UNIVERSIDAD LAICA VICENTE ROCAFUERTE DE GUAYAQUIL

FACULTAD DE ADMINISTRACION

CARRERA DE CONTABILIDAD Y AUDITORIA

MODALIDAD COMPLEXIVO PREVIO A LA OBTENCIÓN DEL TÍTULO
DE

LICENCIATURA DE CONTABILIDAD Y AUDITORIA

CASO DE ESTUDIO

IDENTIFICAR LA CRIPTOMONEDA Y SU RELACION CON EL LAVADO DE ACTIVOS EN EL ECUADOR PERIODO 2022

AUTORES

JOCELYN GALARZA MARTINEZ

GUAYAQUIL

2023

CERTIFICADO DE SIMILITUD

IDENTIFICAR LA CRIPTOMONEDA Y SU RELACION CON EL LAVADO DE ACTIVOS EN EL ECUADOR PERIODO 2022

INFORME DE ORIGINALIDAD

7%	7%	1%	3%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	repositorio.usfq.edu.ec Fuente de Internet	4%
2	Submitted to Universidad Internacional SEK Trabajo del estudiante	2%
3	humanrightscommission.house.gov Fuente de Internet	1%

Excluir citas	Activo	Excluir coincidencias	< 1%
Excluir bibliografía	Activo		

PAMELA ROXANA LOPEZ PINCAY

ÍNDICE

ÍNDICE GENERAL

I. INTRODUCCIÓN

Antecedentes:

En los últimos años, el crecimiento y la adopción de las criptomonedas han generado tanto entusiasmo como preocupación en todo el mundo. A medida que estas formas de dinero digital se vuelven más populares, también ha surgido la necesidad de examinar su relación con el lavado de activos, un delito financiero que busca ocultar el origen ilícito de los fondos.

En el contexto específico de Ecuador, un país que ha experimentado un aumento en la adopción de criptomonedas y una creciente conciencia sobre el lavado de activos, resulta relevante analizar y comprender la relación entre una criptomoneda específica y este delito.

La presente investigación tiene como objetivo identificar la criptomoneda y su relación con el lavado de activos en Ecuador durante el período de estudio. Se examinarán los antecedentes, los casos relevantes y las tendencias observadas en el uso de la criptomoneda en actividades ilícitas en el país. Además, se analizarán las medidas y regulaciones vigentes en Ecuador para prevenir y detectar el lavado de activos relacionado con criptomonedas.

Esta investigación se llevará a cabo mediante la revisión de fuentes primarias y secundarias, como leyes y regulaciones, informes gubernamentales, investigaciones académicas y noticias actualizadas. Se utilizarán herramientas de análisis para recopilar y examinar la información relevante que permita comprender la dinámica entre la criptomoneda seleccionada y el lavado de activos en Ecuador.

Los resultados de esta investigación proporcionarán una visión más clara de la relación entre criptomonedas y lavado de activos en el contexto ecuatoriano, lo que puede contribuir al fortalecimiento de las medidas y regulaciones existentes para combatir este delito. Además, permitirá a los actores gubernamentales,

reguladores y académicos tener una base sólida para tomar decisiones informadas y desarrollar estrategias efectivas para abordar este desafío en constante evolución.

Objetivo General:

• Identificar la criptomoneda específica y analizar su relación con el lavado de activos en Ecuador durante el 2022.

Objetivos específicos:

• Realizar una revisión de las criptomonedas utilizadas en Ecuador y seleccionar la criptomoneda específica que se analizará en relación con el lavado de activos.

• Investigar y recopilar datos sobre la adopción y el uso de la criptomoneda seleccionada en el contexto ecuatoriano, incluyendo la cantidad de transacciones, los usuarios y los casos relevantes.

• Examinar casos y eventos en los cuales se haya utilizado la criptomoneda seleccionada para realizar actividades de lavado de activos en el país.

Preguntas de la Investigación Científica:

1. ¿Cuáles son las criptomonedas más utilizadas en Ecuador?

2. ¿Cuál es el nivel de adopción y uso de la criptomoneda seleccionada en Ecuador, incluyendo la cantidad de transacciones realizadas, el número de usuarios involucrados y los casos relevantes relacionados con su uso?

3. ¿Cuáles son los casos y eventos identificados en Ecuador en los cuales se ha utilizado la criptomoneda seleccionada para realizar acciones de lavado

de activos, cuáles son las características y estrategias utilizadas en dichos casos?

Concepto de criptomonedas:

Las criptomonedas son formas de dinero digital emplean técnicas criptográficas para asegurar operaciones y supervisar la generación de nuevos elementos. Estas divisas digitales operan con la tecnología blockchain, un registro abierto y distribuido de todas las actividades efectuadas con la criptomoneda.

Una característica fundamental de las criptomonedas es su descentralización, lo que significa que no están controladas por ninguna entidad centralizada, como un banco central o una autoridad financiera. En cambio, las transacciones y el mantenimiento de la red son gestionados por una red de nodos distribuidos en todo el mundo.

Cada criptomoneda tiene su propia infraestructura y conjunto de reglas. Las transacciones de criptomonedas se registran en bloques que se agregan mediante la cadena de bloques (blockchain), se asegura la confiabilidad y salvaguarda de las operaciones.

Además, las criptomonedas permiten la transferencia de valor de forma rápida y directa entre dos partes, sin intermediarios financieros tradicionales. Esto significa que las transacciones pueden realizarse de forma más eficiente y con costos potencialmente más bajos.

Si bien Bitcoin es la criptomoneda más conocida y utilizada, existen miles de criptomonedas diferentes, cada una con sus propias características y aplicaciones. Algunas criptomonedas se utilizan como medios de pago, mientras que otras se centran en casos de uso específicos, como contratos inteligentes o soluciones de privacidad.

Es importante tener en cuenta que el valor de las criptomonedas puede ser volátil y está sujeto a fluctuaciones del mercado. Además, su uso plantea desafíos regulatorios y de seguridad, y puede estar asociado con actividades ilícitas, como el lavado de activos. Por lo tanto, los gobiernos y las autoridades financieras de diferentes países han implementado regulaciones y medidas para abordar el uso de criptomonedas y garantizar su uso legítimo y seguro.

