vez habrá más la desaparición de la prueba documental en sentido estricto, a favor de la prueba desmaterializada.

En particular, en el caso de la cadena de bloques, los únicos elementos sujetos a investigación pueden ser las transacciones ingresadas en el registro, así como las direcciones de los actores de la transacción, tal como sostiene el mismo autor Barrios (2018) en su libro "Delitos 2.0". Por lo tanto, en los juicios por delitos cometidos a través de la computadora e Internet se hará un uso cada vez más frecuente de pruebas electrónicas.

Dado que no existe un registro en papel de la lista de transacciones de blockchain que puedan ser consultadas o incautadas con fines probatorios, las pruebas del tipo anterior se utilizarán necesariamente en los procesos penales. Por último, la transnacionalidad reiteradamente subrayada del mencionado tipo de delito involucra cuestiones importantes en términos de competencia y jurisdicción, así como cuestiones fundamentales en términos de cooperación internacional entre autoridades judiciales e investigadoras (Bajo, 2009).

Acerca de las pruebas digitales: Tras el aumento del uso de sistemas informáticos y telemáticos, es cada vez más frecuente presenciar en los procesos penales la experimentación de técnicas de investigación caracterizadas por un alto contenido tecnológico y también por el uso de pericias informáticas. Esto ha llevado a los protagonistas del proceso a competir con

pruebas contenidas en computadoras, en internet o en una cadena de bloques, presenciando así el declive de las pruebas tradicionales como, por ejemplo, el testimonio como bien afirma Almenar (2018).

Cabe señalar que las pruebas digitales y las investigaciones informáticas no conciernen única y exclusivamente a los llamados delitos informáticos (en sentido estricto), pero también son relevantes para delitos comunes, muchos de los cuales pueden cometerse mediante sistemas informáticos o telemáticos (Galán, 2020). Dado que los sistemas informáticos son los protagonistas de la vida social, laboral y privada de los individuos, es enteramente fisiológico que los datos transmitidos, recibidos y almacenados tengan cada vez más relevancia a nivel probatorio con respecto a los hechos del procedimiento.

En particular, la evidencia digital tiene características peculiares que la diferencian claramente de la evidencia que estamos acostumbrados a considerar. En primer lugar, lo que caracteriza principalmente a la evidencia digital es la inmaterialidad. Aquellos no son más que datos informáticos, en forma de código binario (cadenas de bits), almacenados en medios físicos (como ordenadores) o flotando en Internet. En virtud de este aspecto, las pruebas digitales no son tangibles, y para su existencia no es imprescindible un soporte informático específico ya que son autónomas e independientes de la resolución que las contiene, pudiendo ser duplicadas y reproducidas en innumerables ocasiones.

La evidencia digital también es frágil, ya que puede ser alterada, modificada y definitivamente eliminada tanto por la persona que dio vida al dato objeto de la evidencia digital, como por investigadores expertos e inexpertos. De hecho, es fundamental que el procedimiento de adquisición de la prueba se lleve a cabo con el uso de técnicas altamente especializadas de tal manera que no se contamine de ninguna manera la prueba detectada sino que también se prevea su conservación de manera segura y efectiva, protegida de cualquier intento de manipulación (Ferro, 2020).

La búsqueda de pruebas electrónicas, por tanto, puede tener un fuerte impacto en los derechos garantizados por la Constitución precisamente en virtud de que los dispositivos informáticos se han convertido en "contenedores" de una cantidad inagotable y variada de datos personales; solo piense en los correos electrónicos, chats, sitios web visitados hasta incluir la posición GPS y los movimientos físicos de un lugar a otro. Por tanto, es necesario encontrar un equilibrio entre la protección de los derechos y libertades fundamentales y los requisitos procesales mediante el establecimiento de garantías óptimas para evitar un daño profundo al derecho a la intimidad (Barrio, 2018).

Los problemas no se limitan a las características de la prueba digital, sino que también se extienden a su clasificación por la doctrina y la trazabilidad relativa a las normas del procedimiento penal. En primer lugar, la pertenencia de la prueba digital, en términos del resultado obtenido de la prueba, a la categoría de pruebas representativas directas o pruebas críticas indirectas era cuestionable. Como han señalado varios autores, pueden pertenecer a ambas categorías, pero si se quisiera encontrar un solo factor en común entre toda la evidencia digital, este se puede identificar en la inmaterialidad intrínseca antes mencionada.

Parte de la doctrina se ha expresado a favor de la tesis que califica la evidencia digital como evidencia científica, por involucrar el uso de la informática. Sin embargo, a diferencia de la prueba científica estrictamente entendida, la prueba digital requiere altas habilidades técnicas ya en el momento de la identificación y aprehensión de los datos que constituirán la prueba (Sztandarowski, 2019). Como ya se ha aclarado, es peligroso equiparar la evidencia digital con el rango de prueba que confiere certeza absoluta sobre el hecho a probar. Si bien es cierto que un sitio web en particular ha sido visitado por una computadora en particular en un momento dado, la identidad de la persona que realmente llevó a cabo estas acciones no puede ser absolutamente segura.

2.3.5.- Principales técnicas informáticas de lavado de activos mediante criptomonedas

Desde la experiencia de Rigters (2021), de investigación más remota, es evidente que las organizaciones criminales siempre están buscando nuevas herramientas. La naturaleza del sistema virtual descrito anteriormente sugiere que hay varias formas que permiten a las organizaciones criminales convertir sin esfuerzo bitcoins sucios en moneda física y limpia o moneda proveniente de ilícitos en criptomonedas, cualquiera que esta sea bitcoin u otras.

Las transacciones generalmente tienen lugar en plataformas peer-to-peer (intercambios no registrados): las dos partes eligen reunirse en un lugar público, necesariamente cubierto por una red wi-fi, para transferir bitcoins al precio actual del mercado a cambio de moneda legal. El vendedor recibe los detalles de la billetera del comprador y, luego de obtener el registro en la blockchain, recibe el pago en moneda legal que corresponde al monto pagado en bitcoin sujeto al tipo de cambio vigente, más una comisión que varía entre el 10 y el 15%, mucho más alta que la comisión del 1 o 2% requerida por las plataformas con licencia. Esta diferencia resultaría ser el precio a pagar para no atraer el interés de la autoridad contra el blanqueo de capitales (Bashir, 2019).

Además, no debe subestimarse la posibilidad de transferencias internacionales. Los ingresos ilícitos se pueden convertir aún más fácilmente en bitcoins en aquellos países conocidos como paraísos fiscales que cuentan con controles limitados y una legislación inadecuada contra el lavado de dinero como el caso ecuatoriano. Esta estratagema debe tenerse muy en cuenta cuando se trabaja en la legislación actual, ya que no obstaculiza la financiación de fondos a organizaciones terroristas.

Los problemas derivados de una legislación diferente entre uno y otro Estado también se encuentran en un segundo caso. En 2014 se instaló el primer cajero automático Bitcoin conocido como ATM (Automated Teller Machine), distribuidores que permiten convertir efectivo en bitcoins, el cual se acredita directamente en la billetera electrónica o e-wallet y

viceversa. Después de dos años, ya se habían instalado 640 cajeros automáticos en todo el mundo. Hay dos problemas principales encontrados: en primer lugar, en virtud de una legislación contra el lavado de dinero diferente y más incompleta, algunos Estados no aplican procedimientos de recopilación de datos y diligencia debida sobre los clientes; en segundo lugar, incluso cuando la legislación prevé el cumplimiento de estas obligaciones, los cajeros automáticos rara vez tienen la capacidad de distinguir un documento real de uno obtenido en la web oscura o mediante otros procedimientos ilegales (Reyes, 2021).

Igualmente disimuladoras son las prácticas de volteo, que le permiten descomponer una cantidad significativa relacionada con una sola transacción en una multitud de operaciones, cada una de ellas de tamaño modesto. Esto se debe a que dado que las transacciones siempre son visibles en la cadena de bloques, aunque es difícil rastrear la identidad del usuario, el sujeto criminal desea evitar que una cantidad significativa atraiga la atención de las autoridades supervisoras.

De esta manera, incluso si una micro transacción fuera interceptada y fuera incautada, no afectaría el monto total. Al igual que con las plataformas peer-to-peer, las tarifas proporcionadas por los servicios de rotación varían entre el 5 y el 15%, según el volumen de la cantidad y el grado de fragmentación como bien señala Bashir (2019). El trabajo de las autoridades policiales y de control se vuelve más difícil cuando entra en juego el mercado de los juegos de azar en línea. Las plataformas de este tipo son la herramienta ideal para quienes necesitan hacer circular las ganancias de actividades ilícitas, con fines de corrupción y lavado de dinero.

En primer lugar, porque la amplia ramificación de estas plataformas dificulta el seguimiento del dinero, sobre todo porque los servidores que se ocupan del cobro y gestión de apuestas suelen estar ubicados en países extranjeros con respecto a la sede legal y operativa de la empresa. Además, es igualmente difícil identificar la posición exacta del jugador, que puede

fácilmente farolear declarando una ubicación diferente a aquella en la que se encuentra realmente.

Las posibilidades que ofrece el juego en línea a las organizaciones criminales son múltiples. Baste decir que un jugador podría usar una suma de dinero para perderla voluntariamente a favor de cómplices. Estos últimos, declarando el origen de la suma como ganancias de juego, de hecho tendrán dinero limpio en sus bolsillos. Estas múltiples oportunidades de transferencia de dinero han hecho de la criptomoneda una herramienta valiosa para diversificar las fuentes de financiamiento de organizaciones terroristas que hasta hace poco se limitaban a los confines del mercado ilícito de drogas, armas y secuestros. De hecho, como sostiene Reyes (2021),

> "(…) es evidente que las fronteras dentro de las cuales nos movemos son una especie de puerto libre de la web, en el que es posible reservar espacios amplios para la convergencia entre empresa y aplicaciones digitales, finanzas sin fronteras y negocios invisibles" (p. 95).

2.3.5.1.- Investigaciones sobre Blockchain: notas generales sobre el análisis forense del Bitcoin acerca del injusto lavado de activos

Para los expertos en la materia como Barrio (2018), La difusión del uso de criptomonedas entre los usuarios está poniendo cada vez más en conocimiento de las autoridades judiciales la necesidad de realizar investigaciones eficientes que les permitan utilizar pruebas significativas en los procesos penales para respaldar las tesis propuestas por los fiscales. Ya se ha comentado cómo las monedas virtuales se prestan perfectamente a ser utilizadas como moneda en la comisión de ciberdelitos, es decir, como una forma de lucro al que los cyberdelincuentes pretenden acceder.

