Julio/2021 www.csirt.gob.cl

ESPECIAL CIBER SUCESOS

Investigación, Tendencia y Concientización

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Historia de las criptomonedas y su estrella, el bitcoin

Cripto Noticias

Blockchain y criptomonedas

Estafas con criptomonedas

La fiebre del bitcoin

El lado oscuro de las criptomonedas

CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

CSIRT es el Equipo de Respuesta ante Incidentes de Seguridad Informática del Gobierno de Chile. Su misión es reducir los riesgos de la ciberseguridad en las redes del Gobierno de Chile, asesorando a las diferentes organizaciones que lo componen, actuando como socio estratégico en la defensa de las amenazas y colaborando para brindar mayor seguridad y robustez a las infraestructuras del Estado.

¿Cómo lo **hacemos?**

Contamos con un equipo multidisciplinario de profesionales y las tecnologías para proveer de asistencia técnica y logística a nuestros beneficiarios, así como prevenir la explotación de vulnerabilidades y actuar oportunamente frente a amenazas y ciberataques.

- MONITOREO DE LAS PLATAFORMAS DE INTERNET DE ORGANISMOS PÚBLICOS Y PRIVADOS **24/7**
- INVESTIGACIÓN Y CAPACITACIÓN PARA ENFRENTAR LAS AMENAZAS DEL FUTURO
- DETECCIÓN DE VULNERABILIDADES DE SITIOS Y SISTEMAS WEB DEL ESTADO
- GESTIÓN DE INCIDENTES Y DIFUSIÓN DE MEDIDAS PREVENTIVAS
- INCORPORACIÓN DE NUEVAS TECNOLOGÍAS Y HERRAMIENTAS DE SEGURIDAD INFORMÁTICA
- MEJORA CONTINUA DE LOS ESTÁNDARES DE CIBERSEGURIDAD DEL PAÍS

Alianza del Pacífico · FIRST · CSIRTamericas.org · MERIDIAN Connecting and Protecting

INDICE

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

CIBER SUCESOS
Investigación, Tendencia y Concientización

cibersucesos@interior.gob.cl

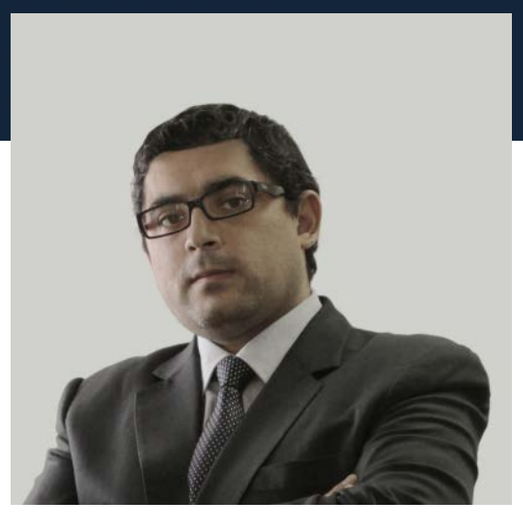
Director: Carlos Landeros Cartes

Jefa de contenidos y edición:
Katherina Canales Madrid

Colaboradores equipo CSIRT:
Ramón Rivera
Hernán Espinoza
Juan Sanhueza

Diseño y diagramación: Jaime Millán

EDITORIAL



Carlos Landeros Cartes
Director Nacional
CSIRT de Gobierno

Hay pocos temas que estén tan presentes en el día a día de los diarios, los noticieros, las redes sociales y la publicidad que las criptomonedas. Numerosos autodenominados expertos llaman a invertir en ellas, principalmente en Bitcoin, pero también en otras como Etherium y Dogecoin. En la misma línea, numerosas cuentas en plataformas como Twitter o YouTube declaran las bondades de estos activos mientras auguran un futuro en que el dinero será electrónico, descentralizado y sin intervención de bancos centrales o estados, lo que postulan como un futuro utópico.

Por otro lado, también se oye hablar de criptomonedas en el contexto del lavado de activos y de ciberdelitos como el ransomware, en el cual para el rescate de los activos digitales secuestrado se exige un pago en Bitcoin o en criptomonedas con énfasis en el anonimato, como Monero.

¿Son entonces las criptomonedas una tendencia positiva o un catalizador del ciberdelito? Como en todas las cosas, la respuesta es compleja. Porque como toda tecnología, en gran parte su efecto depende de las intenciones y objetivos de quienes las utilizan. Por lo mismo, decidimos dedicar un especial completo de CiberSucesos a hablar de criptomonedas, presentando sus promesas y sus amenazas, para ayudar a que la comunidad pueda formarse su propia opinión.

De esta forma es que en este número especial de CiberSucesos revisamos qué son las criptomonedas, su historia, para qué se pueden usar, cómo se generan y qué es la minería, si son o no dinero, sus promesas para mejorar nuestros pagos y el sistema financiero internacional, y también su uso delictivo. Además, explicamos cómo funcionan el blockchain y otros sustentos tecnológicos de las criptomonedas, describimos algo de la montaña rusa que ha sido la cotización del Bitcoin desde su lanzamiento y también entregamos varios consejos para mejorar la ciberseguridad de quienes deciden invertir en estos nuevos activos, incluyendo herramientas de protección.

Además, revisamos varios de los últimos desarrollos que ha enfrentado esta tendencia, como las pruebas realizadas para su adopción masiva, incluyendo el anuncio de El Salvador de reconocer al Bitcoin como moneda de curso legal, todo como parte de la sección Cripto Noticias.

Decidimos asimismo incluir, como en nuestras ediciones tradicionales, la columna Legal, en la cual Francisco Bedecarratz, Observatorio de Ciberseguridad de la Universidad Autónoma de Chile, nos explica las implicancias legales que trae el auge de las denominadas criptomonedas, desde el punto de vista de la legislación chilena.

HISTORIA DE LAS CRIPTOMONEDAS **Y SU ESTRELLA, EL BITCOIN**

Su nombre está en boca de todos desde hace algunos años, pero, ¿qué son realmente las criptomonedas? Con ese nombre se conoce a una serie de activos digitales que se autodefinen como un reemplazo del dinero tradicional.

Tal como lo indica la raíz griega de su nombre ("crypto", que significa secreto u oculto), el origen de la más famosa y transada de las criptomonedas está sumido en el misterio. Bitcoin nació gracias a un paper publicado en noviembre de 2008, cuyos autores aún se desconocen. Este artículo, firmado por un tal Satoshi Nakamoto (que se cree no sea más que un pseudónimo), delineaba la forma de implementar una criptomoneda descentralizada y basada en la distribución pública de un registro llamado "ledger" (algo así como libro de contabilidad) y constituido por una cadena de bloques: la blockchain.

Es importante recordar que, en términos generales, para que algo sea definido como dinero debe servir como mecanismo de intercambio, unidad de medida y como reserva de valor. Para lograr estos objetivos es clave que el activo sea escaso y que no se pueda realizar "doble gasto" (potencial riesgo de las monedas digitales, que haga posible que una misma moneda (o "token") pueda ser usado dos veces). Para evitar el "doble gasto", Nakamoto implementó un protocolo criptográfico que inscribe en cada eslabón de la cadena, en cada compra o venta con estos activos todo el historial de transacciones en bitcoin, haciendo extremadamente difícil alterarlo con el objetivo de volver a usar un bitcoin más de una vez.

Desde entonces ha surgido una infinidad de criptomonedas, aunque Bitcoin sigue dominando la escena, duplicando en capitalización de mercado a la segunda que recibe mayor inversión, Ethereum.


1
00001
00 10 1
10100
000 0
11010 1
1
Crypto-currency
Bitcoin

Mayores criptomonedas hoy, según capitalización de mercado

1.	**Bitcoin**	US$ 654.130 millones
2.	**Ethereum**	US$ 234.700 millones
3.	**Tether**	US$ 62.660 millones
4.	**Binance Coin**	US$ 48.160 millones
5.	**Cardano**	US$ 44.170 millones
6.	**Dogecoin**	US$ 33.140 millones
7.	**XRP**	US$ 31.530 millones
8.	**USD Coin**	US$ 25.480 millones
9.	**Polkadot**	US$ 15.680 millones
10.	**Uniswap**	US$ 10.590 millones

Distintos conceptos de monedas digitales habían surgido ya con anterioridad mucho antes del bitcoin, sin mayor impacto. Un ejemplo fue eCash, lanzado en 1995 en base a un paper describía la forma de desarrollar una forma de dinero anónimo y electrónico, publicado en 1983. Fue puesto a prueba por un banco en Missouri, y a menor escala en otros de Europa, sin éxito, siendo eliminado en 1998. Su énfasis estaba en la privacidad de las transacciones, pero eso no pareció motivar a suficientes clientes en países con amplia penetración de las tarjetas de crédito. Nuevos proyectos surgieron, mayormente relegados a foros de fanáticos de la idea de las criptomonedas, autodenominados "cypherpunks" y seguidores de ideas libertarias, contrarias al control gubernamental de la moneda.