Algunos expertos argumentan que el término "anonimato" no es totalmente adecuado en relación a ciertas criptomonedas, ya que creen que son más bien seudónimas debido a la información asociada con las partes involucradas en las transacciones (como direcciones o claves públicas).

Julian Assange, en colaboración con Jacob Appelbaum, Andy MullerMaguhn y Jeremie Zimmermann. "Cypherpunk: Perspectivas sobre la Libertad Digital y el Porvenir de la Web". Barcelona: Ediciones Deusto, (2012). página 15.

El origen de las criptomonedas se remonta al movimiento cypherpunk de los primeros años noventa. Según Julian Assange, uno de los líderes destacados de esta corriente, un cypherpunk es "un defensor que emplea el uso de la criptografía como forma pacífica de resistencia con el objetivo de lograr transformaciones políticas y sociales".

“Moneda Geek: Bitcoin, la divisa digital privada y argumentos en contra de su regulación”. Revista de Derecho del Consumidor de Loyola, Vol.25. (2012). págs. 12-45.

En sus inicios, los cypherpunks eran activistas especializados en criptografía, computación y programación, alarmados ante el potencial uso del internet por parte del gobierno para reprimir y violar la privacidad y libertad individual. Un subgrupo de estos activistas, pertenecientes a la lista de correo de criptografía, debatían continuamente sobre cómo una moneda digital podría ser anónima o cómo se podría anonimizar a través de la criptografía.

De acuerdo con Lara y Muñoz, la descentralización del sistema Bitcoin se logra de la siguiente forma: Funciona con una base de datos distribuida, denominada registro distribuido o Blockchain. Esta actúa a modo de un registro ledger no centralizado que anota todas las transacciones de la red. Cada nodo de la red posee una copia completa del Blockchain, lo que le otorga una de sus propiedades fundamentales: la ausencia de una institución o banco central que supervise el sistema. En su lugar, todo es gestionado por un conjunto de computadoras distribuidas.

Tecnología blockchain y su aplicabilidad en las criptomonedas:

La tecnología blockchain es la base fundamental de las criptomonedas y desempeña un papel clave en su funcionamiento. La aplicabilidad de la tecnología blockchain en las criptomonedas se puede describir en los siguientes aspectos:

Registro descentralizado: El blockchain es un registro público y descentralizado que almacena todas las transacciones realizadas con una criptomoneda específica. Esta característica descentralizada significa que no hay una entidad central que controle o posea el registro, sino que está distribuido en múltiples nodos de la red. Esto brinda transparencia y seguridad a las transacciones, ya que todos los participantes de la red tienen acceso al historial de transacciones.

Seguridad mediante criptografía: La tecnología blockchain utiliza algoritmos criptográficos para proteger la integridad y seguridad de las transacciones. Cada transacción se registra en un bloque y se enlaza de forma secuencial con los bloques anteriores mediante una función criptográfica. Esto hace que sea casi imposible modificar o falsificar una transacción sin ser detectado, ya que cualquier alteración en un bloque afectaría a todos los bloques siguientes.

Consenso descentralizado: La tecnología blockchain utiliza mecanismos de consenso descentralizado para validar y agregar nuevas transacciones a la

cadena de bloques. En el caso de las criptomonedas más conocidas, como Bitcoin y Ethereum, se utiliza el algoritmo de Prueba de Trabajo (Proof of Work) o, en algunos casos, algoritmos de consenso alternativos como Prueba de Participación (Proof of Stake). Estos mecanismos aseguran que las transacciones sean validadas por la red y evitan la posibilidad de duplicación o falsificación.

Anonimato y pseudonimato: Aunque no todas las criptomonedas garantizan el anonimato completo, muchas de ellas permiten un nivel de pseudonimato en las transacciones. Esto significa que las identidades de las partes involucradas en una transacción no están directamente vinculadas a información personal, sino a direcciones de criptomonedas. Si bien estas direcciones pueden ser rastreadas y analizadas, el anonimato puede ser más difícil de alcanzar en comparación con los sistemas financieros tradicionales.

La aplicabilidad de la tecnología blockchain en las criptomonedas proporciona una forma segura y eficiente de realizar transacciones digitales sin depender de intermediarios centralizados. Sin embargo, es importante tener en cuenta que la tecnología blockchain también tiene otras aplicaciones más allá de las criptomonedas, como contratos inteligentes, registros de propiedad, trazabilidad de productos, votación electrónica, entre otros, que están siendo exploradas y desarrolladas en diversos campos.

Basándose en las observaciones de Acevedo y Rodríguez, existen tres tipos de blockchain:

1. Blockchain Público: En esta malla totalmente distribuida, cualquier individuo tiene la capacidad de ingresar transacciones, formar bloques y estar involucrado en su validación. Su seguridad y confiabilidad provienen de la actividad minera. Este modelo es fundamental para muchas de las criptomonedas existentes. **2. Blockchain de Consorcio:** Este tipo tiene un mecanismo de validación distinto. Aquí, solo ciertos nodos, que han sido previamente seleccionados, tienen la autoridad para validar las operaciones. Es percibido como un sistema de descentralización intermedia. **3. Blockchain**

Privado: Aquí, el registro de datos es controlado por una única entidad o corporación. El acceso a dichos datos puede ser abierto al público o restringido, según lo determine la entidad administradora. (lo resaltado me pertenece)

Estas billeteras electrónicas poseen un par de llaves: una pública y otra privada, conocidas como "llaves". La clave pública funciona similar a una dirección de email, que el usuario comparte con otros miembros de Bitcoin para obtener bitcoins. Por otro lado, la clave privada es comparable al código secreto de una tarjeta bancaria, utilizado para validar que el usuario tiene la intención de utilizar los bitcoins almacenados en su billetera. Alejandro López, 2015. "El Bitcoin en Colombia: Consecuencias Legales y Validez del Acuerdo de Compra-venta Utilizando Bitcoins.

Conforme a Lara y Muñoz, "la privacidad puede ser vital en diversas áreas, en particular en aspectos profundamente personales como la sexualidad, las creencias o la salud.

Por otro lado, numerosos especialistas indican que, aunque Bitcoin pueda ser inmune a la inflación, no está exento de sufrir un proceso de deflación. Esto se debe a razones como la existencia de un límite predefinido considerando el volumen total de bitcoins disponibles y la inclinación de numerosos usuarios a conservar sus bitcoins especulando con su valor, y la disminución gradual en la tasa de emisión de nuevos bitcoins durante el minado. Bit2Me. "El Bitcoin y su inclinación hacia la deflación". Visitado en: https://academy.bit2me.com/deflacion-en-bitcoin/ el 26 de enero de 2019.