No sólo se utilizan para el blanqueo de capitales, sino que, por ejemplo, se exigen como un precio a pagar en el caso de extorsión en línea (phishing, sextortion, ransomware y similares); Las criptomonedas son también las monedas utilizadas en la web oscura para la compra de bienes cuya compra y venta está prohibida por la ley de cada Estado por el origen ilícito de los capitales. Su creciente relevancia en los delitos cibernéticos hace que incluso las técnicas de investigación y la actividad de los órganos de investigación estén necesariamente influidas por sus características estructurales y operativas (de Escamilla, 2019).

Como se ha reiterado repetidamente al discutir el funcionamiento de la cadena de bloques, el registro de transacciones es público y está en manos de todos los nodos de la red; todos pueden acceder a él, consultar las transacciones ingresadas y extraer una copia. Por un lado, esta función es extremadamente útil para fines de investigación, ya que es posible analizar todos los movimientos de las monedas virtuales hasta el primero que se haya producido. De hecho, como se ha explicado ampliamente, el objetivo de la creación de Bitcoin no era obtener el anonimato total (con el objetivo de ocultar transacciones poco claras), sino lograr una privacidad segura en el contexto de los movimientos de dinero, dando lugar a un sistema "pseudo-anónimo" (Almenar, 2018, p. 82).

Por tanto, la sustancial ubicuidad del blockchain es un elemento a favor de los investigadores ya que no será necesario, para acceder a los datos de servidores ubicados en otras jurisdicciones, recurrir a operaciones complejas que involucren también a las autoridades judiciales de otros países que también puede ser reacio a colaborar por falta de interés o incapaz de colaborar debido a habilidades técnicas insuficientes.

El profesor Fernández (2019) recuerda que algunas criptomonedas como Monero y ZChash, con el motivo declarado de fortalecer aún más la privacidad de los usuarios no proporcionan una cadena de bloques completamente transparente, al no indicar el monto de las transacciones y/o direcciones de billetera virtual. En particular, Zchash permite elegir si revelar

el monto y las direcciones de cada transacción, o solo el monto o una de las dos direcciones; todo ello para facilitar a los usuarios el cumplimiento de obligaciones de cumplimiento en particular, obligaciones de lucha contra el blanqueo de capitales o auditorías. De esta forma el uso de estas criptomonedas haría casi imposible poder realizar cualquier operación investigativa ya que, a efectos indagatorios, ni siquiera se daría el detalle de las direcciones y el monto transferido.

El protocolo Bitcoin, en cambio, permite al menos analizar el historial de transacciones, ofreciendo a los investigadores elementos a analizar para reconstruir el origen de los bitcoins o incluso rastrear a los titulares de las direcciones. La criptografía, utilizada en blockchains para garantizar su seguridad y confidencialidad, es explotada por los ciberdelincuentes con el fin de prevenir las actividades de las autoridades investigadoras o en cualquier caso ralentizar considerablemente sus investigaciones según Ferro (2020).

Los sistemas de cifrado avanzados no son imposibles de descifrar, pero implican el uso de enormes recursos y tiempo, lo que haría que las investigaciones fueran ineficaces y daría a los delincuentes la oportunidad de perder el rastro. Por lo tanto, se enfatizó que una cooperación de los productores de bienes y servicios en el sector de telecomunicaciones utilizando criptografía es extremadamente necesaria para que las unidades de investigación puedan realizar las investigaciones necesarias estando en posesión de la clave de descifrado. Por otro lado, en el caso del protocolo Bitcoin y otras criptomonedas (con la excepción de Ripple, cuya gobernanza está centralizada), no existe un organismo central con el que interactuar o tratar en caso de que sea necesario realizar una investigación que involucre al descifrado de cierta información.

Se podría pensar en establecer relaciones con proveedores de billeteras e intercambios de criptomonedas de tal manera que se les pueda pedir que brinden información sobre sus clientes. Sin embargo, esta solución es inverosímil, ya que los proveedores de servicios de

criptomonedas serían reacios a colaborar de este tipo, exponiéndose al riesgo de perder una parte sustancial de sus clientes: quienes deciden operar con monedas virtuales están especialmente preocupados por su privacidad y por tanto, difícilmente optaría por confiar en un proveedor de billetera virtual que colabora con las fuerzas de inteligencia.

No obstante, las obligaciones derivadas de la V Directiva contra el blanqueo de capitales en realidad exigen que los proveedores de billeteras adopten medidas de debida diligencia y reporte de transacciones sospechosas; por lo tanto, al menos en el contexto del funcionamiento de la normativa de la Unión Europea, la cooperación antes mencionada entre particulares y autoridades investigadoras ha sido adecuadamente regulada (Moreno, 2019).

Aunque el llamado análisis forense de bitcoins aún está en sus inicios, es muy básico para enfrentar este tipo de cyberdelitos, destacan los resultados obtenidos al realizar investigaciones sobre la cadena de bloques. Se define como "el uso de herramientas estadísticas para agregar transacciones e identificar usuarios" (Ortiz, 2013, p. 204). La literatura sobre el tema propone diversas metodologías de encuesta, una de las cuales consiste en la desanomización.

Según Almenar (2018), esta técnica consiste en asociar la identidad de un sujeto, una dirección de correo electrónico, un número de teléfono o cualquier otra identidad digital (nombre de usuario, cuenta de Google, etc.) a una dirección bitcoin. Se pueden distinguir dos categorías de métodos de desanomización, activos y pasivos. Los métodos activos consisten en el uso de técnicas de ingeniería social o nodos de red bitcoin maliciosos. Los métodos pasivos, en cambio, se limitan a analizar las transacciones públicas de la blockchain.

En particular, los métodos de la ingeniería social consisten en buscar el contacto directo con el sujeto de tal manera que se descubra la dirección bitcoin asociada a él. Es factible, por ejemplo, mediante la compra de un activo al sujeto ofrecido a la venta en los mercados oscuros; este es el método más efectivo porque el vendedor no proporcionará información falsa ya que está interesado en recibir el pago. Otro ejemplo, más puramente técnico, es la creación de nodos

de la red bitcoin con el objetivo de interceptar las conexiones entrantes y así detectar la dirección IP de los usuarios que transmiten transacciones (Ferro, 2020).

Los métodos pasivos, en particular, consisten en técnicas de investigación y análisis del historial de transacciones de blockchain que pueden ser bastante sofisticadas. Una de las técnicas consiste en fusionar el llamado *clustering,* aquello se traduce a múltiples direcciones bitcoin pertenecientes a un mismo sujeto mediante el análisis de la entrada y salida de la transacción, notando que la primera incluye múltiples direcciones, y la segunda consiste en una sola dirección.

Las técnicas más complejas, en cambio, estudian los movimientos de bitcoins intentando identificar y combinar las direcciones que reciben más dinero sin gastarlo; (Sztandarowski, 2019) De esta forma, se intenta identificar las direcciones de los mercados oscuros de los sitios de apuestas ilegales. Además de estas complejas técnicas, la conveniencia de utilizar las denominadas listas negras, es decir, la marca de bitcoins de sujetos conocidos por sus actividades ilegales, como intentos de phishing, extorsión en línea, etc.

De hecho, existen plataformas en línea la más conocida es "bitcoinwhoswho" destinadas a recopilar informes de direcciones bitcoins fraudulentas; Al hacerlo, los usuarios pueden verificar si una dirección de bitcoin en particular ha sido reportada por haber cometido fraude o intentos de phishing, contribuyendo a la seguridad de la red de bitcoin. También es posible, por propia iniciativa, facilitar los datos a la plataforma mencionada de tal forma que se pueda garantizar que otros usuarios no se involucren en operaciones ilegales, y esto puede ser útil en el caso de vendedores que aceptan y utilizan bitcoins como consideración (White, 2019).

Una consideración final merece el hecho de que el uso de los servicios de mezcla ya discutidos hace que el análisis de las transacciones de blockchain sea extremadamente más complejo, pero no imposible. Además, el uso del navegador TOR y las VPN pueden frustrar

las búsquedas dirigidas a identificar la dirección IP que, con las medidas antes mencionadas, se enmascara o se somete a estratificación criptográfica (Fernández, 2019, p. 39).

Por lo tanto, las investigaciones informáticas en general tienen peculiaridades de no poca importancia en relación con el tema de la investigación, pero las investigaciones relacionadas con las criptomonedas plantean nuevos y arduos desafíos a los investigadores. El uso de servicios de criptografía, mezcla y volteo complica la experimentación de investigaciones rentables, pero en cualquier caso se están desarrollando técnicas de análisis que pueden sortear estos obstáculos.

2.3.6.- Financiamiento del terrorismo a través de criptomonedas

La velocidad típica de las transacciones bitconianas, así como el carácter intrínseco del anonimato, facilitan sin duda la transferencia de grandes sumas de dinero desde países occidentales a países con una alta tasa terrorista y viceversa, o desde estos últimos a favor de los llamados "lobos solitarios" como así lo define Sztandarowski (2019, p. 87), miembros individuales terroristas, pero ciudadanos occidentales. En este caso, es necesario verificar que la conducta antilegal en cuestión sea punible de conformidad con el Código Orgánico Integral Penal.

Para que de forma eficaz regule la financiación de conductas con fines de terrorismo y sancionar a quien ponga a disposición bienes o dinero, de cualquier forma fabricados, destinados a ser utilizados total o parcialmente para la realización de los fines terroristas, independientemente del uso real de los fondos para la comisión del delito en general. En primer lugar, como ya se verificó, la moneda virtual entra en la categoría de bien u otra utilidad.

Sin embargo, estudios recientes muestran como el realizado por Ferro (2020) que en realidad la amenaza de facilitar la actividad de grupos terroristas en la red no es tan real. El financiamiento digital no es uno de los trucos más populares principalmente por dos razones:

el hecho de que la criptomoneda no sea de curso legal, obliga a los prestamistas a confiar en la intervención del intercambiador, que sin embargo está llamado a cumplir con la legislación ilustrada en los párrafos anteriores, segundo, el sistema de transferencia tradicional hawala tiene una alta tasa de éxito hoy como lo fue en el pasado.

Es un sistema de transferencia informal basado en la confianza y que involucra, además del remitente y el destinatario de la suma, dos "*banqueros hawala*". Nacido hace siglos en India y China, este sistema permitía a los inmigrantes en el extranjero transferir sumas de dinero a sus familias, evitando costosas comisiones. El proceso es muy simple: el remitente entrega la suma de dinero al banquero hawala en efectivo más las comisiones; este último paga en la cuenta corriente de su corresponsal, un banquero de Hawala residente en el país del receptor, la suma de dinero neta de comisiones; finalmente, el segundo banquero entrega el dinero al beneficiario en efectivo, reteniendo también las comisiones.