De hecho, el anonimato y la independencia de autoridades centralizadas es un fundamento clave para quienes apoyan a las criptomonedas desde un punto de vista más idealista. A diferencia de las monedas históricas y actuales, las criptomonedas como bitcoin no dependen de una autoridad central, los bancos centrales nacionales y supranacionales (como el euro, el franco CFA y el dólar del Caribe Oriental), monedas que de todas formas desde el abandono del patrón oro en los años setenta no basan su valor en ningún activo real, dependiendo este fundamentalmente de la política monetaria de la autoridad (tasas de interés de referencia y volumen de emisión) y factores fundamentales de cada economía, como su balanza comercial y de pagos, y las expectativas que tengan las personas comunes y corrientes de la inflación a corto y largo plazo.

Por lo mismo, parece lógico que un proyecto como bitcoin haya surgido y logrado popularidad en 2009, justo durante la crisis subprime, punto alto de la desconfianza mundial hacia los bancos centrales y el sistema financiero en general.

SABÍAS QUE se considera como la primera compra hecha con bitcoin en el mundo real a dos pizzas de Papa John's, por las que una persona pagó 10 mil bitcoin en 2010 (claro que para realizar en la práctica el pago a la pizzería se usó la tarjeta de crédito de un intermediario). Cada pizza costó el equivalente a US$317 millones en el peak del precio del bitcoin, este abril, y aproximadamente la mitad al valor actual.

Los Mineros y su rol **para las criptomonedas**

No existiendo una entidad que emita las criptomonedas, esta función es reemplazada por la denominada minería. Tal como cuando las monedas eran, y valían, su precio en metales preciosos, quienes generan criptomonedas como el bitcoin son denominados mineros, quienes invierten en el poder computacional para la resolución de complejos problemas matemáticos (relacionados con la mantención de la blockchain y el protocolo criptográfico dedicado a evitar el "doble gasto") con la creación de nuevas monedas como recompensa.

En la práctica, esto se ha convertido en una ecuación en la que el costo de generar bitcoin son enormes cantidades de poder de procesamiento y energía eléctrica, lo que ha incentivado a la creación de gigantescas granjas de servidores en lugares fríos (como Siberia e Islandia, para facilitar su refrigeración) o con electricidad subsidiada (como Irán) o barata (como el Tibet), además de la popularización de malware para infectar equipos y generar botnets para ayudar a la minería. Lamentablemente, esto también genera como consecuencia una alta huella de carbono en muchas de las instancias de minería de bitcoin, como las que se realizan en China, dependiente en gran parte del carbón para su generación eléctrica.

CRIPTO NOTICIAS

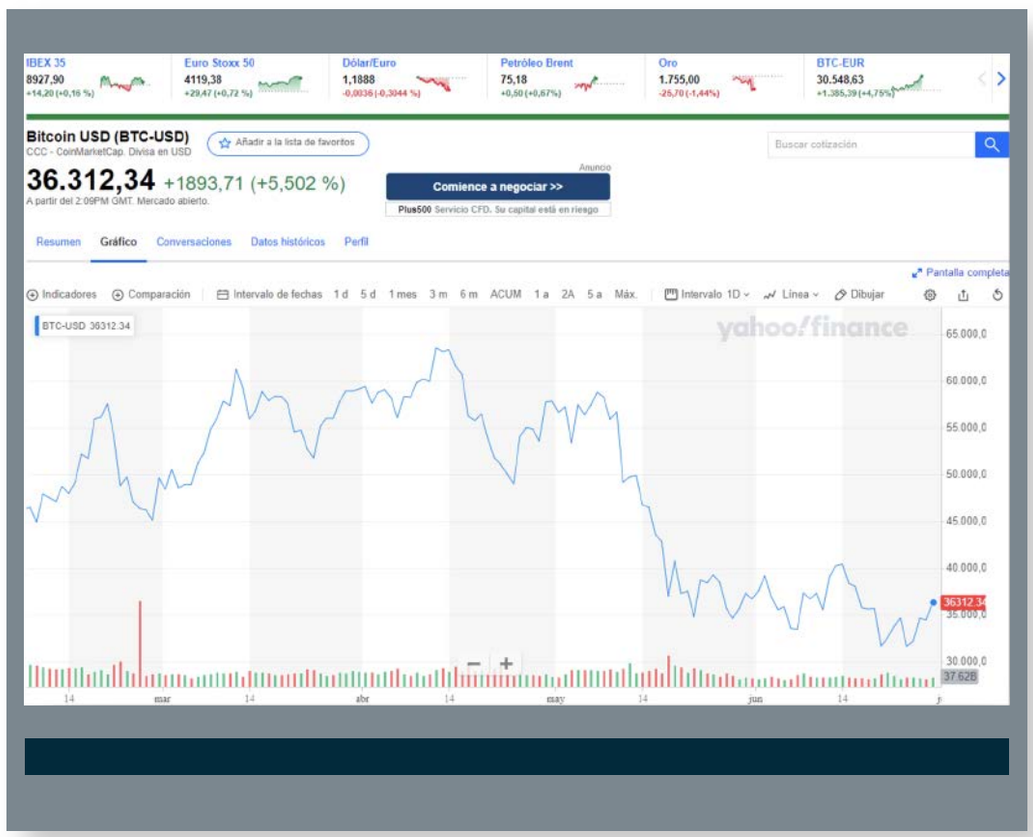
El bitcoin es un tipo de criptomoneda, es decir, una activo digital que, según sus promotores, cumpliría con las condiciones requeridas para constituir una forma de dinero, es decir, ser método de intercambio, unidad de cuenta y reserva de valor, aunque de acuerdo con el Banco Central, no hay consenso en los círculos financieros internacionales de que realmente cumplan con estas tres características[1]. Lo que sí es seguro es que no existe físicamente ni su emisión es controlada por ningún país.

Otra característica del bitcoin y la mayoría de las criptomonedas ha sido una gran volatilidad en sus precios. El bitcoin se puede usar en algunos casos para comprar productos o como instrumento de inversión, aunque no está disponible en todos los países y es aceptado por la mayoría de los comercios. En los casos donde sí es recibido, el bitcoin sirve para hacer pagos rápidos y evitar los cargos de transacción asociados a métodos de pago tradicionales.

Es importante recordar que en Chile el Banco Central, o Instituto Emisor, es la única institución autónoma facultada por Ley Orgánica Constitucional para emitir billetes, acuñar monedas y velar porque exista la adecuada cantidad de dinero circulando para así mantener una inflación baja y estable[2].

En nuestro Banco Central[3] el surgimiento del bitcoin y otras criptomonedas es monitoreado de cerca desde hace algunos años, junto a otras categorías de criptoactivos y posibles sustitutos del dinero.

Cabe notar que en el país no existen actualmente impedimentos para que las personas acepten convencionalmente cambiar bienes o servicios por criptoactivos, tal como podrían acordar el intercambio o trueque de cualquier otro activo.
No obstante lo anterior, conviene tener presente que el marco legal no permite calificar a los criptoactivos como dinero de curso legal o como divisas.



1 https://www.bcentral.cl/documents/33528/133557/IEF1_2018rec4-2criptoactivos.pdf/346a0b40-5dec-672a-57b4-6f1e9f8b695f?t=1573279495173
2 https://www.bcentral.cl/web/banco-central/el-banco/gobierno-corporativo/funciones-del-banco
3 https://www.bcentral.cl/documents/33528/133557/IEF1_2018rec4-2criptoactivos.pdf/346a0b40-5dec-672a-57b4-6f1e9f8b695f?t=1573279495173

ANONIMATO Y **LAVADO DE ACTIVOS**

A pesar de este contexto de incertidumbre que rodea a las denominadas criptomonedas, estas siguen ganando adeptos y notoriedad, siendo un problema su utilización para realizar transacciones ilícitas, gracias a la dificultad de conocer la identidad de los dueños de las billeteras que pagan y reciben bitcoin y otros criptoactivos.