En realidad, las criptomonedas ganaron notoriedad mundial cuando, en 2011, investigadores del FBI detectaron que la plataforma virtual clandestina, Silk Road, realizaba todas sus operaciones usando Bitcoin, debido a la necesidad de que estas transacciones fueran descentralizadas y confidenciales. Andrew Greenberg. (2019). "El renacimiento del mercado negro: Silk Road 2.0 en la web oscura". Consultado en:

https://www.forbes.com/sites/andygreenberg/2013/11/06/silk-road-2-0launches-promising-a-resurrectedblack-market-for-the-darkweb/#6f9bb4535714.

Antes del surgimiento de las criptomonedas, otras monedas digitales ya habían sido utilizadas en actividades ilegales. En realidad, el incidente más significativo documentado de blanqueo de capitales a través de medios digitales involucró a una moneda digital, conocida como “LR” de la empresa Liberty Reserve, como herramienta para perpetrar el delito. Brill, Allan y Keene, Lonnie. (2014). "¿Criptomonedas: El Futuro Financiamiento del Terrorismo?". Defence Against Terrorism Law Review. Vol 6. No. 1, Spring & Fall, pp. 7- 30.

Liberty Reserve, con base en Costa Rica, era "una empresa dedicada al procesamiento de pagos y a las transferencias de moneda". Esta compañía fue imputada por lavar aproximadamente 6 mil millones de dólares estadounidenses mediante 55 millones de operaciones en línea. Marc Santora, William K. Rashbaum, y Nicole Perlroth. Online Currency Exchange Accused of Laundering $6 Billion. https://www.nytimes.com/2013/05/29/nyregion/libertyreserve-operators-accusedof-money-laundering.html (acceso: 27/1/2019).

Con base en lo indicado por Brill y Keene, el funcionamiento de Liberty Reserve era así: Para abrir una cuenta en Liberty Reserve y convertir las monedas LR, bastaba con que los usuarios proporcionaran una dirección de correo, incluso si esta era confidencial. A diferencia de las instituciones bancarias o financieras tradicionales, Liberty Reserve no requería verificación de identidad. Por un cargo extra de 75 centavos por transacción, llamado "cuota de confidencialidad", la firma ocultaba el número de cuenta de los usuarios en las operaciones, logrando así imposible su seguimiento. Para hacer depósitos o retiros, los usuarios se valían de Exchangers (intermediarios o entidades de cambio), lo que facilitaba a Liberty Reserve evitar la recopilación de información sobre sus clientes mediante operaciones bancarias u otras acciones que generaran un registro financiero central. Estos Exchangers transformaban las

LR en monedas convencionales y las transferían a cuentas bancarias de los beneficiarios. Estos intermediarios solían ser empresas de transferencia monetaria no autorizadas, operando sin un control o regulación gubernamental riguroso, y estaban predominantemente en lugares como Malasia, Rusia, Nigeria y Vietnam.

Lavado de activos: definición y etapas del proceso:

El lavado de activos, también conocido como blanqueo de capitales, es un proceso mediante el cual se busca disfrazar o validar la procedencia ilegal de los recursos o propiedades adquiridos a través de actividades criminales.
Consiste en convertir los activos generados por actividades delictivas en apariencia de fondos legítimos, de manera que puedan ser utilizados sin levantar sospechas y se les dé una apariencia de legalidad.

El proceso de lavado de activos generalmente se divide en tres etapas principales:

Etapa de colocación (placement): En esta etapa, el objetivo principal es introducir los fondos ilícitos en el sistema financiero de forma que parezcan legítimos. Esto implica convertir el dinero en efectivo o activos físicos, como bienes raíces o joyas, en activos financieros o cuentas bancarias. Se busca dispersar los fondos en múltiples transacciones pequeñas para evitar levantar sospechas y dificultar su rastreo.

Etapa de estratificación (layering): Una vez que los fondos ilícitos se encuentran en el sistema financiero, se realiza una serie de transacciones complejas y sofisticadas para dificultar aún más su rastreo. En esta etapa, se llevan a cabo transferencias de fondos entre diferentes cuentas bancarias, se realizan inversiones en activos financieros, se crean empresas ficticias o se utilizan intermediarios para enmascarar la verdadera fuente de los fondos. El objetivo es generar múltiples capas de transacciones y entidades para ocultar la pista del dinero.

Etapa de integración (integration): En esta última etapa, los fondos ilícitos se reintroducen en la economía legal como activos legítimos. Los activos se utilizan para adquirir bienes y servicios, como propiedades, vehículos de lujo o inversiones comerciales. Con el tiempo, los activos adquiridos ilegalmente se mezclan con activos legales, lo que dificulta aún más la identificación y recuperación de los fondos de origen ilícito.

Es importante es importante subrayar que el blanqueo de capitales es un crimen complicado que implica la participación de diferentes actores y métodos. Los perpetradores buscan aprovechar las debilidades del sistema financiero y utilizar técnicas sofisticadas para ocultar la verdadera naturaleza y origen de los fondos ilícitos. Los esfuerzos para prevenir y combatir el lavado de activos implican la implementación de regulaciones y controles financieros, así como la cooperación entre las autoridades nacionales e internacionales.

La compañía Chainalysis, especializada en servicios de cumplimiento relacionados con criptoactivos, presentó un informe sobre la actividad delictiva asociada a las criptomonedas. Según este estudio, los dos crímenes más recurrentemente vinculados a las criptomonedas son el blanqueo de capitales y el fraude. Debido a esto, se ha decidido enfocar esta tesis en estos dos delitos en particular. Chainalysis. (20.19). "Informe sobre Delitos Cripto: Descifrando hackeos avanzados, mercados oscuros y estafas". págs. 3-29.

En 1951, Edwin Sutherland, un criminólogo de Estados Unidos, lanzó su libro "White Collar Crime", marcando el inicio de una nueva área de análisis en la criminología y jurisprudencia al acuñar el concepto de delito de cuello blanco. La representación que Sutherland propuso acerca del delincuente de este tipo distaba mucho de los rasgos tradicionalmente asociados a los criminales. Se tenía la noción de que los delitos eran cometidos principalmente por individuos de niveles socioeconómicos bajos, y aquellos crímenes cometidos por personas de la élite eran vistos como excepciones a esta norma general, que vinculaba el crimen violento especialmente a las clases más desfavorecidas.