La falta de evidencia documental de estos flujos de dinero hace de este proceso una herramienta muy útil para el lavado de dinero que, sin embargo, al carecer de documentación, podría inducir a los banqueros a retener las sumas optando por no dar por terminada la operación. Precisamente por eso siempre se ha conocido como un mecanismo basado en el honor y la confianza. Confirmando lo analizado, la propia Comisión Europea considera bajo el riesgo de que los grupos terroristas confíen en canales de financiación que utilizan bitcoin en promedio. Específicamente, la amenaza relacionada con el uso de moneda virtual con fines terroristas se cuantifica con un valor de 2 en una escala de 1 a 4 (Almenar, 2018).

2.4.- Cyberlaundering o Cyberlavado y su prevención

En palabras de Posada (2017) El ciberlavado:

> "(…) es un fenómeno que se ha consolidado en los últimos años, y representa la nueva frontera del blanqueo de capitales ya que explota la pulverización del dinero a través de

> Internet y la consiguiente posibilidad de transferir grandes sumas al amparo del anonimato y difícil rastrear.” (p. 327).

También en este caso, las innovaciones tecnológicas han hecho posible que el crimen organizado opere no solo en el mundo real offline, sino también en la red, lo que en realidad representa un terreno más fértil para la persecución de fines ilícitos, tanto que el crimen organizado, logra generar ganancias en mayor medida que los métodos tradicionales de reciclaje, especialmente gracias a los menores costos de operación garantizados por el uso de medios telemáticos y la red.

De hecho, la tecnología de la información y la digitalización de valores han propiciado la transición de un tipo de sociedad basada en el intercambio material de bienes o dinero, a una nueva y diferente economía virtual basada en sistemas de pago digitales, monedas electrónicas, *e-commerce*., donde las transacciones se procesan en segundos y con el mínimo esfuerzo por parte del individuo (Pérez, 2014).

El lavado virtual/cibernético o ciberlavado, evolución del reciclaje tradicional, incluye todas las actividades encaminadas a ocultar el origen delictivo de capitales, activos, valores u otras utilidades, utilizando sistemas informáticos y utilizando la red, incluida tanto la web y de la web oscura y profunda. Es parte de la llamada delitos cibernéticos, es decir, delitos cometidos a distancia mediante el uso de la conexión a internet y sistemas informáticos o electrónicos, y en particular está calificado entre los considerados "Delitos facilitados por computadora", a diferencia de los "delitos informáticos", delitos en los que las computadoras son el objetivo material de la conducta delictiva.

Generalmente, el lavado de dinero “tradicional” desde el punto de vista criminológico se divide en varias fases, y las mismas características también están presentes en el lavado de dinero cibernético. En particular, sin embargo, si para la primera fase (la colocación de dinero de origen delictivo) en el caso del lavado de dinero como se entiende generalmente, es necesaria

una transferencia material del dinero sucio en la economía legal, en el lavado cibernético esto no es necesario. Por tanto, como manifiesta la autora Núñez (2008) el ciberlavado resuelve uno de los mayores problemas del lavado de activos, el manejo físico de grandes flujos de dinero, ya que el dinero a blanquear ya está desmaterializado (ya sea en forma de dinero electrónico o criptomoneda).

Cabe mencionar que se hace una distinción común entre "reciclaje digital instrumental" y "reciclaje digital integral" según Cano (2001). El primero se caracteriza por el uso de internet para mejorar y / o incentivar las operaciones de saneamiento del dinero sucio y se desarrolla en tres fases tradicionales. La fase crítica es sin duda la primera, la de la colocación de capitales de origen delictivo, ya que implica la transferencia física de dinero a purgar en instituciones financieras.

Estos están obligados por ley a someter a los clientes a ciertos procedimientos de verificación, control y denuncia, los cuales solo pueden ser eludidos si existe una asociación delictiva antes del responsable del tratamiento y el control o por corrupción efectiva. Las siguientes fases de estratificación e integración consistentes en realizar un número importante de transacciones financieras mediante la fragmentación del capital para purgar en muchas porciones diminutas y finalmente reubicarlo en actividades formalmente legítimas como establecimientos destinados a diferentes actividades económicas con apariencia o fachada netamente legal.

El reciclaje digital integral, por otro lado, se caracteriza por el hecho de que todos los pasos descritos anteriormente si se realizó completamente en línea y cubiertos por el anonimato. A diferencia del lavado de dinero digital instrumental, en la fase de colocación no es necesario interactuar materialmente con bancos o intermediarios financieros, ya que el dinero de origen ilícito ya está en formato digital.

Esto hace que las otras dos fases sean superfluas, ya que simplemente es necesario apoyarse en una cabeza de madera (la llamada mula del dinero), que también puede ser una identidad virtual, creada mediante la producción de un documento. De hecho, es muy posible abrir una cuenta en línea, sin someterse a los controles impuestos a los bancos al registrador de un nuevo cliente.

Existen varias formas prácticas de configurar el reciclaje digital integral según Pérez (2014), como la constitución de empresas ficticias (las llamadas empresas pantalla), la creación de líneas telefónicas, la falsa facturación y el denominado préstamo, juegos de azar en línea y más. Las empresas fantasma, en particular, son empresas que básicamente no realizan ninguna actividad comercial, y se constituyen con el único propósito de hacer depositar el capital ilícito para luego reintroducirlo en la economía real, todo ello con el acuerdo de un testaferro. Generalmente se establecen en los denominados paraísos fiscales, ya que las regulaciones de los países antes mencionados garantizan el anonimato a través del secreto bancario y muy a menudo están poco interesados o alentados a cooperar con las autoridades investigadoras extranjeras.

Un breve examen merece la pregunta sobre el juego online, una de las actividades más rentables para el crimen organizado. Gracias también a los enormes volúmenes de dinero que implica, no solo implica la proliferación de comisión de actividades de lavado de activos, pero también usura, extorsión y financiamiento criminal. Dado que está digitalizado, el juego online se presta tanto como una actividad dentro del reciclaje digital instrumental, como una actividad real de ciberlavado (Posada, 2017), ya que es posible mover grandes cantidades de capital ilícito en poco tiempo sin necesidad de ningún contacto físico.

Según Luna (2020), sugiere que hay que tener en cuenta que operar online permite utilizar VPN (TOR, tunnelbear y similares), que enmascaran la dirección IP y resulta casi imposible determinar la ubicación y más aún la identidad del delincuente, dificultando de tal suerte la

identificación y localización del usuario en la red. Si luego se utilizan criptomonedas como bitcoin o CasinoCoin, la identificación será aún más difícil, también porque es posible limpiar aún más las criptomonedas ilícitas mediante la compra de bienes o servicios o la conversión a moneda fiduciaria.

Ejemplos de blanqueo cibernético aún más simple en la práctica son el uso de pago electrónico, o tarjetas inteligentes: son utilizadas diariamente por el crimen organizado como alternativa al efectivo para realizar transacciones telemáticas con las que se compran bienes o servicios mediante el intercambio de dinero electrónico o incluso dinero virtual (Lacarte, 2018).

Debe tenerse en cuenta que el uso de tarjetas inteligentes, como medio alternativo de hacer circular dinero en efectivo, está fuertemente fomentado por las regulaciones contra el lavado de dinero de varias jurisdicciones en virtud de la posibilidad de rastrear electrónicamente los movimientos de dinero de cualquier monto. Dicho esto, se podría argumentar que las tarjetas inteligentes eliminan por completo los riesgos de lavado de dinero, pero no es así: la trazabilidad de las transacciones es una excelente herramienta de control, pero realmente sería posible rastrear e identificar al actor de las transacciones solo si son rastreables a una cuenta corriente a nombre de una persona previamente identificada (Ledezma, 2018).

Además, es posible duplicar o alterar ilegalmente los chips de almacenamiento de datos de las tarjetas inteligentes, interviniendo tanto en los datos de identificación como en la suma disponible; también es posible modificar los límites de gasto diario (impuestos con fines de prevención de blanqueo de capitales), así como incluir transacciones de origen ficticio. Pero las posibilidades de evadir los controles no terminan ahí, ya que es posible explotar los incumplimientos en la normativa antilavado de dinero de los países más permisivos, y así también poder abrir cuentas bancarias y hacerse con tarjetas inteligentes a través de la red de presentación de documentos falsos o la creación de identidades ficticias (Almenar, 2018).

Por último, hay casos en los que hacerse con una tarjeta inteligente no es necesario abrir una cuenta bancaria y por tanto pasar por los controles anti-blanqueo que los bancos están obligados a realizar, y ni siquiera es imprescindible contactar con el emisor, especialmente en el momento del depósito inicial del capital. De hecho, existen máquinas expendedoras automáticas de tarjetas prepago que le permiten convertir efectivo en dinero digital sin identificación previa, o recargar tarjetas inteligentes ya emitidas.

Esto facilita la fase de estratificación, ya que bastará con tomar posesión de dichas tarjetas inteligentes emitidas por las mencionadas máquinas expendedoras y recargarlas con el dinero a limpiar. La última fase, la de integración, se implementará simplemente gastando el dinero almacenado en las tarjetas inteligentes en bienes y servicios legítimos. También cabe mencionar la posibilidad de abrir una cuenta en la plataforma Paypal, que solo requiere una dirección de correo electrónico y un número de móvil (Martínez & Fernández, 2020).

La característica de Paypal es que le permite recibir y enviar pagos sin ningún depósito previo de dinero, posponiendo así los cheques anti-lavado de dinero solo en la siguiente fase y cualquier crédito a una cuenta bancaria. Por tanto, Paypal se presta para ser utilizado eficazmente para operaciones de colocación y también ocultación de dinero sucio, especialmente si va acompañado de identidades digitales falsas o robado ilegalmente a terceros.

No obstante, el uso de tarjetas prepago emitidas por emisores autorizados y por tanto el uso de dinero electrónico, o la ejecución de transferencias bancarias realizadas a través de identidades falsas o las denominadas ficticias, no son de ninguna manera comparables al uso de nuevos sistemas de pago no regulados y cuyo funcionamiento no es gestionado por un organismo central autorizado como las criptomonedas.

Estas operaciones están completamente fuera del sistema financiero y bancario, su emisión y circulación no está centralizada y por lo tanto es aún más difícil oponer controles al movimiento de dinero dentro y fuera de lo virtual. La verificación de la autenticidad de las

transacciones no se delega en un intermediario o un organismo garante, sino que se basa en el sistema de consentimiento y, por lo tanto, en la confianza mutua de los participantes de la red (Ortiz, 2013). Para enviar y recibir bitcoins no es necesario abrir una cuenta corriente, ni utilizar tarjetas de crédito ni realizar depósitos y retiros.