Para contrarrestar esto último la Interpol lleva a cabo el proyecto Titanium[4] , financiado por la Unión Europea, y que ha tenido como fruto el desarrollo de GraphSense, una herramienta de análisis de cadenas de bloques que permite rastrear las transacciones realizadas con criptomonedas. Gracias a ella, los investigadores podrán buscar direcciones, etiquetas y transacciones de criptomonedas con las que identificar los clústeres en torno a una dirección, lo les permitirá "seguir el rastro del dinero" para avanzar en sus investigaciones.

Asimismo, y basándose en las necesidades expresadas por los países miembros, Interpol ha comenzado a desarrollar una herramienta analítica denominada Darkweb Monitor para recopilar datos sobre actividades delictivas en la red oscura, con los que luego se generará una información policial que facilitará las investigaciones de casos en todo el mundo. A partir de esos datos y de su posterior análisis no solo se podrán identificar nuevas tendencias delictivas, sino que se podrá avanzar en la investigación para recomendar actividades de prevención. Entre los datos que se pretende recabar se encuentran los siguientes:

- **Direcciones de criptomonedas**
- **Claves PGP**
  (programa de cifrado con privacidad bastante buena)
- **Direcciones IP**
- **Nombres de usuario y alias**
- **Direcciones electrónicas**
- **Dominios de los mercados de la red oscura**
- **Foros de la red oscura**
- **Historial de datos recopilados en la red oscura desde 2015**

El Equipo Especial de Interpol sobre la Red Oscura y las Criptomonedas está elaborando una taxonomía mundial de las criptomonedas, esto es, un conjunto de clasificaciones para determinar qué categorías de datos de transacciones sospechosas con criptomonedas deben recopilarse. Puede tratarse, por ejemplo, de las plataformas de intercambio de criptomonedas utilizadas, o de los tipos de delito a los que está vinculada cada distinto tipo de transacción.

Así pues, se seguirá un procedimiento similar al del etiquetado de fotografías digitales, a las que se añade una etiqueta digital con la localización geográfica de la imagen, la fecha en la que fue tomada y el tipo de cámara utilizada.

El proyecto de taxonomía, que se puede consultar en línea[5] , se ha organizado en torno a tres categorías de información:

- **Entidades: particulares, organizaciones y entidades digitales.**
- **Servicios: mercados de la red oscura, plataformas de intercambio de criptomonedas, facilitadores de mensajes y otros proveedores de servicios relacionados con la transacción.**
- **Tipos de delitos: delitos con los que está relacionada la transacción, tales como el comercio ilícito en línea de drogas o armas, abusos sexuales de menores, terrorismo o ciberdelitos.**

4 https://www.interpol.int/es/Quienes-somos/Marco-juridico/Information-communications-and-technology-ICT-law-projects/Project-Titanium
5 https://github.com/INTERPOL-Innovation-Centre/DW-CC-Taxonomy#_blank

El “lavado de activos” o llamado también “blanqueo de capitales” sigue siendo un desmesurado problema para los estados[6] . Su regulación data de los años ochenta y sabemos que consiste en el conjunto de mecanismos o procedimientos destinados a dotar de apariencia legal a aquellos bienes o activos de origen ilícito. Lo controvertido y novedoso se encuentra en las múltiples modalidades que van apareciendo en el transcurso del tiempo. Nuestras sociedades se vuelven cada vez más complejas y consecuentemente, es menester una legislación que se anticipe al lavado de dinero mediante criptomonedas, que aprovecha características como:

- **Descentralización y extraterritorialidad**
- **Anonimato y transparencia**
- **Volatilidad y falta de reserva**

Cabe advertir que las criptomonedas no son per se algo negativo, no obstante, resulta alarmante el uso de estos activos digitales por la «criptocriminalidad».

En base a estas supuestas características de anonimato e intrazabilidad es que también grupos terroristas buscan usar estos criptoactivos como forma de financiar sus actividades. En las regiones de Siria donde aún controlan territorio los rebeldes que luchan contra el régimen de Bashar al Assad y donde también operan filiales de ISIS y Al Qaeda, funcionan decenas de oficinas especializadas en el cambio de bitcoin y otras denominaciones virtuales. El partido militar Hamas que controla la Franja de Gaza también elude las sanciones recibiendo fondos en criptomonedas. En Francia, continúa el juicio contra un grupo de yihadistas que crearon “la arquitectura de una red de financiación al terrorismo a través de ciberdivisas”. Los cálculos de Interpol hablan de que los grupos terroristas manejaron más de 1.000 millones de dólares en monedas virtuales en 2020[7].

INCENTIVO PARA **EL MALWARE**

Desde otra mirada, criptoactivos como el bitcoin necesitan de un gran poder de cálculo computacional para que, a través de una actividad denominada criptominería[8] , sean encontradas matemáticamente las soluciones del algoritmo que permite su creación y posterior validación distribuida. Quien logra llevar a cabo estas tareas recibe un pago en bitcoin.

A partir de febrero de 2021, los criptomineros ganan 6,25 bitcoins por cada nuevo bloque minado, lo que equivale a unos 227.153 dólares

```
from setuptools import setup

setup(
    name='learninglib',
    version='0.2',
    packages=[],
    install_requires=['maratlib==0.6'],
    description='A working ml python API.'
    )

```

según el valor actual (26.344,40 US$/Bitcoin al 29 de Junio de 2021). También se les permite quedarse con las tasas de transacción de cada operación realizada en ese bloque, lo que equivale a 20 dólares por operación. Dado estos incentivos y el alto poder de cálculo que implica esta tarea, algunos criptomineros buscan fórmulas lícitas e ilícitas de acceder a mayor capacidad de cómputo para sus fines.
Una de las formas maliciosas de acceder a esa capaci

6 https://www.enfoquederecho.com/2021/04/06/hacia-un-nuevo-paradigma-del-lavado-de-activos-las-criptomonedas-y-el-cibercrimen/
7 https://www.infobae.com/america/mundo/2021/06/27/los-terroristas-de-isis-al-qaeda-y-hamas-recaudan-mas-de-1000-millones-de-dolares-al-ano-en-criptomonedas/
8 https://www.muyinteresante.es/tecnologia/articulo/que-es-la-criptomineria

dad de cómputo extra es desarrollar malware e infectar la mayor cantidad de computadores o servidores posibles, con tal de utilizar de manera no autorizada la capacidad de las máquinas infectadas. Por ejemplo, recientemente se detectó que el repositorio de índice de paquetes de Python estaba infectado con varios paquetes maliciosos, que hacían que las estaciones de muchos desarrolladores se convirtieran en máquinas de minería criptográfica[9] .

EXPERIMENTOS **EN EL SALVADOR, PARAGUAY Y EMIRATOS ÁRABES UNIDOS**

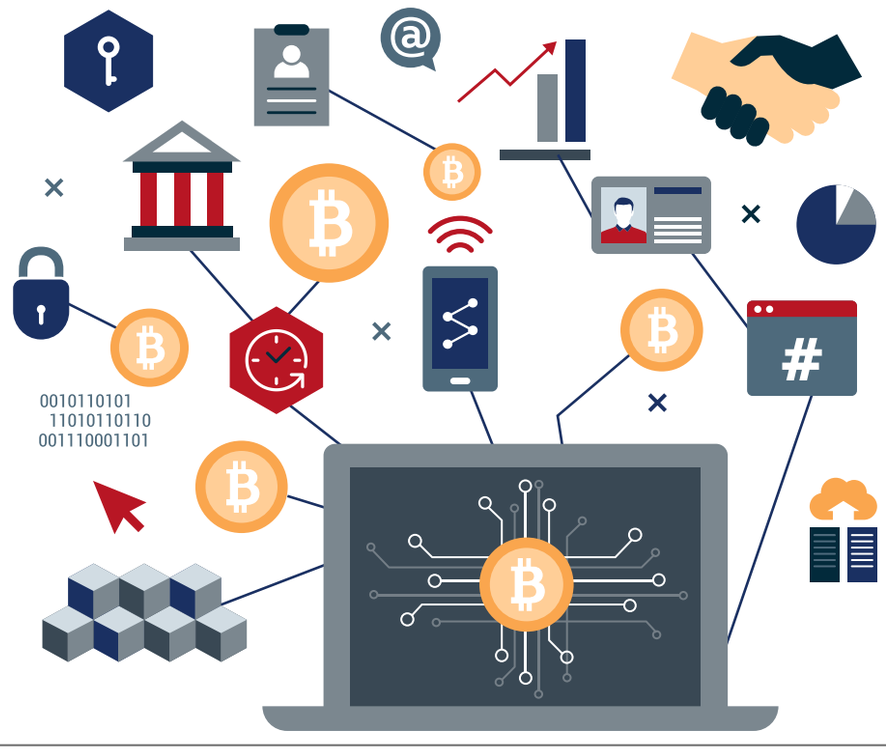
Por otro lado, hay países como El Salvador que están tratando de oficializar este criptoactivo dentro de su estructura monetaria, lo que no está exento de dificultades y dudas planteadas por instancias de apoyo financiero internacional como el Banco Mundial[10] .