Sin embargo, Sutherland reveló que los delincuentes de cuello blanco provienen de niveles socioeconómicos elevados y poseen una notable posición y acceso al poder.

Sutherland**,** en su obra, destaca una distinción crucial entre el crimen de cuello blanco y el crimen de guante blanco, expresiones que frecuentemente se mezclan pero que simbolizan ideas diferentes. La distinción establecida por Sutherland indica que: El crimen de cuello blanco no debe confundirse con el delito de guante blanco, pese a su similitud terminológica. El primero se centra en el poder que el perpetrador posee en relación al acto delictivo, mientras que el segundo se refiere a la meticulosidad con la que se lleva a cabo el delito. El delito de guante blanco es ejecutado con perfección, como un robo hábil, un engaño maestro a un casino o un asesinato limpio y sin violencia física. De esta manera, el crimen de guante blanco se caracteriza por la exactitud y maestría al cometer el hecho ilegal, y generalmente se relaciona con la pericia profesional del autor. Mientras tanto, el crimen de cuello blanco se asocia a un estatus destacado en la sociedad, tal como el de un empresario, médico, jurista, político, comunicador o cualquier otra figura con acceso y poder significativo.

Si bien fue Sutherland quien introdujo el concepto de crimen de cuello blanco, su investigación se enfocó principalmente en grandes corporaciones multinacionales. Así, la definición original que propuso abarcaba solo cuatro tipos de conductas: prácticas contrarias al libre comercio, publicidad engañosa, violaciones a normas de patentes y otros derechos de propiedad industrial, y desacato a las leyes laborales. Con el paso del tiempo, la concepción de crimen de cuello blanco se ha transformado para abarcar un espectro más diverso de delitos. Estudios actuales sobre el asunto incorporan categorías tales como: acciones anticompetitivas, quiebra engañosa, infracciones a la propiedad intelectual, revelación no autorizada de secretos corporativos, espionaje en la industria, delitos cibernéticos, delitos contra el bienestar del consumidor, infracciones medioambientales, evasión de impuestos, lavado de dinero, crimen estructurado y su financiamiento, falsificaciones, fraudes, engaños,

delitos contra el cuerpo administrativo (tales como apropiación indebida, desvío de recursos y tráfico de favores), falso testimonio y obstrucción judicial.

Según el Dr. Nava Garcés, los delitos informáticos se definen así: De manera general, un delito informático se refiere a cualquier acción delictiva que emplea la tecnología electrónica, ya sea como herramienta, medio o propósito. En un sentido más específico, son aquellos actos que se consideran ilícitos y reprobables en los cuales las computadoras, junto con sus métodos y roles, son fundamentales, actuando como instrumento, canal o fin del acto delictivo.

La Unión Internacional de Telecomunicaciones (UIT), en su Manual de Ciberseguridad para Naciones en Desarrollo, ofrece una de las definiciones más completas sobre delitos informáticos: Se entiende por delito informático aquel acto ilícito cuyo objetivo o instrumento es un sistema informático, vinculado a tecnologías digitales y que se enmarca dentro e la criminalidad de cuello blanco. Mientras tanto, el ciberdelito es una forma del crimen informático que se vale de las tecnologías en línea para llevarse a cabo, abarcando todos los actos delictivos cometidos en el ciberespacio.

En relación a esto, Pérez López expone la conexión entre los malos usos de las criptomonedas y las particularidades comunes de la ciberdelincuencia: Debido a que las criptomonedas son puramente electrónicas, coinciden perfectamente con las características predominantes de la ciberdelincuencia: agilidad en las operaciones; distanciamiento entre el infractor y el sitio de ocurrencia gran parte del proceso delictivo; naturaleza transnacional, con los retos legales que implica determinar la jurisdicción adecuada y la necesaria cooperación internacional para abordar el delito; y su naturaleza intangible, que facilita la destrucción de evidencia.

Un aspecto crucial de los ciberdelitos es su carácter transnacional y multinacional. A menudo, acciones delictivas asociadas a ciberdelitos se originan en un país, pero su desarrollo y consecuencias afectan a múltiples naciones en distintos continentes. Por esta razón, la mayoría de los países

busca formalizar acuerdos y pactos de colaboración jurídica con otras naciones para crear redes y mecanismos eficaces para prevenir, investigar y sancionar ciberdelitos. Un ejemplo prominente de estos acuerdos es el Acuerdo de Budapest de 2001 relacionado con la ciberdelincuencia, al que Ecuador no se ha sumado Convenio Sobre la Ciberdelincuencia (2001).

Es relevante hacer una distinción esencial: las acciones ilícitas llevadas a cabo por cibercriminales mediante criptomonedas no se alinearían con el delito de estafa según la legislación de Ecuador. El ilícito adecuado para tratar estos comportamientos sería el de "usurpación fraudulenta a través de medios electrónicos", definido en el artículo 190 del COIP. Dicho artículo se formula de la siguiente forma: Código Orgánico Integral Penal. Art. 186. Publicado en el Registro Oficial Suplemento 180. (2014). Art. 190.- Apropiación fraudulenta por medios electrónicos: La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años. La misma sanción se impondrá si la infracción se comete con inutilización de sistemas de alarma o guarda, descubrimiento o descifrado de claves secretas o encriptadas, utilización de tarjetas magnéticas o perforadas, utilización de controles o instrumentos de apertura a distancia, o violación de seguridades electrónicas, informáticas u otras semejantes.

A pesar de ello, en muchas legislaciones internacionales, la usurpación engañosa a través de medios electrónicos se considera una variante de fraude. Esta percepción es ampliamente aceptada a nivel global. Albán Gómez articula esta idea diciendo: La formulación del delito de apropiación fraudulenta, según el Art. 190, tiene una complejidad destacada y quizás innecesaria. Si, en su

núcleo, el delito implica la apropiación de bienes usando medios electrónicos de forma engañosa, se podría argumentar que estamos ante una variante de la estafa. Por ello, una redacción más simplificada podría ser adecuada siguiendo el Art. 284 del Código español: “Aquellos que, con intención de obtener beneficio y mediante una manipulación tecnológica o truco similar, logren una transferencia no autorizada de un bien patrimonial en detrimento de alguien más”. Ernesto Albán Gómez. Guía de Derecho Penal Ecuatoriano. (2018). Sección Especial. Volumen I. Publicaciones Jurídicas: Quito, pág. 204.