Simplemente necesita descargar el cliente oficial de criptomonedas, que es una billetera electrónica que contiene y le permite intercambiar la criptomoneda, o necesita comprarlos a través de un intercambio (proveedores de servicios que operan como cambistas de dinero) y luego transferirlos a un billetera (la mayoría de los intercambios también brindan un servicio de billetera); en el primer caso, los usuarios nunca pueden entrar en contacto con el sistema bancario o financiero, mientras que en el segundo caso los usuarios tendrían que interactuar con los intercambios financieros.

Disposiciones sobre blanqueo por parte de la V Directiva. Esto no hace que las criptomonedas sean intrínsecamente ilegales, pero de hecho facilitan no pocas actividades delictivas de todo tipo, no solo el lavado de dinero, sino también la extorsión a través de la web, la corrupción y el tráfico ilícito, además de ser un medio de recompensa para los Smart contracts (Arbulú, 2018).

De hecho, el anonimato, la confidencialidad, la inmediatez y la flexibilidad no solo facilitan la limpieza del dinero sucio, sino que son sin duda las razones por las que se prefiere el intercambio de criptomonedas al cambio de moneda fiduciaria a pesar de la extrema volatilidad del valor, lo que los convierte en un verdadero paraíso para la delincuencia.

El ejemplo más inmediato de lavado de activos a través de bitcoins está representado por la compra de bitcoins u otras criptomonedas con producto de otros delitos, obstaculizando así efectivamente el origen criminal de los mismos. Las ganancias sustanciales generadas por los delitos económicos y las ganancias obtenidas en forma de efectivo (derivadas del tráfico de drogas, extorsión, prostitución, etc.) pueden digitalizarse de la manera descrita anteriormente y

luego limpiarse con un mínimo esfuerzo mediante la compra de moneda virtual, que como resultado del creciente número de personas dispuestas a aceptarlo como contraprestación, permite la depuración del capital ilícito con el mínimo riesgo de ser rastreado.

Aún más simple, es posible limpiar el efectivo "sucio" contactando a los poseedores de criptomonedas que estén dispuestos a venderlo a cambio de efectivo; incluso una simple aplicación de teléfono inteligente es suficiente y es posible realizar la transacción en vivo cara a cara, en un lugar público, sin tener que digitalizar primero el efectivo (Franco, 2014).

Resumen del capitulo

Al culminar este interesante capitulo nace una incógnita: ¿Están las criptomonedas realmente dispuestas a revolucionar la industria de la inversión financiera o son un instrumento creado para el cyberdelito? Nunca antes las noticias internacionales se habían ocupado tanto de las criptomonedas y, en particular, de bitcoin, por criptomoneda, literalmente, nos referimos a una moneda digital que se puede utilizar a través de claves de acceso públicas o privadas que solo pueden ser interpretadas por aquellos que están autorizados a leerlas.

No son administrados por autoridades centrales, sino por computadoras descentralizadas y prácticamente cualquier persona puede unirse a esta red mundial. Bitcoin es sin duda la criptomoneda más famosa, creada en 2009 por Satoshi Nakamoto, seudónimo de quien inventó esta criptomoneda. No tiene soporte físico, se puede almacenar en carteras online y ahora se puede utilizar para realizar numerosas transacciones como compraventa de inmuebles, bienes, servicios, productos ilícitos, financiación de la delincuencia organizada, etc., esta moneda virtual tiene sin lugar a dudas la ventaja de ser de uso inmediato y de tener unos costes de transacción muy reducidos, sensiblemente inferiores a los de los instrumentos financieros tradicionales, razón por la cual, en opinión de algunos, sería fuertemente opuesta por el sistema bancario que sí lo hace.

Sin embargo, también tiene algunas desventajas, ya que el dinero virtual se puede robar o perder como consecuencia de un ataque de piratas informáticos o un mal funcionamiento de Internet, por lo que tiene menos garantías que cualquier otra inversión financiera. El crecimiento global del fenómeno de las criptomonedas no hace más que incrementar este tipo de riesgos, estos métodos de pago permiten, con un simple acceso vía internet, tener rápidamente un medio que le permita realizar pagos entre diferentes países, sin tomar en cuenta ningún tipo de distancias y límites. Continuando, entre los factores de riesgo, hay que tener en cuenta que los métodos de funcionamiento de las criptomonedas suelen estar basados en multitud de infraestructuras informáticas, también ubicadas en países extranjeros; la presencia de una pluralidad de sujetos fragmentados, y muchas veces ubicados en diferentes países, dificulta mucho más a las autoridades reguladoras y policiales el acceso a este tipo de información.

Nuevamente, debe recordarse que algunas de las jurisdicciones donde se encuentran asentados los sujetos (componente en diversas capacidades de los nodos de estas redes distribuidas de operadores) no cumplen, a nivel de legislación, con los estándares mínimos en materia de prevención del uso del sistema financiero para el blanqueo de capitales o la financiación del terrorismo. Finalmente, se puede decir que las criptomonedas con su naturaleza de descentralizadas permiten finalizar transacciones anónimas de sujeto a sujeto, y esta dimensión del intercambio se da fuera del perímetro de una jurisdicción en particular, en un ciberespacio completamente desmaterializado e imperceptible.

CAPÍTULO III

MARCO METODOLÓGICO

3.1.- Unidad de análisis

Corresponde en este apartado el manifestar que en el presente trabajo investigativo se utilizó la doctrina, legislación y demás fuentes del derecho acerca del estudio del fenómeno en análisis, esto es la ausencia de normativa penal para reprimir el lavado de activos a través de criptomonedas, abordando características de real importancia como el análisis de sus elementos, cuestiones de forma y de fondo, estudio de la cuestión en el país.

3.2.- Métodos empleados

Con el fin de estudiar el tópico en correspondencia hemos seleccionado los métodos de investigación jurídica que se puntualizan a continuidad:

Método sistemático: Es aquel que analiza la normativa cotejándola con las demás normas jurídicas relacionadas con la materia y con los principios generales del derecho.

Método de interpretación lógico: Explora el espíritu de la ley tomando también en consideración particularidades externas a la norma como el argumento histórico, la intención racional (razón) que sirvió para la creación y expedición legislativa.

Método de interpretación doctrinal: Esta es la interpretación jurídica que forman los juristas, académicos, abogados, para alcanzar a comprender una disposición normativa o para aclarar aspectos científicos y su dialéctica.

3.3.- Enfoque de la investigación

En la presente investigación se le dio un enfoque mixto esto es cualitativo y cuantitativo, este último porque se recolectaron datos concretos del mundo real, el problema es medible, se apoya en el marco teórico, la creación de la hipótesis es realizada antes de la investigación, es decir, en el planteamiento del problema; es también de enfoque cualitativo porque por parte del investigador se ha observado de manera directa el fenómeno de una forma más social, está basada también en la observación directa, entonces podemos decir que es un enfoque mixto porque se complementan entre las dos, de tal suerte que mejora la comprensión del problema, mejora la creatividad porque en esta se puede usar o utilizar varios métodos de recolección de datos que consiente llegar a una mejor conclusión o conclusiones dentro de la indagación, y por último permite una recolección deferente de la información como datos numéricos y no numéricos lo cual hace que la investigación tenga una perspectiva mucho más amplia. (Pulido, 2014).

3.4.- Tipo de investigación

Investigación teórica: Su principal visión es el establecer nuevas sapiencias referentes al problema que se inquiere, sin que sea menester de comprobarlos con la práctica. (Baena, 2014).

Investigación documental bibliográfica: Es la exploración del contenido de libros elaborados por juristas de relevancia en el tema, cuando se trata de trabajos de derecho, guiado por el principio de referencia, a la vez estudio y análisis de sentencias, artículos científicos y demás textos académicos que tengan un gran aporte en el tema y demás elementos y características con referencia al tópico indagado. (González S. , 2015).

Investigación descriptiva: Busca de forma metódica la descripción de las características del objeto de estudio a través de fuentes de información precisa, verídica y comprobable para abordar de mejor manera la realidad de los hechos. (Sabino).

3.5.- Diseño de la investigación

En el presente trabajo de carácter académico investigativo el diseño es no experimental porque no se ha alterado las variables de estudio, sino que se ha observado el fenómeno como se desarrolla en su contexto natural y lo que se hizo es examinarlo.

3.6.- Población de estudio

Para el presente trabajo de carácter académico indagatorio, no es menester utilizar a un grupo de personas, debido a que fue una de carácter teórico con enfoque de investigación jurídica, específicamente se estudió las fuentes del derecho a nivel internacional y nacional, usando los métodos de investigación antes descritos, como el de interpretación doctrinal, el cual se basa en análisis de referentes juristas de la materia, por eso es innecesario inmiscuir a personas para esta exploración.

3.7.- Técnicas de recolección de datos

Los datos fueron recogidos desde la lectura, análisis, examen, exploración de documentos de tal forma que se realizó primero un acopio de la información y se procedió a la elaboración de fichas bibliográficas.

3.8.- Técnicas e instrumentos de análisis e interpretación de la información.

La información recolectada, analizada y sistematizada ha sido desarrollada y ubicada tal como consta en el índice de contenido de la presente investigación académica después de haber elaborado anotaciones de carácter informático y manuscrito. Como instrumentos de investigación se utilizaron las fichas de contenidos donde se recoge la información relativa a cada una de las fuentes como es el autor, año de publicación, tipo de fuente y citas y referencias

incorporadas en el presente texto. Asimismo se utilizaron tablas analíticas para comparar los aportes de cada uno de los autores y las características principales de los conceptos y categorías analizadas, como son el lavado de activos, criptomonedas y las diferentes manifestaciones delictivas que se cometen a través del ciberespacio.

3.9.- Comprobación de hipótesis

Como punto de partida tenemos a una hipótesis afirmativa: "Existe ausencia de normativa penal para reprimir el lavado de activos a través de criptomonedas.", razón por la cual a través del andamiaje analítico desarrollado *ut supra*, se puede decir que se comprueba la hipótesis de forma positiva por haber corroborado el estudio en las dos variables, en ese sentido tenemos de primera mano que las criptomonedas en el contexto internacional y más aún en el país no cuentan con regulación y es por eso que se facilita a la delincuencia el cometimiento de delitos específicamente el lavado de activos por su ausencia de regulación y prevención en el Ecuador. Por lo tanto podemos arribar a establecer que la hipótesis se encuentra comprobada afirmativamente, como se demuestra en los resultados obtenidos, las conclusiones y la propuesta que se formula en el capítulo siguiente.