En otros casos, se está permitiendo su uso para ciertas actividades económicas, como el pago de servicios de educación. Es así como la Universidad Americana de Paraguay comenzará a aceptar las criptomonedas bitcoin, ether, dash y XRP como formas de pago[11] ., según dijo a CoinDesk su director general, Camilo Jiménez Agüero. La Universidad Americana tiene 17 mil estudiantes, 60% de los cuales lo hacen virtualmente.

También se están utilizando criptomonedas en algunos países para establecer fondos de inversión, como el caso del primer fondo Bitcoin del Medio Oriente, en Dubai (Emiratos Árabes Unidos). Llamado The Bitcoin Fund, este ha sido incluido en el Nasdaq Dubai por 3iQ Corp, el administrador de fondos de inversión de activos digitales más grande de Canadá. El fondo es el primero de su tipo en el Oriente Medio, lo que abre esta próspera región a más inversiones en bitcoin, especulan algunos medios de comunicación.

Sin embargo, los usuarios de estas criptomonedas deben estar alertas. Hoy en día, el ecosistema de las monedas digitales suma cada vez una mayor cantidad de entusiastas y seguidores, muchos de los cuales tienen principalmente la expectativa de multiplicar su inversión en el corto o mediano plazo, aprovechando la volatilidad presente y las perspectivas que suponen para el futuro. Sin embargo, además de la propia volatilidad y nulas garantías que ofrecen estas inversiones, existen estafadores que hacen ofertas y plantean oportunidades de inversión falsas. Por eso es importante estar alerta ante las siguientes señales para sospechar de ofertas con criptomonedas que puedan ser demasiado buenas para ser verdad[12] :

- **Intermedian el proceso de compra**
- **Aseguran tener respaldo de celebridades o personas influyentes**
- **Se enmascaran como programas educativos. Presentan irregularidades al momento de captar la inversión**
- **Prometen márgenes de ganancias asegurados. Promueven su propia criptomoneda**
- **Incluyen un sistema de referidos con grandes beneficios (típico de una estafa piramidal)**
- **Presentan trabas para retirar su capital.**



9 https://www.ehackingnews.com/2021/06/python-package-index-repository.html
10 https://www.bbc.com/mundo/noticias-america-latina-57512089
11 https://finance.yahoo.com/finance/news/paraguay-university-accept-bitcoin-ether-180743610.html
12 https://www.diariobitcoin.com/negocios/estafas/usuarios-cuentan-como-cayeron-en-estafas-relacionadas-con-criptomonedas-conozca-las-trampas-mas-frecuentes/

BLOCKCHAIN Y **CRIPTOMONEDAS**

La tecnología que promete hacer a los criptoactivos infalsificables

Las criptomonedas se basan en el concepto de blockchain. Los blockchains, a su vez, son implementaciones de "distributed ledgers" o libros mayores públicos. En su sentido tradicional, un libro mayor es un registro de los ingresos y egresos de dinero en una empresa. De forma análoga, un libro mayor distribuido puede ser entendido como un libro mayor con varias copias sincronizadas en nodos, generando una red.

La idea detrás de hacer que este libro mayor sea distribuido es que, si un registro es falsificado, el resto de los nodos que tengan una copia del libro mayor pueda alertar (o rechazar) el registro falso.

Por otra parte, si uno de los nodos anuncia un nuevo registro, y este respeta el historial financiero existente, el nuevo registro es informado al resto de la red para que se replique en cada nodo. Naturalmente, no cualquier registro puede ser aceptado, lo cual implica reglas para que el registro pueda ser añadido, las cuales son validadas durante la minería y aceptación de criptomonedas.

Las llamadas billeteras son, estrictamente hablando, direcciones con claves y firmas digitales, y poseen un "balance", el cual es un deducible del historial de monedas generadas en la blockchain desde y hacia su dirección[1] . Cuando un usuario con una billetera quiere realizar una transferencia, se notifica una solicitud, conteniendo el destino, la cantidad de criptomoneda de la transacción, el costo que se quiere pagar por procesar la transacción[2] y las firmas digitales necesarias, hacia los mineros, los cuales la incluyen en un bloque.

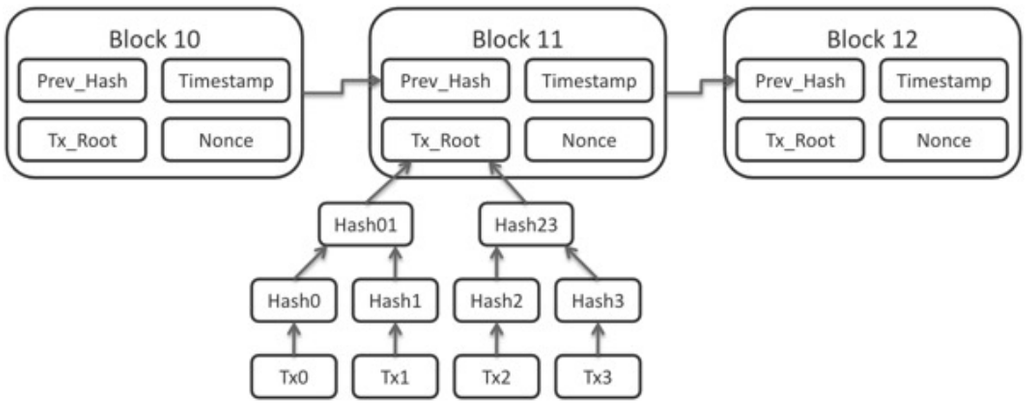


Ilustración 1 –
Diagrama de bloque de un blockchain

Un concepto igualmente importante para la validación de una transacción es el uso de una función de cifrado o hash. Estas son funciones que cifran un contenido de forma irreversible. Tienen una propiedad importante llamada efecto avalancha, que significa que el más mínimo cambio en el contenido original genera un cifrado completamente diferente. A modo de ejemplo, utilizando la función de hash sha-256 (usada por bitcoin), el cifrado del primer párrafo del clásico de literatura Don Quijote de la Mancha entrega el siguiente valor hexagesimal:

17d340a9f9b8ea4978feccb5285ff64fdc8e5bffac9698-fc734ef018150c7172

Si se agrega un segundo punto aparte al final del párrafo, el cifrado cambia al siguiente valor:

229d3f28669f78133db4d48c06c39f3b71e5cd7-db682338a7fa66f7d35e4fcb0

1 Dado que las monedas son en realidad transacciones individualizables, existen consideraciones adicionales al momento de recibir y enviar monedas, sin embargo, estas consideraciones se dejan fuera del alcance de este documento.
2 Además de que la cantidad de espacio disponible por bloque para guardar transacciones es limitada, el costo de transacción es parte de la recompensa para el minero, por lo existe un incentivo para incluir en un bloque las transacciones con mayor costo.

Como se puede observar, incluso el más pequeño cambio modifica enormemente el resultado final. Una función hash también tiene la propiedad de ser deterministica (el hash de un contenido es siempre el mismo mientras no se modifique el contenido) y no-predecible (no es posible obtener el resultado parcial o total sin ejecutar la función hash)

Volviendo al concepto de bloque, se puede ver que un bloque contiene una serie de datos y hash. En primer lugar, contiene un hash del bloque anterior. El efecto avalancha de la función hash implica que el bloque anterior ya no puede ser modificado puesto que el hash del bloque previo está vinculado al bloque presente. También contiene un campo llamado Timestamp con la fecha del bloque. TX_Root es el contenido del bloque, un arbol Merkle con las transacciones aceptadas en el bloque. Estas transacciones también son hasheadas y los hash resultantes se hashean en pares también de forma iterativa, formando una estructura de árbol[3] . Finalmente, contiene un nonce, que es un texto libre y una de las partes más importantes de la cadena, pues es de utilidad para obtener la prueba-de-trabajo.