Código Orgánico Integral Penal. Art. 186. Difundido en el Registro Oficial Suplemento 180. (2014). El delito de estafa está definido conforme al artículo 186 del Código Orgánico Integral Penal (COIP) se expresa así: Art. 186.- Engaño. - Aquel que, con el propósito de lograr un beneficio económico para sí o para otro, por medio de la representación de situaciones falsas o la tergiversación u ocultación de la realidad, confunda a alguien para que ejecute una acción que dañe su economía o la de un tercero, enfrentará una pena de cinco a siete años de privación de libertad.

Esto queda reflejado en la sentencia dictada por la Corte Nacional de Justicia en 2013, que establece lo siguiente:

Corte Nacional de Justicia. Sala Primera Penal. Caso No. 014-2010. Registro Oficial Suplemento. (2013). El delito de estafa, definido en el artículo 563 del Código Penal, posee una estructura intrincada. Por ello, cuando se argumenta su presencia, es vital evidenciar su conformidad con el tipo penal. El elemento de estafa es crucial para esta tipificación. Además, es esencial determinar el daño, refiriéndose al impacto al derecho protegido, que es la propiedad en un marco amplio. El corazón de esta conducta es conseguir que se entreguen activos ajenos con la intención de adueñarse de ellos.

Desde una perspectiva doctrinal, Albán Gómez identifica los elementos centrales de este delito como: la inducción al error (esencia), el ánimo de lucro (intención de lograr una ganancia material para uno mismo o para otra persona) y el engaño (representación de situaciones ficticias o distorsión u ocultación de

eventos verdaderos). Ernesto Albán Gómez. Guía de Derecho Penal Ecuatoriano. (2018).

Es importante mencionar que tanto la Estafa como la apropiación fraudulenta por medios electrónicos están contemplados en la sección novena del COIP, dedicada a los Crímenes contra el derecho a la propiedad. Estas infracciones, tal y como indica su denominación, perjudican el derecho a la propiedad individual. Es esencial establecer una distinción entre el derecho de propiedad tal y como se define en el Código Civil. y cómo se define en el COIP para prevenir malentendidos. Albán Gómez distingue estas dos interpretaciones del derecho de propiedad del siguiente modo: Aunque en el Código Civil (Art. 599) la palabra "propiedad" se usa quivalente al derecho real de posesión (aludiendo al goce y gestión de un bien concreto), hay quienes defienden que la salvaguardia penal excede esta interpretación. Argumentan que determinadas infracciones icónicas, como el hurto y el robo, no perjudican directamente la posesión, dado que esta no se desvanece con tales acciones. En estos casos, lo que directamente se ve afectado es la posesión o simplemente la tenencia del bien, y en otros escenarios, otros derechos reales pueden verse comprometidos. Sin embargo, es crucial comprender que el Derecho Penal no siempre emplea terminología de la misma forma que otras disciplinas jurídicas, como es el caso del Derecho Civil. Por lo tanto, en esta situación, "propiedad" debe ser comprendido en un contexto más extenso, acorde a lo que la Constitución estipula (Arts. 66.26 y Arts. 321 y siguientes) en relación a la actividad económica de la comunidad. Este derecho comprende bienes materiales como intangibles, incluyendo los derechos reales sobre bienes corporales e incorporales mencionados en el Código Civil. Artículo 186 del Código Orgánico Integral Penal. Difundido en el Suplemento 180 del Registro Oficial. (2014).

II. ANÁLISIS

Identificar la criptomoneda y su relación con el lavado de activos en el ecuador periodo 2022

Basados en nuestra investigación y sabiendo la expansión de las criptomonedas en el Ecuador en el año 2022, nos vamos a enfocar en la más popular que es el BITCOIN y la cual se tiene registros históricos en la relación con el lavado de activos.

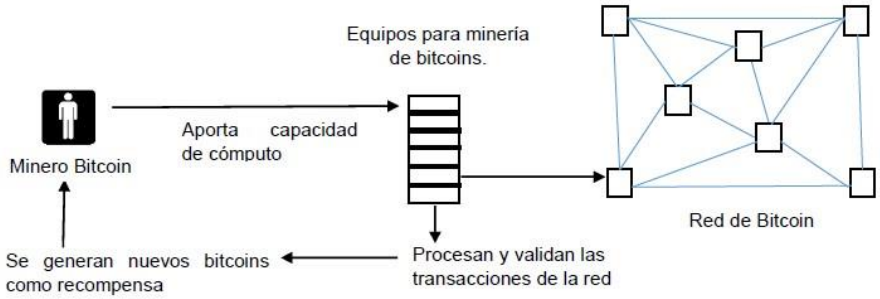
Para entender hemos investigado cómo funciona y quien desarrollo esta criptomoneda. Satoshi Nakamoto, al desarrollar Bitcoin, se basó en los conceptos fundamentales de los prototipos y antecesores de las criptomonedas. Particularmente, tomó inspiración basándose en las propuestas de Wei Dai, quien ya en 1998 había planteado la idea de una divisa digital anónima mediante criptografía. Fundamentalmente, las criptomonedas son divisas digitales que funcionan con un sistema de pagos no centralizado utilizando la modalidad "peer-to-peer" (P2P). Bitcoin permite el intercambio de valor entre usuarios sin requerir una entidad mediadora.

A pesar de que estas divisas no son consideradas monedas de curso oficial, operan al margen de autoridades gubernamentales o bancarias y se apoyan en una red global y distribuida. Las operaciones están codificadas para garantizar la información personal de los usuarios, lo que hace que las transferencias sean anónimas.

Todas estas operaciones se registran en un libro contable público, conocido como blockchain, accesible para todos los participantes.

Figura 1

Proceso Bitcoin



Fuente (López 2015)

Cualquier usuario que quiera enviar o recibir bitcoins necesita una cartera específica, denominada Bitcoin wallet.