3.10. Referentes empíricos y limitaciones del estudio

Los referentes empíricos de la investigación están constituidos por los recurrentes hechos de lavado de activos a través de diferentes vías, una de las cuales son las criptomonedas que por su naturaleza anónima pueden ser utilizadas por cualquier persona para esos fines. Desde el punto de vista conceptual los referentes empíricos son los datos o aspectos de la realidad que se observan y se analizan en la búsqueda de la verdad; en el presente estudio esos referentes son casos que han sido investigados y leyes vigentes para prevenirlos y sancionarlos.

Frente a la ocurrencia de esos hechos de lavado de activos mediante criptomonedas que hasta el presente son aislados en el Ecuador, el país ha ido adoptando medidas a través de las instituciones competentes como la Unidad de Análisis Financiero y Económico que considera que existe un riesgo medio-alto que debe ser enfrentado con las herramientas y las tecnologías adecuadas para ello.

Una de las propuestas que se han realizado en la materia es que se realice sobre las "monedas virtuales deberán ser sujetas a un control estatal que permita garantizar la transparencia de sus operaciones, eliminado riesgos como el lavado de activos, fraude o evasión tributaria" (Navarrete y Wong, 2018, p. 2). Otros referentes empíricos se obtuvieron de investigaciones realizadas en otros países como Perú y Colombia.

En Perú Fiorela Pinco Espinal y Rafael Rodríguez Lizana investigaron el tema "El delito de lavado de activos y la utilización o uso de criptomonedas." Su conclusión más relevante para el presente estudio fue que "a la fecha no hay un marco normativo para la persecución y sanción de los sujetos que, usando criptomonedas puedan estar lavando activos; sin embargo, esta ausencia legal no debe constituir impedimento para establecer que los factores criminológicos que inciden en el lavado de activos usando criptomonedas, y que deben tomarse en cuenta para su posterior regulación, tiene relación indubitablemente con el uso de herramientas tecnológicas" (p. 91).

En la Universidad Militar Nueva Granada de Colombia Erika Brigette Parra Tabares investigó el tema "Las criptomonedas: una nueva modalidad de lavado de activos en Colombia", donde concluyó que "si bien el gobierno en Colombia ha intentado la implementación de diferentes normas para la regulación de las criptomonedas, no se han llevado a cabo efectivamente y han sido insuficientes por la multidimensionalidad que alcanza el uso y la actividad de esta nueva modalidad de pagos. Por lo anterior, se considera necesario que se comience hablar de una legislación y regulación pronta, ya que hay muchas empresas al rededor

del mundo que están aceptando pagos con Bitcoins, esto puede comenzar a generar más iniciativa por parte de estas organizaciones para la creación de nuevas plataformas ilícitas. Así como un mecanismo de control para evitar que los grupos delictivos accedan al mercado de las monedas virtuales."

Como puede apreciarse, en ambos casos los autores señalan que en sus respectivos países no existe un marco regulatorio para prevenir, investigar y sancionar el delito de lavado de activos a través del uso de criptomonedas, y con base en ello formulan diversas propuestas en el ámbito normativo que podrían ser herramientas útiles para solventar el problema señalado. Una situación similar en el Ecuador como se puede advertir en la legislación vigente, por lo que en el capítulo IV se presenta una propuesta que incluye reformas legales y medidas de tipo tecnológico para controlar el uso de criptomonedas y evitar su uso como canal para el lavado de activos.

Las principales limitaciones del estudio se encuentran en la imposibilidad de aplicar instrumentos de investigación empírica a expertos en materia de lavado de activos, criptomonedas y criminalidad cibernética, ya que hubiera sido pertinente conocer su opinión sobre este fenómeno y sus manifestaciones concretas en el Ecuador, así como las medidas que consideran deberían adoptarse para su correcta prevención y sanción.

Otra de las limitaciones del estudio es la falta de un estudio de Derecho Comparado a nivel internacional para sistematizar las principales medidas aplicadas en diferentes países en cuanto a la regulación y control del uso de criptomonedas, la prevención del lavado de activos por esa vía y la investigación y sanción de los responsables, lo cual hasta el momento es un sector incipiente de estudios, pero va creciendo vertiginosamente.

También es una de las limitaciones en la presente investigación es por el hecho de ser un tema jurídico de vanguardia , de actualidad, nuevo; no hay jurisprudencia sobre el tema de investigación, esto es una limitación para profundizar el eje temático, por lo que las propuestas

de solución se encuentran a nivel de investigaciones teóricas con muy poco sustento empírico, legal y jurisprudencial.

Con base en ello consideramos que en futuras investigaciones sobre el tema se deberían hacer estudios empíricos aplicando cuestionarios a expertos en los temas señalados, así como estudios de Derecho comparado que permitan construir una panorámica general sobre el tema y sustentar la propuesta con datos teóricos, empíricos y legislativos que permitan dotarla de una mayor viabilidad en el contexto del régimen jurídico ecuatoriano vigente.

3.11 Resultados: el delito de lavado de activos: generalidades y concepciones en el Ecuador

Los resultados que se presentan en este apartado dan respuesta a cada uno de los objetivos específicos planteados en la investigación; consecuentemente, se hace un análisis del delito de lavado de activos que es cometido mediante criptomonedas como una nueva forma de delinquir en el Ecuador y se identifican las normas procesales que regulan el lavado de activos y las criptomonedas en el Ecuador. La propuesta de regulación especial a las criptomonedas para evitar el cometimiento de lavado de activos en el Ecuador se formula en el capítulo siguiente.

Por blanqueo de capitales, Seaoane (2020) lo define así: "el medio por el cual se oculta la existencia, la fuente ilícita o el uso ilícito de ingresos y luego estos ingresos se disfrazan para hacerlos parecer legítimos" (p. 41). Este tipo penal da lugar a una serie de actividades delictivas de carácter transnacional y ha alcanzado un nivel de globalización igual al del mercado financiero, desde el cual explota los cauces para la conservación y aumento de la riqueza de origen ilícito.

Como la doctrina autorizada recordó recientemente, el concepto metajurídico de lavado de dinero puede resumirse en la definición ahora clásica proporcionada en 1985 por la Comisión Presidencial de los Estados Unidos sobre el Crimen Organizado (*The Cash Connection: Organized Crime, Financial Institutions, and Money Laundering*) y posteriormente

implementado por la doctrina de nuestro país: por blanqueo de capitales entendemos el medio por el cual nace la existencia, la fuente ilícita o el uso ilícito de los ingresos y luego estos ingresos se disfrazan para hacerlos parecer legítimos (Gudiño, 2013).

El blanqueo se divide normalmente en varias fases que se suceden en el tiempo. Originalmente se consideraba un modelo de actividad que se desarrollaba en dos fases: blanqueo, que se identificaba en operaciones de corto plazo destinadas a camuflar el origen ilícito del dinero u otros activos; y el uso (reciclaje), consistente en operaciones de mediano o largo plazo destinadas a reintroducir el capital lavado en el ciclo económico lícito. Según Tondino (2009) esta subdivisión prevé un caso de este injusto y otro para el uso de dinero, bienes o beneficios de procedencia ilícita según.

Con el tiempo, la literatura internacional ha adoptado una división de actividades más compleja en tres fases diferentes: ubicación, estratificación e integración. La colocación consiste en la colocación material del producto del delito (piense en el dinero obtenido de la venta de drogas) con instituciones financieras o intermediarios, directamente en el mercado o en el exterior.

Para Callegari (2003) al explicar la estratificación, la misma consiste en realizar una serie de operaciones financieras encaminadas a separar el capital de su origen ilícito: en los grandes circuitos internacionales de reciclaje esta fase involucra a profesionales de las altas finanzas, capaces de secuestrar capital sucio vía cable a través de las instituciones financieras de muchos países, con especial preferencia, por supuesto, por los paraísos fiscales.

Finalmente, la integración está constituida por el esfuerzo de integración en los circuitos de la economía lícita de las capitales que derivan su origen de actividades delictivas. En cualquier caso, el reciclaje da lugar a una sucesión de actividades interconectadas, a un proceso continuo, cuyas fases en ocasiones tienden a superponerse y confundirse.

Como han señalado autores de la materia como el estudioso del Cid (2007) en la época actual los lugares eminentes del blanqueo de capitales ya no son solo los bancos y los intermediarios financieros, sino también muchas otras actividades no estrictamente financieras, sobre las que el advenimiento de los métodos típicos de la economía *net economy*, que ha introducido una nueva dimensión sumamente atractiva y buscada por quienes se dedican a actividades de lavado: la del ciberlavado, y de hecho: cuando se trata de banca en línea, comercio en línea, dinero electrónico (e-cash), pero también instrumentos de crédito más comúnmente computarizados, como tarjetas prepagas o tarjetas inteligentes, etc. todas noticias recientes pero ya bien probadas en la web: nos referimos a contextos extraordinariamente fructíferos para las operaciones de blanqueo, donde muy a menudo es posible eludir fácilmente el principio (solo nominalista) de "conocer a su cliente" (del Cid, 2007, p. 88). De hecho, la progresiva centralidad de Internet es indiscutible, como un lugar eminente para el lavado de activos que apoya cada vez más al canal bancario tradicional, y se sabe que los nuevos actores de la economía de la red son los potenciales operadores que pueden ser utilizados para el blanqueo de dinero.

El lavado de activos da lugar a una serie de actividades delictivas de carácter transnacional y ha alcanzado un nivel de globalización igual al del mercado financiero, desde el cual explota los cauces para la conservación y aumento de la riqueza de origen ilícito. Se ha señalado que la delincuencia transnacional muchas veces ya está aguas arriba: no es casualidad que la represión del fenómeno se originara en la necesidad de contrarrestar el beneficio económico derivado del tráfico internacional de drogas (blanqueo de ingresos de drogas).

Sin embargo, con mucha más frecuencia es el proceso de saneamiento o lavado de capitales ilícitos, debido a la dislocación de las distintas fases en las que se articula en diferentes contextos nacionales y extranacionales. La dimensión transnacional del lavado de activos

corresponde a la necesidad, sentida por la comunidad internacional, de preparar estrategias comunes para la represión del fenómeno. (Bajo, 2009).

En primer lugar, las Cuarenta Recomendaciones contenidas en el Informe presentado el 7 de febrero de 1990 por el Grupo de Acción Financiera (GAFI), el organismo internacional más autorizado para la formulación de políticas contra el lavado de dinero, establecido en París en julio de 1989. Describe en detalle las medidas, tanto preventivas como represivas, que se adoptarán para combatir el fenómeno en cuestión.