Poseer esta prueba-de-trabajo permite que el bloque sea aceptado por la red. Su funcionamiento se encuentra vinculado al concepto de dificultad en la red. Cuando se entrega un bloque para su aceptación, se exige que el cifrado de ese bloque reúna ciertas condiciones, específicamente, que su valor cifrado sea menor a cierto valor deducible por la dificultad. Dado que las funciones de cifrado son no-predecibles y tienen efecto avalancha, el minero debe modificar el contenido de su bloque (este es el uso del nonce), de

forma que el cifrado del bloque cumpla los requerimientos de dificultad.
La recompensa de realizar latarea de generar un bloque válido que cumpla los requerimientos de dificultad es la creación de una cierta cantidad de criptomoneda a nombre del minero (o dirección, técnicamente) junto con la suma de todos los costos de transacción. El bloque válido descubierto es luego compartido con el resto de la red, la cual valida el bloque y sus transacciones. El nuevo bloque es añadido a la blockchain, se entrega la recompensa al minero y el proceso vuelve a comenzar[4] .

Bitcoin, la criptomoneda más famosa, se basa, a grandes rasgos, en el funcionamiento explicado anteriormente. Por otra parte, existen monedas alternativas (Altcoins), las cuales se basan en blockchain pero que ofrecen otros casos de uso.

Ethereum, por ejemplo, permite la ejecución de aplicaciones descentralizadas en su plataforma. XRP está orientado a las transacciones financieras entre distintas monedas mientras que Cardano, además de poder ejecutar aplicaciones, utiliza una prueba-de-participación[5] en lugar de una prueba de trabajo, disminuyendo el costo de energía de la minería.

Este último punto es muy importante, ya que el interés en las criptomonedas, unido a la recompensa que existe por realizar la minería ha incentivado el establecimiento de grandes granjas de minería, ocasionando un enorme costo en términos de energía. Por ello, Ethereum, en particular, ha mostrado gran interés en cambiar su modelo a prueba-de-participación para reducir el costo medioambiental[6] .

3 Esta estructura permite realizar validaciones de una transacción sin tener que descargar todo el bloque. Basta validar que el hash de la transacción que se quiere validar junto con los hash de las demás ramas en el formato del árbol coincidan con el hash de la raíz.
4 Es posible que se encuentren dos bloques válidos al mismo tiempo. Por lo general esto se resuelve a medida que pasa el tiempo, puesto que la cadena más larga es la considerada como canónica. También es posible que no se llegue a un acuerdo entre distintos nodos de la criptomoneda, lo cual puede llevar a un fork en el cual el blockchain diverge en dos versiones de la criptomoneda.
5La prueba-de-participación, a grandes rasgos, elimina la prueba de trabajo y la validación de transacciones se realiza calculando la participación total del validador en el mercado de monedas. Por ejemplo, si una persona tiene el 10% de las monedas emitidas, puede congelar el uso de ese porcentaje a cambio de volverse un validador y obtener la recompensa del 10% de las transacciones validadas.
6 https://fortune.com/2021/05/27/ethereum-founder-vitalik-buterin-proof-of-stake-environment-carbon/

ESTAFAS CON **CRIPTOMONEDAS:**

No todo lo que brilla es bitcoin

Para evitar resultar víctima de una estafa, cualquiera sea su tipo, la clave gira siempre en torno a la prevención, y las criptomonedas no son una excepción. Quien quiera trabajar con ellas deberá documentarse sobre su funcionamiento y el de sus mercados, lo que será muy útil para descubrir posibles estafas. Asimismo, deberá incorporar herramientas de protección como las siguientes:

1.– Armory: gestión segura de bitcoin

Armory[1] es una implementación en Python de código abierto, que permite a los usuarios hacer una gestión de sus billeteras de bitcoin de forma segura. Está disponible para ser implementada en los tres sistemas operativos más utilizados: Windows, Mac OS X y Linux.

2.– Electrum: modelo basado en la velocidad

Electrum[2] es un cliente ligero de bitcoin que está basado en un protocolo cliente-servidor, en el cual el archivo que contiene los bitcoins está cifrado y las transacciones se firmaron a nivel local, es decir, las claves privadas no se comparten con el servidor. Este modelo, bajo licencia GNU GPL v3, permite a cualquier persona auditar el código, lo cual reduce las posibilidades de puntos de falla.

3.– Blockchain.info: una cuenta en línea segura

Blockchain.info[3] ofrece el servicio de Mi Monedero[4], que brinda la facilidad de hacer pagos en todo el mundo de manera anónima y gratuita, de una forma sencilla y segura utilizando una computadora o un dispositivo móvil. Este servicio utiliza algoritmos de cifrado AES para proteger la billetera de posibles robos. Antes de ser almacenada en los servidores, la información de los bitcoins cifra en AES de 256 bits. Además, el usuario puede cifrar la cuenta con una segunda contraseña de forma opcional, necesitando la principal para el inicio de sesión y la secundaria para retirar fondos.

4.– Xapo.com: modelo híbrido de seguridad

Xapo[5] combina lo mejor de los dos mundos: la conveniencia de una billetera con la seguridad de una bóveda de almacenamiento fuera de línea. Los bitcoin pueden ser manejados desde una aplicación móvil a través de un correo electrónico o incluso con una tarjeta de débito.

5.– Trezor: el dispositivo de bolsillo

Este dispositivo está diseñado para funcionar en sistemas operativos Windows, Mac y Linux, y es amigable, ya que con solamente conectarlo a la computadora se pueden accionar sus dos únicos botones: confirmar o negar la acción. En contraste con las opciones anteriores o muchas otras similares, Trezor[6] basa su seguridad en mantener las claves en un dispositivo que se puede llevar en el bolsillo. Esto reduce posibles ataques a servicios que estén basados en la web.

1 https://bitcoinarmory.com/
2 https://electrum.org/
3 https://blockchain.info/
4 https://blockchain.info/es/wallet
5 https://xapo.com/
6 https://www.bitcointrezor.com/


****
OK

GOLPES A **LA CRIPTOMINERÍA**

Ahora bien, la propia industria de equipos optimizados para criptominería se ha visto afectada por la reacción contraria de algunos países. Por ejemplo, el banco central de China instó recientemente a tomar medidas más enérgicas contra la industria cripto, provocando una migración de numerosas compañías mineras a otros países. Esto provocó una caída de los precios de los equipos de minería y llevó a Bitmain, el principal fabricante de estos aparatos, a suspender temporalmente su venta[7] .

POTENCIALES VENTAJAS **DE UN CRIPTOACTIVO, SEGÚN SUS PROMOTORES.**

1. Global: no pertenece a ningún estado o go bierno y se puede utilizar en todo el mundo, independientemente de las barreras geográ ficas y políticas.
2. Ajeno al sistema fiduciario: su valor no depen de de las decisiones de un Banco Central.
3. Límite de emisión: el aumento predecible y a tasas decrecientes de la masa monetaria, permitiría en teoría mejorar el poder adquisi tivo de los usuarios.
4. Ampliamente divisible: actualmente se puede utilizar hasta con 8 decimales, aunque no hay límite por lo que en un futuro se podrían utili zar más decimales.
5. Transacciones rápidas: en menos de una hora puede estar realizada la transacción.
6. Irreversibilidad de las transacciones: no hay un tercero en medio que pueda echar atrás una transacción. De todos modos, existen servicios que custodian los bitcoin hasta que el receptor ha cumplido con su parte del acuerdo.
7. Teóricamente imposible de falsificar: hasta el momento y tal como está definido, no se podría construir un bitcoin falso ni efectuar un doble gasto sin que la red lo detecte.
8. No hay un regulador: ningún comité de exper tos controla el destino del bitcoin. Hay reglas, definidas en el protocolo ideado por Satoshi Nakamoto, que ha de aceptar libremente quien quiera utilizar el bitcoin.
9. Anonimato: nadie está obligado a revelar su identidad, lo que hace al bitcoin especialmen te útil para su uso en países donde gobiernan regímenes totalitarios.
10. Menores pagos a intermediarios: el bitcoin tiene menores costos de transacción que la utilización de tarjetas de crédito, transferen cias o Paypal. Realizando un pago con bitcoin se eliminan intermediarios.
11. Protocolo seguro: el bitcoin cuenta con un fuerte respaldo criptográfico, que lo protege de falsificaciones, y se puede guardar en múl tiples localizaciones simultáneamente. La tecnología en la que se basa el protocolo del bitcoin es varias veces más segura que la que utilizan bancos y tarjetas de crédito.
12. Transparencia: todas las transacciones quedan grabadas en un registro de libre acceso.
13. Micropagos: dado su divisibilidad y sus bajos costes de transacción es una moneda ideal para realizar micropagos.
14. Funciona las 24 horas al día: para las operacio nes en bitcoins no existen horarios ni días fes tivos.
15. Se acumula en un espacio ínfimo: podría guar darse una fortuna enorme en una memoria USB, que puede ser guardada o trasladada sin depender de terceros.