El Bitcoin ofrece varias ventajas en comparación con el sistema financiero tradicional. Por un lado, gracias al sistema blockchain, las transacciones son casi sin coste y se realizan de forma instantánea. En cambio, en el sistema financiero convencional, las transacciones suelen implicar comisiones y pueden tardar más tiempo debido a la naturaleza centralizada de este sistema.

Como se señaló antes, las criptomonedas ganaron prominencia en 2013 cuando se reveló que Silk Road, un mercado negro en línea, realizaba todas sus transacciones en bitcoins, beneficiándose del carácter anónimo y no centralizado de estos recursos. Silk Road, iniciado en 2011, ofrecía una amplia gama de bienes y servicios ilícitos, desde drogas y armas hasta identificaciones falsas y servicios de hackers, incluso llegando a servicios de sicariato. Para evadir a las autoridades, Silk Road no solo usó Bitcoin sino que también se valió de la red "The Onion Router", o "TOR". Según Brill y Keene, esta es "una red global concebida para ocultar las direcciones IP y, consecuentemente, las identidades de quienes la utilizan". En 2013, las autoridades de EE.UU. detuvieron a Ross Ulbricht, creador de Silk Road, y lo condenaron a cadena perpetua por múltiples cargos, entre ellos el blanqueo de capitales. Ese mismo

año, Charlie Shrem, vicepresidente de Bitcoin Foundation y fundador de BitInstant, fue arrestado por facilitar operaciones de lavado de dinero a clientes de Silk Road. Al cerrar Silk Road, tenía más de 957,000 cuentas de usuario, había logrado ventas por 1.2 billones de dólares y obtenido 80 millones en comisiones.

La aparición de las criptomonedas y la tecnología que las respalda han dado a los delincuentes una herramienta innovadora y eficaz para facilitar actividades ilícitas, presentando un reto significativo para los legisladores y entidades reguladoras. Es vital resaltar que la gran mayoría de individuos que recurren a las criptomonedas no tienen intenciones delictivas y, en su lugar, ven a estas monedas digitales como una inversión para obtener beneficios mediante la especulación. Sin embargo, no se puede ignorar que las criptomonedas tienen aplicaciones ilícitas. Entre la amplia variedad de delitos que se han visto potenciados por esta tecnología, hay dos en particular que han capturado la atención y preocupación de las autoridades debido a su seriedad y crecimiento acelerado en el ámbito de la ciberdelincuencia. La estafa y el lavado de activos se han convertido en el foco central de los debates sobre cómo regular adecuadamente las criptomonedas.

III. PROPUESTA

Esta sección analizará en profundidad las características de los delitos de lavado de dinero, proporcionando una descripción detallada de su estructura típica. También se ofrecerán criterios y valoraciones basadas en la doctrina sobre los componentes objetivos y subjetivos de estos delitos. Concluirá con un análisis de los métodos que utilizan los ciberdelincuentes para perpetrar estos delitos mediante el uso de criptomonedas.

Este segmento se ajustará a los rasgos particulares de los crímenes de engaño y blanqueo de capitales, dando una definición detallada desde su configuración estándar. Además, se proporcionarán juicios y apreciaciones basadas en la doctrina jurídica sobre los componentes objetivos y subjetivos que forman estos actos delictivos. Para finalizar, se expondrán los procedimientos que los ciberdelincuentes usan para llevar a cabo estos delitos utilizando criptomonedas.

Ecuador ha establecido regulaciones sobre lavado de activos a través del Código Orgánico Integral Penal, la Ley Orgánica Prevención, Detección y Erradicación del Delito de Lavado de Activos y del Financiamiento de Delitos, así como su normativa anexa y otras pautas vinculadas. Al comienzo, el blanqueo de capitales era principalmente percibido como un medio para disfrazar actividades ilícitas. Sin embargo, organizaciones internacionales como el Grupo de Acción Financiera Internacional (GAFI), la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) y el Grupo Egmont han destacado la necesidad de abordar este delito con seriedad. Estas entidades han propuesto recomendaciones, que son reconocidas como estándares internacionales, instando a los países a clasificar el lavado de activos como un delito independiente. Esta designación como un delito autónomo surge como resultado de una estrategia consciente en la lucha contra el crimen.

Fases del ciclo de lavado de dinero

A nivel global, se reconoce que el proceso que utilizan los delincuentes para legitimar fondos provenientes de actividades ilícitas se desarrolla en tres fases clave: colocación, estratificación, e integración. A continuación, se detallan las características y acciones asociadas a cada una de estas fases.

Colocación: La colocación es la etapa inicial en la que se introduce el dinero ilícito en el sistema formal, ya sea comercial o financiero. El objetivo principal en esta fase es desvincular el capital de su origen delictivo. Marengo enfatiza que esta es la fase donde los lavadores enfrentan el mayor riesgo, principalmente debido a los requerimientos de identificación y monitoreo de transacciones que superen ciertos montos. Existen varias tácticas utilizadas para realizar la colocación. Algunas de las más comunes incluyen: El "smurfing" o "pitufeo", que implica dividir el dinero ilícito en montos menores para evadir los controles de las instituciones financieras. Por ejemplo, depositar pequeñas sumas en diferentes cuentas bancarias de forma que no se perciban como transacciones atípicas o sospechosas por las entidades y eviten ser reportadas como operaciones inusuales a las autoridades financieras. El uso de empresas ficticias que existen solo en papel para mover fondos. Adquisición o construcción de propiedades inmobiliarias. Comprar billetes de lotería o tickets de viaje. Adquirir negocios que manejen grandes cantidades de efectivo, como discotecas o bares, y manipular sus registros contables para que parezca que tienen mayores ventas de las que realmente tienen, entre diversas técnicas.

Estratificación: Esta etapa, comúnmente denominada "layering", tiene como objetivo enmascarar el origen ilícito de los fondos mediante múltiples transacciones, complicando así el rastro y la identificación de su procedencia inicial. En esencia, se trata de redistribuir el dinero de manera repetida para alejarlo de su origen y dificultar su identificación por las entidades de control. Marengo señala que el propósito de la estratificación es romper cualquier conexión con la operación inicial, que es la más propensa a levantar sospechas, y así integrar el dinero al sistema legal sin alertas.