Las recomendaciones no incluyen una verdadera definición de lavado de dinero, pero se refieren expresamente a la provista por la Convención de Viena, que el GAFI sugirió extender a todos los delitos graves que puedan generar ganancias significativas. Al respecto, Mallada (2012) señaló que, si bien tienen una fuerte trascendencia política y reputación internacional, las recomendaciones del GAFI no tienen un impacto directo en la modificación de las leyes de los Estados Miembros.

Debido a la influencia directa que se ejerce en el ordenamiento jurídico de los Estados miembros, debe informarse la Convención sobre el blanqueo, registro, embargo y decomiso del producto del delito, adoptada por el Consejo de Europa en Estrasburgo el 8 de noviembre de 1990 (Seaoane, 2020), con la que se proporcionó un nueva definición de delitos de blanqueo de activos, se amplía la categoría de delitos determinantes, que ya no se limitan a los vinculados al narcotráfico, y la adopción de sanciones también por blanqueo de carácter culposo cuando el autor debió haber creído que los bienes constituían ingresos.

En cuanto a los actos legislativos de matriz comunitaria, refiriéndome a la Unión Europea, la Directiva del Consejo de las Comunidades Europeas relativa a la prevención del uso del sistema financiero para el blanqueo del producto de actividades ilícitas de 10 de junio de 1991 (n. 91/308 CE). La Directiva, que en el contexto del artículo 1 define las prácticas de blanqueo de capitales, resume el contenido de documentos anteriores que habían abordado los

mecanismos para prevenir la contaminación del mercado financiero por capitales ilícitos y establece los siguientes principios identificados por Náquira (2018):

a) necesidad de combatir el lavado de activos a través de leyes penales específicas, adoptadas como parte de la cooperación internacional encaminada a combatir el fenómeno, por considerarse indispensable; b) la necesidad de prever también instrumentos no penales, garantizando en particular la colaboración de las autoridades supervisoras bancarias y del sistema financiero en general; c) la necesidad de ampliar el concepto de blanqueo de dinero también a delitos determinantes distintos de los relacionados con el tráfico de drogas; d) la necesidad de asegurar que las instituciones de crédito y financieras, como todas aquellas que realizan profesionalmente actividades de importación de transferencias de dinero, requieran la identificación de personas que realicen transacciones que superen cierto monto; e) la necesidad de imponer a las instituciones de crédito y financieras la obligación de mantener, por lo menos durante cinco años, el registro de identificación de las personas que han realizado las operaciones señaladas; f) la necesidad de que estas entidades presten atención a cualquier transacción sospechosa y la denuncien a la autoridad competente; g) finalmente, la necesidad de limitar, en estos casos, el funcionamiento del secreto bancario.

En el Ecuador el delito de lavado de activos se tipifica en el artículo 317 del Código Orgánico Integral Penal, es necesario precisar que existen algunos verbos rectores de esta conducta atribuible a una persona sin especificar si es jurídica o natural. Dentro de los referidos verbos que hacen parte de la tipicidad objetiva del injusto, se observa a la persona que tenga, transfiera, posea, oculte, disimule, adquiera, resguarde, transporte, entregue o se beneficie de cualquier forma de capitales ilícitos, a la vez a la persona que disimule, o impida determinar la procedencia de ilícitos penales; a quien financie, participe, gestione, o asesore este tipo de injustos; a quien haga por sí o por medio de terceros operaciones o transacciones de carácter

económico o financieras con el fin de transformar los fondos ilícitos en lícitos; a la persona que ingrese al país o se vaya del mismo con dinero de origen ilícito.

Este tipo de delito es considerado como uno autónomo y subsiste el deber de fiscalía de inquirir el origen de estos fondos; a criterio de Pedro Intriago (2015, p. 45) el fiscal es un investigador, quien debe buscar el equilibrio de la justicia; pero con una exigencia académica especializada en el ámbito en el cual desempeña sus funciones, es por tal motivo que la sociedad necesita de fiscales entendidos en la materia para que de esta forma puedan actuar con objetividad, apegados a derecho, y requerir de justicia ante el juez competente.

Como podemos observar en el Ecuador, el legislador ha previsto el Código Orgánico Integral Penal, para tipificar en la parte sustantiva los delitos y las penas, en este caso con referencia al lavado de activos, únicamente regula en el artículo 317 las modalidades para efectuar y sancionarlo, dejando en blanco o en atipicidad la modalidad del injusto penal en estudio que se comete a través de criptomonedas.

De hecho en el país no tenemos legislación para detectar, prevenir y sancionar dicha modalidad del lavado de activos, eso será motivo de estudio más adelante conforme abordaremos la temática en cuestión, pero cabe mencionar que existe una Ley de Prevención de Lavado de Activos y del Financiamiento de Delitos, su reglamento; una resolución de la Superintendencia de Compañías emitida el 16 de marzo de 2021; otra resolución de la Corporación Financiera Nacional No. 104 de 08 de febrero de 2021, existe un Manual de Ingreso y Salida de Dinero Sujeto a Control de Lavado de Activos, del año 2016; y, en todos estas normas jurídicas vigentes no se hace referencia a las criptodivisas que puedan servir como instrumento al cometimiento de lavado de activos, sino se hace referencia de su existencia peor aún de su regulación, prevención y sanción.

CAPITULO IV

PROPUESTA

Consideraciones previas

A partir de los análisis realizados en este trabajo académico, hemos identificado los dos caminos que enfrenta el delincuente que se dedica al lavado de activos a través de criptomonedas, y por los que tendría la posibilidad de sanear el producto de origen delictivo. Por un lado, puede optar por acudir a un *exchange* para convertir la criptomoneda en moneda de curso legal, pero en este caso la legislación ya ha delineado claramente las obligaciones que la figura del cambio de divisas está llamada a cumplir con los fines de blanqueo.

Por otro lado, el blanqueador podría decidir mantener las ganancias dentro de fronteras virtuales. En este segundo caso, imaginamos que el sujeto pretenderá gastar las sumas obtenidas a través de actividades ilícitas en aquellos sitios web que acepten moneda virtual como medio de pago.

En el país identificamos en este pasaje un vacío normativo, que establece que los proveedores de servicios relacionados con el uso de moneda virtual están obligados a cumplir con las obligaciones contra el blanqueo de capitales o lavado de activos, limitadas a realizar la conversión de monedas virtuales desde o hacia monedas fiduciarias. Por tanto, los proveedores de servicios relacionados con el uso de criptomonedas que no realizan actividades de conversión, como por ejemplo, los gestores de sitios de comercio electrónico que aceptan moneda virtual como medio de pago, parecen quedar fuera del grupo de sujetos obligados. De esta manera, el sujeto activo de la infracción puede limpiar de manera segura el dinero sucio comprando bienes y servicios en sitios donde la criptomoneda este permitida o aceptada para el comercio. En consecuencia, es necesario establecer una serie de obligaciones que deben cumplir todas las empresas de comercio electrónico que afirmen aceptar pagos en criptomonedas.

Propuesta

De acuerdo con la ausencia normativa del país es necesario que se reforme el artículo 317 del Código Orgánico Integral Penal, y a la vez varias resoluciones que no contemplan a las criptomonedas como la Resolución de la Superintendencia de Compañías, publicada en el Registro Oficial Suplemento 411 de 16 de marzo de 2021, la Ley de Prevención de Lavado de Activos y del Financiamiento de Delitos, su reglamento, y demás resoluciones que tratan el lavado de activos pero no con modalidad virtual a través de criptodivisas, esto con el fin de prever y regular este tipo de actos ilícitos las siguientes consideraciones a tomar en cuenta:

1.- El sitio web que opere en el Ecuador, que acepta pagos en criptomonedas y tiene la intención de realizar sus negocios dentro de las fronteras ecuatorianas esté inscrito en un registro especial mantenido por la Policía Nacional u órgano de control como el Servicio de Rentas Internas. Adjunto será necesario entregar una lista que contenga los nombres y datos personales de los empleados del grupo comercial.

2.- Considerando que en el derecho penal económico tenemos el compliance, y esto obedece a que los sitios web como empresas o compañías, cualquiera sea su naturaleza, tengan por imperio de la ley, responsables de cumplimiento o compliance officers del sitio web mencionado, en armonía con el Art. 35 y siguientes de la Resolución de la Superintendencia de Compañías, publicada en el Registro Oficial Suplemento 411 de 16 de marzo de 2021, y que esté obligado a:

2.1.- Identificar al cliente que tiene la intención de pagar en criptomonedas;

2.2.- Verificar su identidad sobre la base de documentos, datos e información obtenidos de una fuente confiable;

2.3.- Conservar los datos relativos al cliente y la operación y comunicarlos inmediatamente a la Policía Nacional u órgano de control. Este último mantendrá todos los

datos relacionados con los pagos realizados en criptomonedas en los sitios de comercio electrónico dentro de las fronteras nacionales en un registro especial;

2.4.- Informar la imposibilidad de concluir la venta cuando no sea posible proceder con la debida diligencia del cliente;

2.5.- Informar al Servicio de Rentas Internas, de la venta de uno o más productos a un cliente por un pago igual o superior a 3.000 dólares, o de varios pagos cuya suma sea superior o igual a 3.000 efectuados en menos de 15 días;

2.6.- Informar la posible transacción, antes de concluir la venta, a la Unidad de Análisis Financiero y Económico (UAFE), en caso de que tenga motivos razonables para sospechar que una actividad de blanqueo de capitales está en curso, teniendo en cuenta la capacidad económica y la actividad que realiza la persona a quien se refiere.

3.- Adopción de salvaguardas, controles o procedimientos internos específicos;

4.- Adoptar cursos de capacitación y actualización permanente para el personal en materia de prevención del blanqueo de capitales.

Utilizamos un ejemplo práctico para comprender cómo cambios de este tipo podría, por un lado, dificultar al sujeto activo la limpieza de sus ganancias y, por otro, facilitar la investigación de las autoridades: Supongamos que la parte lesionada, descubrió que su computador estaba infectada con *roansomware*, un virus que impide el acceso a su software excepto mediante el pago de un rescate en criptomonedas. El sujeto pasivo o victima paga la suma solicitada y acude a la Policía Nacional o Fiscalía General del Estado para presentar una denuncia. El perjudicado que paga el precio no incurre en ningún perfil penal. En este punto la Policía, mediante el registro especial en el que todos los pagos realizados en criptomonedas en todos los sitios de comercio electrónico que acepten moneda virtual como medio de pago, podrá identificar un grupo de usuarios a los que gastaron la exacta cantidad que pagó, la víctima con una sola compra o múltiples compras.