7 https://www.diariobitcoin.com/tecnologia/mineria/bitmain-pricipal-fabricante-de-equipos-mineros-bitcoin-del-mundo-detiene-ventas-para-apuntalar-precios/


+6.59
99.99
5.412
71.45
15.44
75.25
+8.76
65.32
+1.332
-12.14
64.25
55.01
1..233
-1.23
11.08

LA FIEBRE DEL BITCOIN

Si bien bitcoin se dio a conocer en 2009, esta y otras criptomonedas tardaron en masificarse, y aún no se consolidan, aunque han ido siendo cada día más acep tadas por instituciones más tradicionales, como em presas y bancos.

La principal razón de la dificultad en la aceptación de estos activos digitales parece ser la amplia volatilidad de su valor, que convierte a una inversión en bitcoin, por ejemplo, en algo riesgoso.

Así, un bitcoin podía comprarse por US$ 0,0008 en 2010, año en que su valor saltó 100 veces, hasta los US$ 0,08. Y mientras en abril del año siguiente un bit coin se transaba a un dólar, su precio se elevó 3.200% en dos meses (alza que se atribuye principalmente a su aparición en artículos de la revista Forbes y del sitio Gawker), llegando a los US$ 32 en junio. Con su nueva notoriedad, el bitcoin parecía para muchos ser la moneda del futuro, pero del mismo modo se populari-zó su uso para realizar intercambios ilícitos en el famoso sitio Silk Road, de la dark web.

Pero el auge no sería eterno. El bitcoin se desplomó nuevamente y cerró el año en torno a los US$ 2, en medio de noticias de la filtración de información de usuarios en la mayor bolsa de bitcoin de ese entonces, Mt. Gox, y la desaparición de la mitad de las bitcoin del servicio billeteras virtuales Mybitcoin.com. Por esta época también, en 2013, fue además que nació doge-coin, criptomoneda que surgió como una broma basada en el meme de un perro shiba inu apodado “doge”.

La aceptación por algunas compañías establecidas empezó por aquel entonces, aunque aún su uso no es extendido. En 2014, Microsoft comenzó a recibir bitcoin, y lo mismo hizo Paypal. El año siguiente, se unió Rakuten, el gran Marketplace virtual japonés. Whole Foods, el supermercado de Amazon, se sumaría en 2019, aunque no su firma matriz. Starbucks permite cargar bitcoin a sus sistemas de fidelización, para pagar con ellas por sus productos.

El ciclo de alzas y caídas del bitcoin solo comenzaba, aunque con una tendencia alcista hasta la explosión que le llevó a todas las portadas en 2017, cuando tras comenzar el año en los US$ 1 mil, llegó a rozar los US$ 20 mil, pero se desplomó cerrando el 2018 en torno a los US$ 3.500. Para mediados de 2019 el activo llegó a recuperar la mitad de su valor peak, alcanzando los US$ 11 mil, cayendo hasta los US$ 7 mil a fines de ese año, recuperándose casi hasta los US$ 10 mil a principios de 2020, cuando la pandemia del coronavirus (aparentemente) derribó su valor hasta los US$ 5.300 a mediados de marzo.

Recién en este punto, hace poco más de un año, vendría el gran vaivén del bitcoin, que desde entonces multiplicó más de 10 veces su valor en dólares en una loca carrera que parecía para muchos como su consagración, alcanzando los US$ 63.500 a mediados de abril del presente año... para volver a desplomarse y perder la mitad de su valor hasta estos días, donde ronda los US$ 30 mil.

Más allá de la variación del precio del bitcoin, su volatilidad es desafiante porque estos cambios de precio no parecen estar basados en fundamentos sólidos, sino en especulación e incluso los tweets de personajes influyentes.

ENTRE CHINA Y **ELON MUSK**

Precisamente, el bitcoin vio impulsado su valor en febrero de este año, cuando Elon Musk, principal dueño de la automotriz eléctrica Tesla, anunció que la empresa empezaría a aceptar esta criptomoneda como forma de pago para sus modelos, y reveló que Tesla había invertido US$ 1.500 millones en bitcoin. Y del mismo modo, el precio del activo bajó cuando en mayo Musk twitteó que Tesla dejaría de recibir bitcoin.
Musk también ha provocado dramáticos cambios en el precio del dogecoin. Tweets suyos y de celebridades de la música como Snoop Dogg y Gene Simmons promoviendo la criptomoneda, que llegó a su peak de US$ 0,67 en mayo, desplomándose luego de la aparición de Musk en el programa de NBC Saturday Night Live burlándose de dogecoin, ubicándose hoy en la mitad de dicho máximo.

La actual caída del bitcoin, eso sí, parece fundamentada por un factor más fundamental: la arremetida de China, que ha endurecido sus instrucciones a los bancos del país de reducir sus inversiones en criptomonedas, e incluso algunas de sus provincias han prohibido la criptominería. Y es que junto a su mayor relevancia, han crecido también los esfuerzos de los gobiernos por regular el uso de los criptoactivos, especialmente en lo relativo al anonimato en su utilización, que lleva a su empleo para transacciones ilícitas, y la forma en que pueden ser usadas para evitar pagar impuestos.

El futuro de las criptomonedas se dificulta asimismo por el surgimiento de versiones digitales de las monedas nacionales ya existentes, algo que China ya está probando con un yuan virtual.


09/30/2013 to 07/05/2021
1h 12h 1d 1w 1m 3m 1y all
$60000
$50000
$40000
$30000
$20000
$10000
2014
2016
2018
2020
coindesk


07/05/2020 to 07/05/2021
1h 12h 1d 1w 1m 3m
$60000
$50000
$40000
$30000
$20000
$10000
Oct
Jan
Apr
Jul
coindesk