Integración: Esta fase implica reintegrar el dinero procedente de actividades ilícitas en la economía formal, haciendo que parezca que proviene de fuentes legales. Después de haber pasado por las etapas anteriores, estos fondos adoptan una apariencia de legalidad, lo que dificulta su detección por las autoridades. En este punto, distinguir entre ganancias legales e ilegales se vuelve muy desafiante. Tácticas frecuentes en esta etapa incluyen la adquisición de propiedades, la compra de bienes de lujo o metales valiosos, el uso de empresas pantalla y la participación en organizaciones no lucrativas, entre otras estrategias.

Método del uso de criptomonedas en esquemas de lavado de activos

Uso de cajeros automáticos para criptomonedas en el lavado de dinero

Debido al auge respecto a las criptomonedas, diversas compañías han comenzado a trabajar con cajeros automáticos especializados en estas divisas. En Quito, Ecuador, actualmente existen dos de estos cajeros, situados en la oficina 410 del edificio Metropolitan, donde se puede comprar y vender criptomonedas como Bitcoin, Dash y Pura a cambio de efectivo. La aparición de estos servicios ha generado inquietud entre las autoridades, ya que ven en estos cajeros una herramienta potencial para el lavado de dinero. Es importante destacar que, ante la falta de regulaciones y leyes internacionales claras sobre criptomonedas y servicios asociados, estos cajeros no se adhieren a las normas KYC o AML, ni siguen las directrices establecidas por en lo que respecta a protocolos de seguridad y diligencia que las entidades bancarias deben seguir, tanto la Superintendencia de Bancos y Seguros como la Junta Bancaria han establecido directrices a seguir.

Para la adopción de criptomonedas y la prevención de su uso indebido en Ecuador, se requieren las siguientes medidas:

Establecer una Fiscalía Especializada en Ciberdelincuencia, que no solo será crucial para abordar los delitos asociados con las criptomonedas, sino también para combatir la ciberdelincuencia en general. Esta fiscalía debe estar equipada con personal capacitado para lidiar con los ciberdelitos, incluyendo fiscales, secretarios, asistentes y expertos en el campo, todos equipados con las herramientas necesarias para perseguir estos delitos. Es esencial también la formación de jueces para lograr los objetivos previamente mencionados.

Ecuador necesita reforzar sus mecanismos de colaboración internacional en materia penal. Esto significa que debería ratificar el Convenio de Budapest de 2001 relacionado con la ciberdelincuencia y establecer más acuerdos bilaterales con diferentes naciones.

La Unidad de Análisis Financiero y Económico (UAFE) debe considerar a las empresas y entidades que comercian con criptomonedas como sujetos obligados, imponiendo condiciones de funcionamiento y la entrega de informes a la UAFE, tales como el Reporte de Sujetos Obligados (RESU) o el Reporte de Operaciones Inusuales e Injustificadas (ROII) y asegurándose de que cumplan con las normas Anti Lavado de Activos y Contra el Financiamiento del Terrorismo (ALA/CFT).

De la encuesta, se infiere que el 48,6% de los participantes está familiarizado con la criptomoneda Bitcoin. Esto sugiere un panorama prometedor para su integración en el sistema financiero. Sin embargo, esta cifra puede tener matices: posiblemente algunos lo conocen superficialmente, habiendo oído o leído sobre ello sin profundizar en su funcionamiento. Además, es notable que el 73% muestra interés en aprender más sobre la criptomoneda, lo que coincide con el 53% que expresó curiosidad en invertir en ellas en algún momento.

En un artículo reciente del medio digital “Primicias” de junio de 2021, se menciona: “En Ecuador, la circulación de bitcoins representa alrededor de USD 400 millones” Primicias. (2021). A pesar de esta cifra, el Banco Central del Ecuador ha emitido comunicados para informar a la población, destacando: “El Banco Central del Ecuador quiere hacer saber que el bitcoin no está permitido

como forma de pago en el país. Esta criptomoneda no posee respaldo y su valor se basa en pura especulación. Cualquier transacción financiera realizada con bitcoin escapa al control y regulación de las autoridades ecuatorianas, lo que supone un riesgo financiero para quienes decidan utilizarla.” Banco Central del Ecuador. (2018).

A pesar de los riesgos, la ciudadanía ha mostrado inclinación hacia las ventajas económicas del bitcoin. El volumen de dinero relacionado con esta moneda digital en el país es notorio, especialmente en comparación con algunas de las principales exportaciones del 2021. Es vital considerar la magnitud de las transacciones anuales en estas plataformas y cómo pueden influir en la economía nacional.
De acuerdo con Minsait Payments, las criptomonedas se sitúan entre las opciones favoritas de los ecuatorianos con acceso bancario.

Los datos de la firma indican que alrededor del 30% de los ecuatorianos con cuentas bancarias, que suman aproximadamente 2,4 millones, han realizado operaciones vinculadas a criptomonedas. El estudio muestra que el 15,8% de las transacciones monetarias en Ecuador durante el último año se hicieron mediante criptomonedas.

Adicionalmente, se destaca que la mayoría de los entusiastas de las criptomonedas en Ecuador son jóvenes menores de 35 años, con ingresos medios o altos.

IV. CONCLUSIONES

Objetivo General:

- Identificar la criptomoneda específica y analizar su relación con el lavado de activos en Ecuador durante el 2022.

  Se Identificó a la criptomoneda el BITCOIN como específica para analizar también su relación con el lavado de activos en Ecuador.

  Por lo tanto, este objetivo general se ha cumplido.

Objetivos específicos:

- Realizar una revisión de las criptomonedas utilizadas en Ecuador y seleccionar la criptomoneda específica que se analizará en relación con el lavado de activos.

Mediante la investigación se realizó una revisión de las criptomonedas más utilizadas en Ecuador, se seleccionó al BITCOIN para analizar la relación con el lavado de activos.

Por lo tanto, este objetivo específico se ha cumplido.

- Investigar y recopilar datos sobre la adopción y el uso de la criptomoneda seleccionada en el contexto ecuatoriano, incluyendo la cantidad de transacciones, los usuarios y los casos relevantes.

Se investigó y se recopilo información sobre la adopción del BITCOIN en el contexto ecuatoriano cantidad de transacciones, los usuarios y los casos relevantes.

Por lo tanto, este objetivo específico se ha cumplido.

- Examinar casos y eventos en los cuales se haya utilizado la criptomoneda seleccionada para realizar actividades de lavado de activos en el país.