Es cierto que la persona que recibió la suma de dinero de la víctima puede haber entregado el producto en manos de diferentes cómplices que luego gastaron las sumas en diferentes sitios de comercio electrónico en diferentes días, por lo que el registro anterior no será particularmente útil, pero sin duda facilitará la actividad de investigación. Las autoridades competentes podrán rastrear fácilmente las identidades de los posibles delincuentes, y no depender simplemente de códigos alfanuméricos que ocultan los datos de la persona física que realiza los pagos en criptomonedas.

También es necesario "educar" a los usuarios: cualquier persona que posea una computadora personal, teléfono inteligente o tablet debe saber cuáles son los organismos competentes a los que acudir en caso de hacking. Esto se debe a que, por ejemplo, el artículo 190 del Código Orgánico Integral Penal, sanciona a todo aquel que acceda ilegalmente a un sistema informático o telemático protegido por medidas de seguridad. Esto significa que el agraviado debe necesariamente presentar una denuncia ante la autoridad competente para la investigación, caso contrario es imposible que de oficio se indague el caso.

Con respecto a los sitios de juego y casinos en línea, es de fundamental importancia obligar al jugador a declarar su identidad personal a través de un documento válido y que se realice un proceso de validación con los registros oficiales. Esto no será un gran problema para el jugador que no tiene nada que ocultar, pero indudablemente inducirá al blanqueador a elegir otro camino para limpiar las ganancias ilícitas.

Finalmente, el tema de la transnacionalidad merece una atención especial, es decir, la oportunidad de colaborar con organizaciones criminales residentes en el extranjero. Aunque utópico, la solución ideal sería construir una legislación que no solo traspase las fronteras nacionales, sino también las de la comunidad europea, para evitar que las organizaciones delictivas disfruten de las oportunidades que garantizan países que no cuentan con una legislación estricta contra el blanqueo de capitales. Por tanto, sería conveniente trabajar en un

tratado internacional que involucre y requiera sobre todo la colaboración de la Oficina de las Naciones Unidas para el Control de las Drogas y la Prevención del Delito, entre las que destaca la lucha contra la delincuencia organizada transnacional. Solo en presencia de la legislación internacional sería posible considerar la criptomoneda como una moneda real en todos los aspectos.

CONCLUSIONES

1.- Dentro de la legislación vigente en nuestro país tenemos a un Código Orgánico Integral Penal, que en primer plano tipifica en su artículo 317 el lavado de activos pero de una manera general establece sus verbos rectores y sus diferentes modalidades, obviando que la ley penal debe ser interpretada en un modo literal, restrictivo y no análogo; por otro lado tenemos a la Ley de Prevención de Lavado de Activos y del Financiamiento de Delitos, ni en su reglamento, que en nada tratan a las criptomonedas, con lo cual se soslaya que no existe la modalidad concreta para la regulación y prevención del delito de lavado de activos que es cometido a través de criptomonedas.

2.- Las criptomonedas en el Ecuador no están prohibidas, pero tampoco están reguladas por un ente de control por lo tanto se facilita para el blanqueador de capitales o sujeto activo del delito de lavado de activos el cometer este injusto en el país por ausencia de norma, debido a que la falta de norma permite que los usuarios introduzcan capital ilícito y también exporten dicho capital a fronteras internacionales desde el Ecuador.

3.- La Policía Nacional y Fiscalía General del Estado, carecen de recurso humano y tecnológico para afrontar las nuevas formas del delito, específicamente del lavado de activos a través de criptomonedas, en el sentido de que no gozan de un equipo tecnológico suficiente para la detección de esta modalidad y tampoco las personas que intervienen en este tipo de investigaciones tienen el conocimiento que se requiere para poder conducir de una forma adecuada la indagación de estos delitos.

RECOMENDACIONES

1.- A la Asamblea Nacional, se tome en cuenta la propuesta contenida en este trabajo investigativo y se reforme el Art. 317 del Código Orgánico Integral Penal, para que en atención a los principios que regulan a la interpretación de la ley penal, se prevea el uso de criptomonedas para la prevención, tipificación y sanción del lavado de activos que es cometida en esta modalidad.

2.- A la Asamblea Nacional y a la Función Ejecutiva, para que en el ejercicio de sus atribuciones y funciones implementen un ente de control de los portales web que operan en el Ecuador como *e-wallets*, y proveedores de criptomonedas; efectuando mecanismos de detección de operaciones financieras inusuales con criptomonedas, y las mismas sean investigadas en la brevedad posible para punir estos actos ilícitos que atentan el orden socioeconómico, reformando el Manual de Ingreso y Salida de Dinero Sujeto a Control de Lavado de Activos, publicado en el Registro Oficial Suplemento 879 de 11 de noviembre de 2016.

3.- A la Policía Nacional y Fiscalía General del Estado, este último como titular de la acción penal pública y en concordancia con los preceptos legalmente establecidos dirija y coordine con Policía Nacional y sus miembros especializados bastas investigaciones con implementos tecnológicos necesarios para su realización, a la vez contar con la capacitación y experticia debida para combatir a la delincuencia organizada, prevenir, sancionar y mitigar el lavado de activos que es cometido con criptomonedas.

REFERENCIAS BIBLIOGRÁFICAS

Agelán, E. (2018). *Ciberdelincuencia y política criminal: internet, nuevo reto jurídico-penal.* Santiago de Chile: Editora Premium.

Almenar, F. (2018). *Ciberdelincuencia: teoría y práctica, colección de derecho penal DIRE.* Brasilia: JURUA EDITORA.

Antonopoulos, A. (2017). *Internet del dinero.* Sevilla: Merkle Bloom LLC.

Arbulú, J. (2018). *Lavado de activos: gestión del riesgo.* Lima: Iustitia S.A.C.

Arzuaga, G. (2018). *Criptomonedas: Las mejores estrategias para invertir en bitcoins, ICO y tokens.* Buenos Aires: Penguin Random House Grupo Editorial Argentina.

Asamblea Nacional. (2014). *Código Orgánico Integral Penal*. Quito: Registro Oficial 180 de 10 de febrero.

Asamblea Nacional. (2016). *Ley de Prevención de Lavado de Activos y del Financiamiento de delitos.* Quito: Registro Oficial Suplemento 802 de 21 de julio.

Bajo, M. (2009). *Política criminal y blanqueo de capitales.* Madrid: Marcial Pons.

Banco Central del Ecuador. (2018). *Estatuto Orgánico de Gestión Organizacional del Banco Central.* Quito: Registro Oficial Suplemento 319 de 21 de marzo.

Barrio, M. (2018). *Ciberdelitos: amenazas criminales del ciberespacio: Adaptado reforma Código Penal 2015*. Madrid: Editorial Reus.

----- Delitos 2.0: aspectos penales, procesales y de seguridad de los ciberdelitos (La Ley. 2018)

Bashir, S. (2019). *Criptomoneda: La guía definitiva para cadena de bloque, minería y más.* Madrid: Babelcube Inc.

Buscaglia, E. (2015). *Lavado de dinero y corrupción política: El arte de la delincuencia organizada internacional.* México DF: Penguin Random House Grupo Editorial México.

Callegari, A. (2003). *El delito de blanqueo de capitales en España y Brasil.* Bogotá: Universidad Externado de Colombia, Centro de Investigación de Filosofía y Derecho.

Cano, M. (2001). *Modalidades de lavado de dinero y técnicas para la prevención.* Bogotá: G&D Impresores.

Corporación Financiera Nacional. (2021). *Procedimiento para la Identificación de Lavado de Activos.* Quito: Registro Oficial Suplemento 387 de 08 de febrero.

Cossey, Ch. (2019). *Criptomoneda: un libro lleno de conocimientos desde principiantes hasta avanzados.* Madrid: Babelcube Inc.

de Escamilla, A. (2019). *Ciberdelitos.* Buenos Aires, Hammurabi.

Del Cid, J. (2007). *Blanqueo internacional de capitales: Cómo detectarlo y prevnirlo.* Bogotá: Grupo Planeta.

Fernández, D. (2019). *Blanqueo de capitales y TIC: marco jurídico nacional y europeo, modus operandi y criptomonedas : ciberlaundry, informe de situación*, Madrid: Thomson Reuters Aranzadi.

Ferro, J. (2020). *Seguridad informática: aspectos generales y especiales. Introducción a la ciberdelincuencia.* Barcelona: Jose Manuel Ferro Editor.

Franco, P. (2014). *Understandig Bitcoin: Cryptography, Engineering and Economics*. Boston: Wiley.

Hernández, H. (2017). *El lavado de activos.* Bogotá: Grupo Editorial Ibáñez.

Intriago, P. (2015). *El rol del fiscal.* Guayaquil: Editorial CBRAZUL.

Jansson, F. (2018). *Criptomonedas: La Guía Fundamental para el Comercio, la Inversión y la Minería de Bitcoins.* Madrid: Babelcube Inc.

Jiménez, F. (2015). *La prevención y la lucha contra el blanqueo de capitales y la corrupción: interacciones evolutivas en un Derecho internacional global.* Málaga: Editor Comares.

Jones, H. (2019). *Criptomonedas: Una Guía Esencial para Principiantes Sobre la Tecnología de Cadenas de Bloques, la Inversión en Criptomonedas, y Bitcoin, Incluyendo Minería, Ethereum y Comercio.* Durham: Publicado por el autor.

Lacarte, M. (2018). *Dinero, Bitcoin, Criptomonedas y la Blockchain: ¿Qué está sucediendo?. Una guía para No tecnólogos.* eBook.

Lanuza. C., & Olóndriz, P., (2019). *El método cripto: ¿Cómo y Por qué invertir en criptomonedas?* Publicado por el autor.

Lombardero, L. (2009). *Blanqueo de capitales: prevención y repression del fenómeno desde la perspectiva penal, mercantil, administrativa y tributaria.* Barcelona: Bosh.

Luna, J. (2020). *Criptomoneda: La guía definitiva para el comercio en criptomonedas (Haga una gran cantidad de dinero con criptomonedas)*. Durham: Editorial Daniel Heath.

Martínez, G., & Fernández, D., (2020). *Ciberdelitos.* Barcelona: Ediciones Experiencia.

Morales, A. (2020). *Congreso Internacional de Derecho Corporativo: Un mundo sin fronteras.* Lima: Fondo editorial Universidad de Lima.

Moreno, I. (2021). *Introducción al blockchain y criptomonedas en 100 preguntas.* Madrid: Ediciones Nowtilus S.L.