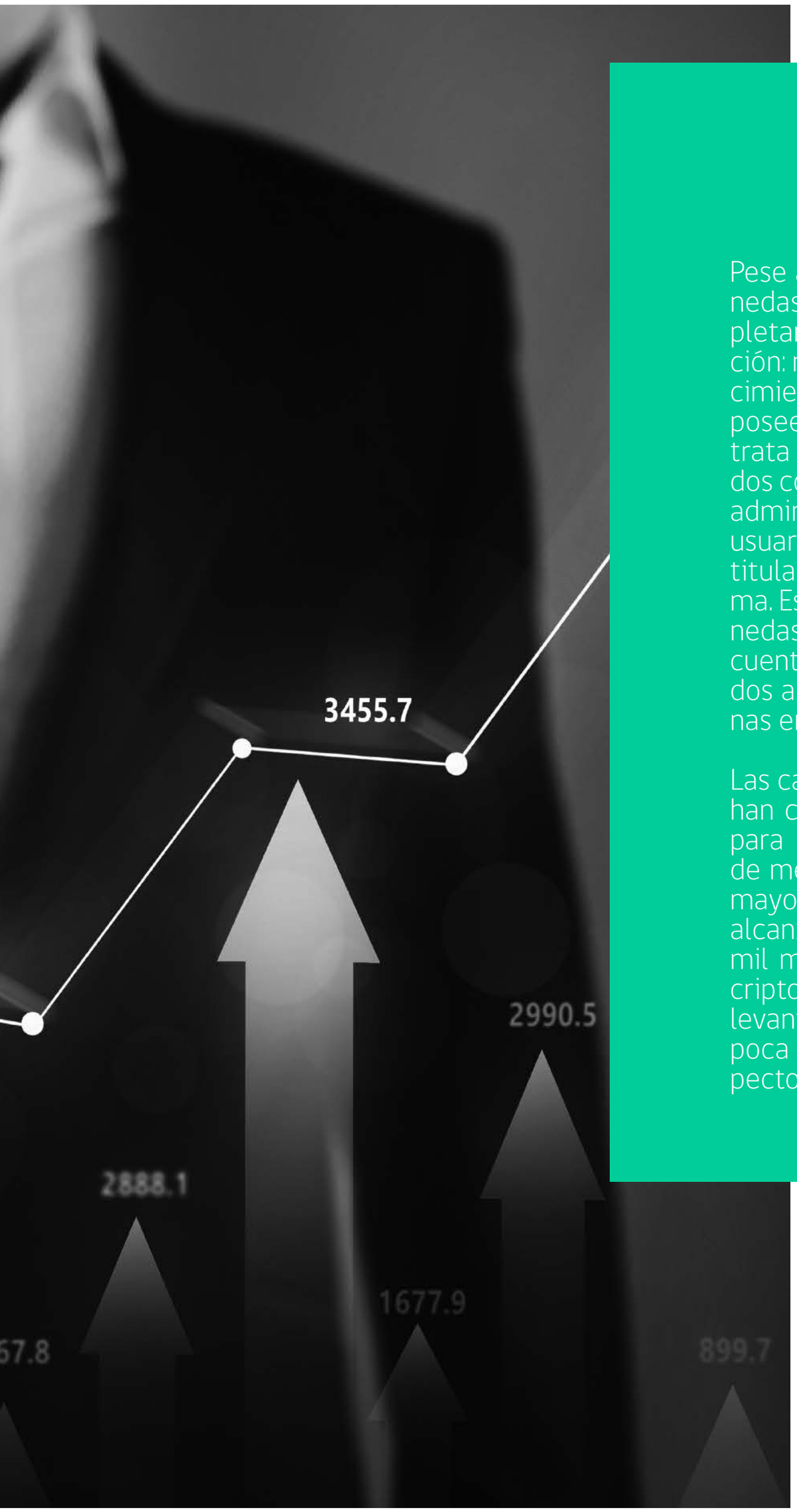
EL LADO OSCURO DE **LAS CRIPTOMONEDAS**

La experiencia internacional ha demostrado, que la inscripción de empresas dedicadas al Fintech, por sí sola, no es suficiente para garantizar un uso seguro y no delictivo de las criptomonedas.

Las criptomonedas han figurado recientemente en el centro de ostentosos titulares, transformado a nerds en millonarios y sido calificadas por numerosos economistas como una burbuja financiera a punto de colapsar. En este contexto, el 9 de febrero de 2021, la Comisión para el Mercado Financiero (en adelante la "CMF") publicó un anteproyecto de ley titulado "Fintech en los Ámbitos del Mercado de Valores", el cual busca establecer un marco jurídico para los prestadores de servicios de financiamiento colectivo y otros modelos de negocios de tecnología financiera, incluyendo lo relacionado con las criptomonedas.

Sin embargo, la experiencia internacional ha demostrado, que la inscripción de las empresas dedicadas al Fintech no es suficiente para garantizar la seguridad de los usuarios de las criptomonedas, ni prevenir que estas sean empleadas en actividades delictivas.

En el presente artículo daremos algunas luces sobre estos problemas y aventuraremos algunas alternativas de solución al respecto.



¿QUÉ SON LAS CRIPTOMONEDAS?

Pese a lo que pudiera sugerir su nombre, las criptomonedas (incluido el Bitcoin) poseen una naturaleza completamente distinta a las monedas reales en circulación: no tienen existencia física, no cuentan con reconocimiento ni aceptación general como medio de pago y poseen un valor esencialmente variable. En realidad, se trata de activos digitales basados en criptografía, creados con plena independencia de instituciones estatales, administrados de manera distribuida por los mismos usuarios en lugar de una autoridad central, y donde sus titulares pueden transferirlas de manera pseudoanónima. Esto último significa que los traspasos de criptomonedas son registrados únicamente con los números de cuenta del emisor y receptor, los que no están asociados a un nombre ni vinculadas a la identidad de personas en el mundo real.

Las características inherentes de las criptomonedas las han convertido en atractivas alternativas de inversión para los entendidos. Recientemente, la capitalización de mercado del Bitcoin alcanzó el billón de dólares en mayo de 2021 (para referencia, el PIB de Chile alcanzó en 2019 menos de un tercio de esa cifra: 282 mil millones de dólares). Considerando lo anterior, las criptomonedas constituyen un fenómeno financiero relevante, respecto del cual la ciudadanía aún ha tomado poca conciencia, particularmente en cuanto a sus aspectos más oscuros.

Dr. Francisco Bedecarratz Scholz
Observatorio de Ciberseguridad
Universidad Autónoma de Chile

¿CUÁL ES SU **POTENCIAL DELICTIVO**?

La relevancia actual de las criptomonedas como alternativa de inversión ha puesto en la sombra su preponderancia en la escena delictiva. Esto último dice relación con su aptitud para ocultar o disimular el origen de fondos adquiridos ilícitamente. Dicha característica obedece a la naturaleza pseudoanónima de las transferencias de criptomonedas, las cuales son realizadas al margen del Estado o de instituciones reguladas. Lo anterior permite realizar traspasos de activos involucrados en actividades ilícitas, incluso de manera transfronteriza, y sin ninguna limitante.

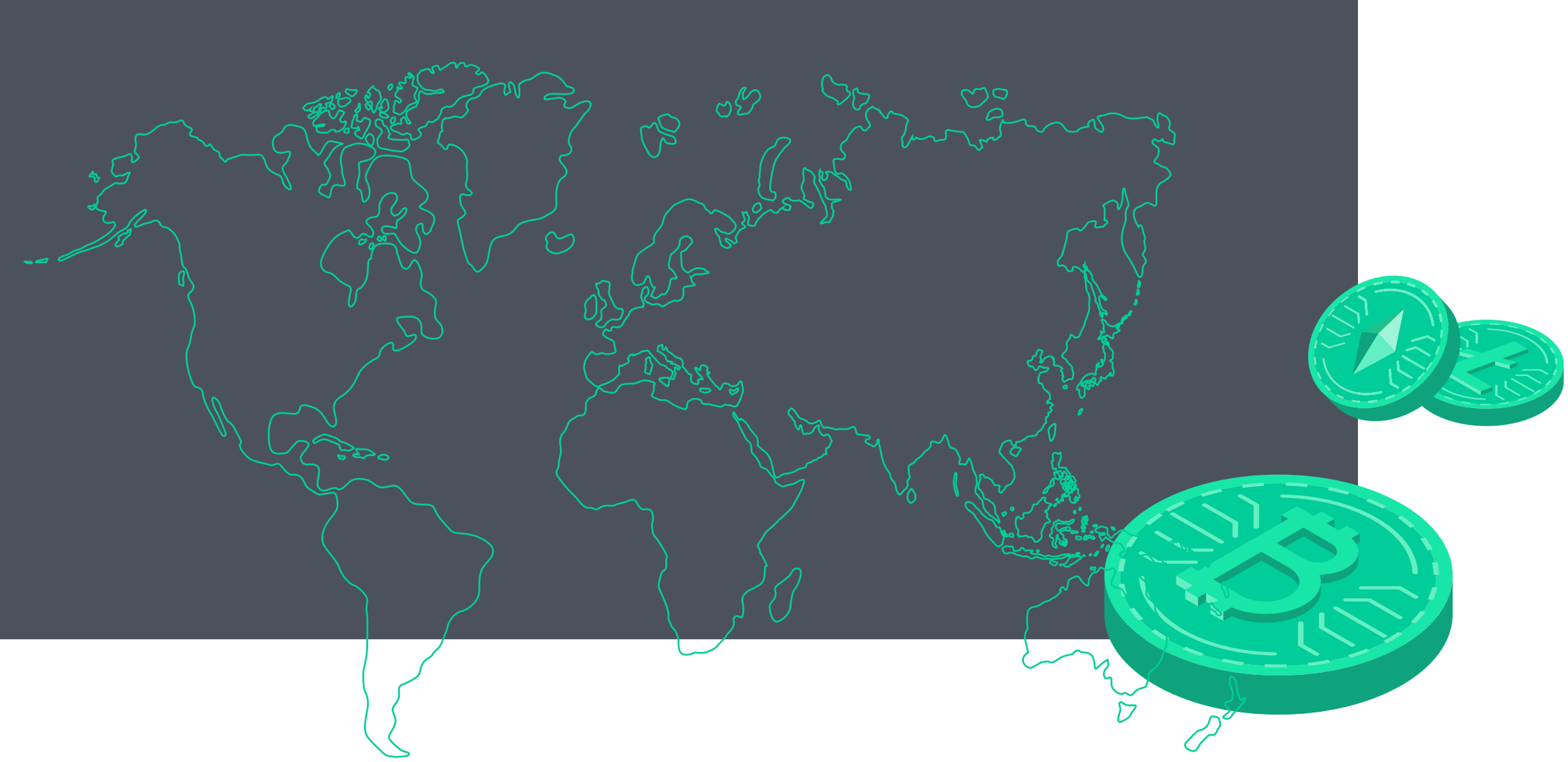
A propósito de esto, las criptomonedas se han transformado en un medio de pago preferente en la Dark Web para la adquisición de objetos calificados como ilícitos, tales como drogas, armas, bases de datos personales, pornografía infantil, o bien la contratación de servicios delictuales tales como sicarios. Un evento reciente es prueba de lo anterior: en enero de 2021 fue capturado en Alemania el administrador y confiscados los servidores del sitio "DarkMarket", un mercado digital destinado al comercio de drogas, datos de tarjetas de crédito, tarjetas SIM anónimas y software malicioso. Según la Fiscalía alemana, en los más de 320.000 negocios desarrollados a través del sitio, fueron traspasados más de 4.650 Bitcoin y 12.800 Monero, con un valor que supera los más de 140 millones de Euro. Así, quien realiza negocios ilícitos en la Dark Web, realiza comúnmente su pago en Bitcoin para no ser rastreado.