Se examinó un caso que ocurrió en la ciudad de Quito en donde se detectó actividades relacionadas al lavado de activos.

Por lo tanto, este objetivo específico se ha cumplido.

Para los ecuatorianos con acceso a servicios bancarios, las criptomonedas se han convertido en una opción atractiva dentro de los activos digitales.
Un notable 30% de estos ciudadanos, que representan cerca de 2,4 millones de personas, ha explorado el universo de las criptomonedas a través de transacciones. Datos recientes reflejan que las criptomonedas representaron el 15,8% de los pagos en la economía del país el último año.
Es interesante observar que aquellos que invierten o utilizan criptoactivos en Ecuador son, en su mayoría, jóvenes por debajo de los 35 años con una capacidad económica media-alta.
Con la creciente popularidad de las criptomonedas, varias compañías han establecido cajeros automáticos dedicados a estas monedas digitales. En la capital ecuatoriana, Quito, se pueden encontrar dos de estos cajeros en la oficina 410 del edificio Metropolitan. Estas máquinas facilitan la compra y venta de criptodivisas como Bitcoin, Dash y Pura a cambio de efectivo.

Estos cajeros automáticos de criptomonedas pueden ser empleados por delincuentes para lavar dinero procedente de actividades ilícitas.

SUGERENCIAS Y RECOMENDACIONES

Sugerencias y Recomendaciones para mejorar evitar el lavado de activos.

Las criptomonedas se crearon para funcionar como un mecanismo de transacción descentralizado utiliza tecnología de peer-to-peer (P2P). Proporcionan un método para transferir valor de un usuario a otro sin la necesidad de un intermediario. No están respaldadas por ninguna divisa reconocida oficialmente y operan sin la intervención de organismos gubernamentales o instituciones financieras.

Aunque todas las transacciones son encriptadas para mantener la privacidad del usuario, los detalles de las transacciones están disponibles públicamente en un libro de contabilidad blockchain, que se distribuye en cada punto de la red.

Así, los rasgos distintivos de las criptomonedas incluyen su naturaleza descentralizada, el carácter anónimo, las transferencias inmediatas de valor y la eliminación de intermediarios. Estas características las hacen atractivas para la comisión de delitos.

Existen principalmente dos tipos de delitos facilitados por las criptomonedas que han provocado preocupación en las autoridades: el lavado de dinero y el fraude.

Hay dos técnicas principales que los delincuentes han utilizado para cometer fraudes con criptomonedas. Estas son las Ofertas Iniciales de Monedas (ICO) fraudulentas y los contratos inteligentes fraudulentos.

Los delincuentes usan ICOs y contratos inteligentes como esquemas de Ponzi para estafar para los inversionistas. Los sistemas Ponzi, también conocidos como fraudes piramidales, operan atrayendo constantemente a nuevos inversores y utilizando su capital para pagar a los inversores anteriores.

En cuanto al lavado de dinero, los delincuentes han encontrado diversas formas de cometer este delito utilizando criptomonedas. Un método es el uso de cajeros automáticos de criptomonedas, que a menudo no están regulados ni cumplen con las medidas de seguridad adecuadas.

Otra técnica es el uso de servicios de mezcla de criptomonedas, también conocidos como mixers. Estos mixers aumentan el anonimato de una transacción de criptomonedas combinando los fondos de una transacción con los de otras operaciones o distribuyéndolos entre múltiples billeteras de criptomonedas propiedad del mixer.

Las características de las criptomonedas que posibilitan actividades ilícitas han motivado a los países a optar por una de tres posturas en su regulación: la pasividad, la restricción total o la regulación. De estas respuestas, únicamente la regulación parece ser efectiva para contrarrestar el uso delictivo de las criptomonedas.

La restricción total de las criptomonedas, sumada a penalizaciones sin distinción entre usos legales o ilícitos, contradice el principio de intervención mínima en materia penal, considerando que no todas las usanzas de las criptomonedas representan una amenaza para los intereses protegidos por la ley.

Malta y Estados Unidos son dos países con regulaciones detalladas y específicas sobre las criptomonedas. Malta ha promulgado legislación exhaustiva sobre las criptomonedas que abarca todos los aspectos jurídicos de los criptoactivos.

Una característica destacada de la legislación maltesa es su tratamiento de las ICOs de manera similar a las Ofertas Públicas Primarias. En cambio, Estados Unidos ha implementado la BitLicense, que impone a las empresas que operan con criptomonedas rigurosos controles, como sistemas de reconocimiento del cliente y análisis de riesgos.

Si Ecuador opta por integrar las criptomonedas en su sistema económico, las normativas de Malta y Estados Unidos podrían servir como un modelo a seguir para la inclusión de estas monedas digitales en la nación.

Ecuador deberá implementar ciertas medidas para adoptar las criptomonedas y prevenir su uso ilícito. Estas incluyen:

- Crear una Fiscalía Especializada en Ciberdelincuencia, que sería útil no solo para tratar los delitos relacionados con las criptomonedas, sino también para combatir la ciberdelincuencia en general.
- Esta fiscalía debería tener personal adecuado, incluyendo fiscales, secretarios, asistentes y expertos capacitados en la materia y equipados con las herramientas necesarias para investigar estos delitos; también es crucial capacitar a los jueces.
- Fortalecer la colaboración internacional en materia penal, lo que conllevaría adherirse al Convenio de Budapest de 2001 sobre Ciberdelincuencia y formalizar acuerdos bilaterales con un mayor número de naciones.
- La Unidad de Análisis Financiero y Económico (UAFE) debe considerar a las empresas y organismos que negocian con criptomonedas como sujetos obligados, imponiendo requisitos operativos y normas de Anti-Lavado de Activos y Contra el Financiamiento del Terrorismo (ALA/CFT).

V. REFERENCIAS BIBLIOGRÁFICAS

Acevedo Eliana, y Rodríguez, Raíza. (2018). "Estudio del Bitcoin en el contexto del blanqueo de fondos en el sistema panameño". Ponencia presentada en el III Congreso de Investigación, Desarrollo e Innovación de la Universidad Internacional de Ciencia y Tecnología, pp. 231-253.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Primicias. (20 de Junio de 2021). El mercado de bitcoins mueve USD 400 millones al año en Ecuador. Obtenido de Primicias: https://www.primicias.ec/noticias/economia/criptomonedas-bitcoinecuador-usodolares/

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