Náquira, J. (2018). *Estudios de Derecho Penal Económico.* Santiago de Chile: Ediciones UC.

Nuñez, M. (2008). *El fenómeno de lavado de dinero en México: causas, efectos y propuestas para reforzar su combate.* México DF: Editorial Porrúa.

Ortiz, J. (2013). *Problemas procesales de la ciberdelincuencia.* San José: Editorial Colex.

Palencia, M., & Pierre, M., Nuques, M. (coordinadora) (2016). *Infracciones a deberes ciudadanos de control, con sanción penal de un estado controlador a un estado sancionador una mirada a la luz del delito de lavado de activos en* "Memorias Jurídicas*"*. Guayaquil: AECUPI.

Parra Tabares Erika Brigette (2019), *Las criptomonedas: una nueva modalidad de lavado de activos en Colombia*. Bogotá: Universidad de Nueva Granada.

Peláez, J. (2019). *Manual Práctico para la prevención de Blanqueo de Capitales*. Madrid: CIss S.A.

Pérez, I. (2014). *El dilema de las operaciones grises: Modus operandi de la delincuencia económica para lavar el dinero sucio.* Buenos Aires: Editorial Dunken.

Pinco Espinal, Fiorela, y Rodríguez Lizana Rafael (2021). *El delito de lavado de activos y la utilización o uso de criptomonedas*. Huancayo: Universidad Continental.

Posada, R. (2017). Los cibercrímenes: Un nuevo paradigma de criminalidad.: Un estudio del título VII bis del Código Penal colombiano. Bogotá: Ediciones Uniandes – Universidad de los Andes.

Presidencia de la República del Ecuador. (2017). *Reglamento a la Ley de Lavado de Activos y del Financiamiento de Delitos.* Quito: Registro Oficial Suplemento 966 de 20 de marzo.

Preukschat, A. (2017). *Blockchain: la revolución industrial de internet.* Bogotá: Grupo Planeta.

Ramsey, T. (2019). *Dinero: criptomonedas: secretos de expertos para el comercio, gestión de inversiones y minería.* Montefranco: Tektime.

Raskovsky, R., & Linares, M. (2019). *Derecho al Día: Criptomonedas y lavado de activos, julio de 2019, todo disponible en* *http://www.derecho.uba.ar/derechoaldia/notas/criptomonedas-y-lavado-de-activos/+7603*

Reyes, Y. (2021). *Las criptomonedas, el nuevo oro digital: una pequeña guía que te ahyudará a comenzar a invertir y a ganar.* Amazon Digital Services LLC - KDP Print US

Rigters, G. (2021). *Bitcoin para principiantes: criptomonedas y blockchain*. Barcelona: Giovanni Rigters.

Robinhood, A. (2021). *¿Invertir en CRIPTOMONEDAS? Finanzas, Dinero Electrónico y Revolución: Compra Bitcoin (BTC), Binance (BNB), Cardano (ADA) y Otras Monedas Digitales para Conseguir Ingresos Pasivos.* Madrid: C.Y.C. Ediciones.

Satoshi, A. (2019). *Criptomoneda: Aprendizaje sistemático acerca de invertir y comerciar en Criptomoneda.* Madrid: Babelcube Inc.

Seaone, A. (2015). *Manual práctico para la prevención de Blanqueo de Capitales.* Navarra: Editorial Aranzadi, S.A.

Servicio Nacional de Aduana del Ecuador. (2016). *Manual de Ingreso y Salida de Dinero Sujeto a Control de Lavado de Activos.* Quito: Registro Oficial Suplemento 879 de 11 de noviembre.

Silva, J., & Montaner, R. (2013). *Criminalidad de empresa y Compliance: Prevención y reacciones corporativas.* Barcelona: Atelier.

Smith, J. (2018). *Criptomonedas: criptomonedas para principiantes (blokchain y bitcoin).* Montefranco: Tektime.

----- Criptomoneda: Una guía simple para dominar la criptomoneda. Montefranco: Tektime.

Superintendencias de Compañías. (2021). *Normas de Prevención de Lavado de Activos, Financiamiento del Terrorismo.* Quito: Registro Oficial Suplemento 411 de 16 de marzo.

Sztandarowski, L. (2019). *La verdadera cibercriminalidad: Manual jurídico del cibercrímen, ensayo de cibercriminología.* París: Cyberdéfenseur.

Terradillos, J. (2011). *Blanqueo de capitales. Lecciones y materiales para el estudio del derecho penal.* Madrid: CIss, SA.

Tondini. B. (2009). *Blanqueo de capitales y lavado de dinero: su concepto, historia y aspectos operativos.* Buenos Aires: Centro Argentino de Estudios Internacionales.

Torres, J. (2019). *Criptomonedas: Qué son, como utilizarlas y por qué van a cambiar el mundo*. Bogotá: Grupo Planeta.

Úbeda, J. (2009). *Terrorismo, narcotráfico, blanqueo de capitales, trata de personas, tráfico ilícito de migrantes, tráfico ilícito de armas:: Lucha global contra la delincuencia organizada transnacional*. Madrid: Liber Factory.

Walker, W. (2018). *El Siguiente Nivel De Inversión En Criptomonedas: Estrategias Avanzadas Para Ganar Dinero Con Bitcoin y Otras Criptomonedas*. Chicago: Wayne Walker Inc.

White, V. (2019). *Criptomoneda: comercio e inversión en bitcoin litecoin y otras más.* Madrid: Bablecube.

Wright, C. (2020). *La visión de Satoshi: El arte de Bitcoin.* Boston: Publicación por autor.

VALIDACIÓN PARA EL DESARROLLO DE LA PROPUESTA:

FICHA TÉCNICA DEL VALIDADOR

Nombre: Kevin Cabezas Páez

Cédula N°: 0603565961

Profesión: Abogado – Especialista en derecho procesal, derecho penal; y Magister en Derecho Penal.

Dirección: Riobamba - Chimborazo

ESCALA DE VALORACION ASPECTOS	MUY ADECUADA 5	ADECUADA 4	MEDIANAMENTE ADECUADA 3	POCO ADECUADA 2	NADA ADECUADA 1
Introducción	x				
Objetivos	x				
Pertenecia	x				
Secuencia	x				
Premisa	x				
Profundidad	x				
Coherencia	x				
Comprensión	x				
Creatividad	x				
Beneficiarios	x				
Consistencia lógica	x				
Cánones doctrinales jerarquizados	x				
Objetividad	x				
Universalidad	x				
Moralidad social	x				

Fuente (Obando, 2015)

Comentario:

Es un tema innovador carente de regulación legislativa en el Ecuador, motivo por el cual se debería implementar.

Fecha: 10 de octubre de 2022

Firma:

KEVIN JOEL CABEZAS PAEZ

Firmado digitalmente por KEVIN JOEL CABEZAS PAEZ
Fecha: 2022.10.10 18:34:04 -05'00'

Ab. Esp. Mgs. Kevin Cabezas Páez
0603565961

DECLARACIÓN Y AUTORIZACIÓN

Yo, Jaime Germán Silva Colcha , con C.C: 0604455998 autor del trabajo de titulación: LA AUSENCIA DE NORMATIVA PENAL PARA REPRIMIR EL LAVADO DE ACTIVOS A TRAVÉS DE CRIPTOMONEDAS, previo a la obtención del grado de **MAGÍSTER EN DERECHO MENCIÓN DERECHO PROCESAL** en la Universidad Católica de Santiago de Guayaquil.

1.- Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de graduación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2.- Autorizo a la SENESCYT a tener una copia del referido trabajo de graduación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de propiedad intelectual vigentes.

Guayaquil, 03 de enero de 2023

f. _____

Jaime Germán Silva Colcha

C.C: 0604455998

REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA			
FICHA DE REGISTRO DE TESIS/TRABAJO DE GRADUACIÓN			
TÍTULO Y SUBTÍTULO:	LA AUSENCIA DE NORMATIVA PENAL PARA REPRIMIR EL LAVADO DE ACTIVOS A TRAVÉS DE CRIPTOMONEDAS		
AUTOR(ES) (apellidos/nombres):	Silva Colcha Jaime Germán		
REVISOR(ES)/TUTOR(ES) (apellidos/nombres):	Vivar Álvarez Juan Carlos		
INSTITUCIÓN:	Universidad Católica de Santiago de Guayaquil		
UNIDAD/FACULTAD:	Sistema de Posgrado		
MAESTRÍA/ESPECIALIDAD:	Maestría en Derecho Mención Derecho Procesal		
GRADO OBTENIDO:	Magíster en Derecho Mención Derecho Procesal		
FECHA DE PUBLICACIÓN:	03 de enero de 2023	**No. DE PÁGINAS:**	98
ÁREAS TEMÁTICAS:	Derecho Penal, Lavado de Activos		
PALABRAS CLAVES/ KEYWORDS:	Lavado de activos, criptomonedas, ausencia de normativa, contratos criminales inteligentes		
RESUMEN/ABSTRACT Dentro del presente trabajo investigativo se aborda un tema de total relevancia jurídica como la ausencia de norma en el Ecuador para reprimir el lavado de activos que es cometido a través de criptomonedas, en un primer momento se estudia al lavado de activos o también conocido como blanqueo de capitales, se examinan las particularidades de las criptomonedas y su utilización a través de herramientas informáticas para darle la apariencia de un dinero legítimo y reinsertarlo al orden socioeconómico tanto nacional como extranjero. Se aplicó una metodología mixta tanto cualitativa como cuantitativa porque desde su complementación una a otra mejora el entendimiento del problema, optimando la creatividad y permite llegar a una mejor conclusión dentro del problema de investigación. Con las conclusiones a las que se han arribado se recomienda una reforma del Código Orgánico Integral Penal, en el sentido de tipificar la conducta de las criptomonedas en el delito de lavado de activos, debido a su facilidad de uso para delinquir, y a la vez capacitar y dotar de equipos tecnológicos a quienes realizan investigación de los delitos de acción pública como Fiscalía General del Estado y Policía Nacional.			
ADJUNTO PDF:	☒ Si	☐ NO	
CONTACTO CON AUTOR/ES:	**Teléfono:** 0982201647	E-mail: jaimesilvacolcha@gmail.com	
CONTACTO CON LA INSTITUCIÓN:	**Nombre:** Andrés Obando Ochoa		
	Teléfono: +593-992854967		
	E-mail: ing.obandoo@hotmail.com		
SECCIÓN PARA USO DE BIBLIOTECA			
Nº. DE REGISTRO (en base a datos):			
Nº. DE CLASIFICACIÓN:			
DIRECCIÓN URL (tesis en la web):			