Las criptomonedas también prestan utilidad como vía de pago en caso de ataques tipo ransomware, es decir, programas maliciosos que bloquean el acceso o el funcionamiento normal de sistemas informáticos, unidos a la posibilidad de un rescate como precio para restablecerlos. Dicho modus operandi ha adquirido relevancia actual en el contexto del ciberataque efectuado al oleoducto "Colonial Pipeline", que abastece al sureste de los Estados Unidos. El ataque generó una interrupción del suministro de combustible, y la empresa administradora fue obligada a pagar un rescate consistente en 75 Bitcoin (a la fecha equivalentes a 5 millones de dólares aproximadamente), con el objeto de desbloquear los sistemas y restablecer el servicio.

En síntesis, las criptomonedas constituyen una forma relevante de traspasar fondos vinculados con actividades ilícitas, que de otra forma serían interceptados a través de los controles del sistema bancario formal, lo cual las convierte en una herramienta ideal para el lavado de activos. La consiguiente dificultad en el esclarecimiento de los responsables de delitos, impide su efectiva persecución penal y consiguiente prevención de otros hechos delictivos a futuro.

¿QUÉ RIESGOS CONLLEVAN **PARA LOS USUARIOS**?

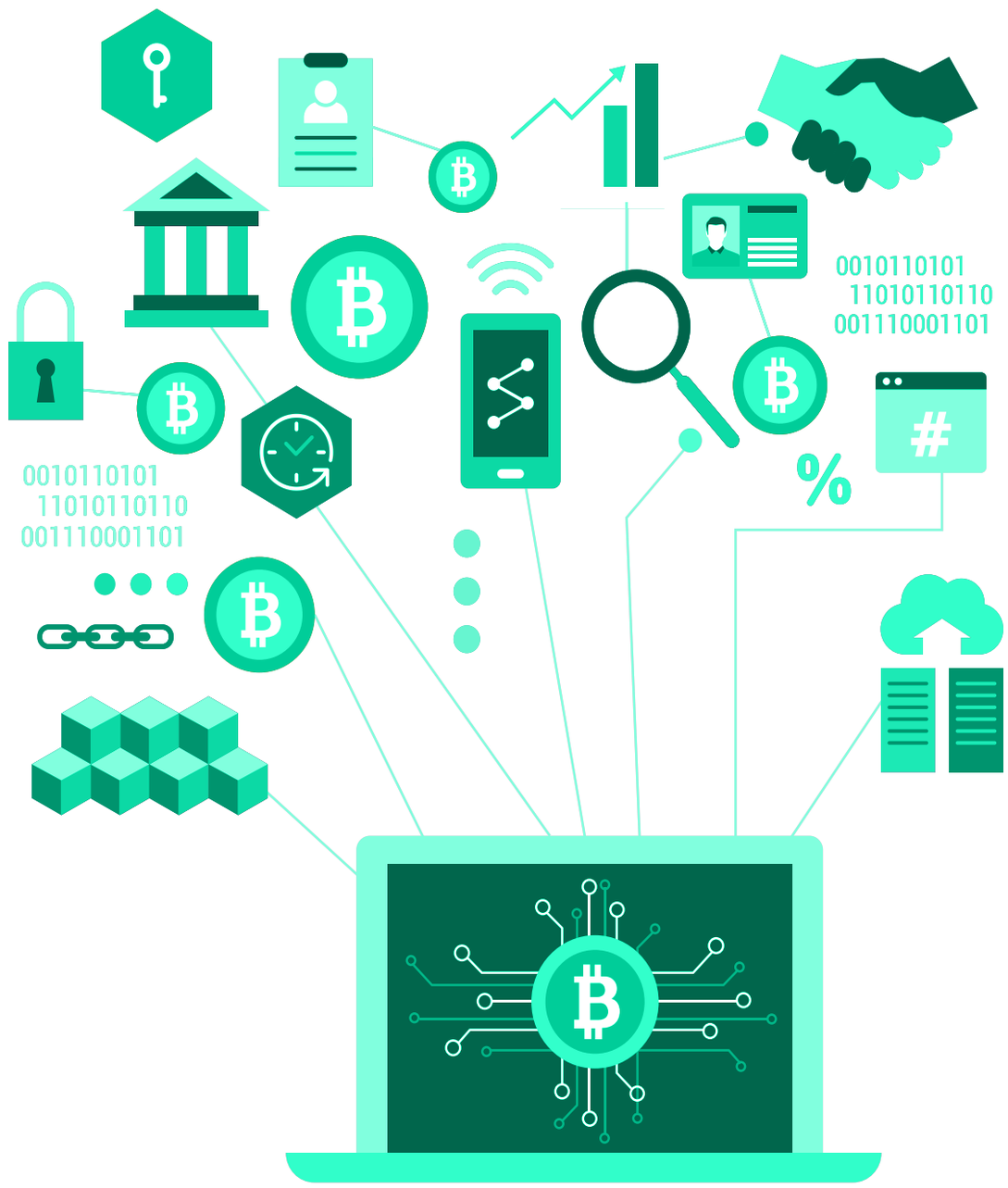
Al igual que en las demás inversiones, la adquisición de criptomonedas debe ser precedida de una investigación cuidadosa, expresión de la debida diligencia previa al inicio de todo nuevo negocio. Sin embargo, la tarea antedicha es especialmente compleja en este contexto. No solo se trata de un activo con una arquitectura compleja, sino que opera al interior de un ecosistema separado del financiero, con actores nuevos y generalmente desregulados. Ello implica una mayor exposición de los usuarios legítimos de criptomonedas, a ser víctimas de actividades delictivas al momento de adquirirlas o transferirlas.



El mayor riesgo lo constituyen los actores no regulados de la industria, que pueden realizar estafas masivas a los usuarios y apropiarse de los fondos. Ello ha ocurrido con ofertas iniciales de moneda (ICO), en las que se ofrece comprar unidades futuras de una criptomoneda nueva, bajo promesa de ser materializadas en cuanto el proyecto sea lanzado. En muchos casos ello finalmente no ocurre, defraudándose a los particulares y generando una pérdida total de los montos invertidos. Por otro lado, casas de cambio de criptomonedas que administran las cuentas de usuarios pueden alegar problemas de operación y suspender temporalmente los servicios, lo cual les da tiempo para apropiarse de los activos invertidos y generar una pérdida masiva de fondos a las víctimas.

Lo anterior se suma a los engaños ya conocidos en la banca en línea. Estos pueden asumir la forma de sitios web falsos con apariencia de ser un mercado de criptomonedas, diseñados para que las víctimas les transfieran sus fondos bajo la creencia errada de estarlas adquiriendo (pharming). O bien correos fraudulentos- que solicitan el envío de las claves de los monederos de Bitcoin, bajo el pretexto de, por ejemplo, realizar una devolución de impuestos o bien pagar un retiro de una AFP, pero en realidad entregándole el control del monedero y, con ello, perdiendo el dominio de los activos (phishing).

Los usuarios de estos activos, particularmente los más novicios, también pueden inadvertidamente ser autores de conductas ilícitas. Por ejemplo, el Servicio de Impuestos Internos ha definido el tratamiento tributario de las criptomonedas (Oficio N°963, de 14.05.2018) aclarando, entre otros, que las rentas obtenidas en la compra y venta de dichos activos están afectas a los impuestos generales de la Ley de Impuesto a la Renta (de Primera Categoría, Global Complementario o Adicional, en su caso) conforme al art. 20 N° 5 de dicha ley. Luego, un propietario de criptomonedas, que a través de su compra y venta obtenga ganancias sustanciales y omita efectuar las declaraciones correspondientes, puede ser responsable del delito de evasión tributaria, según el art. 97 del Código Tributario.



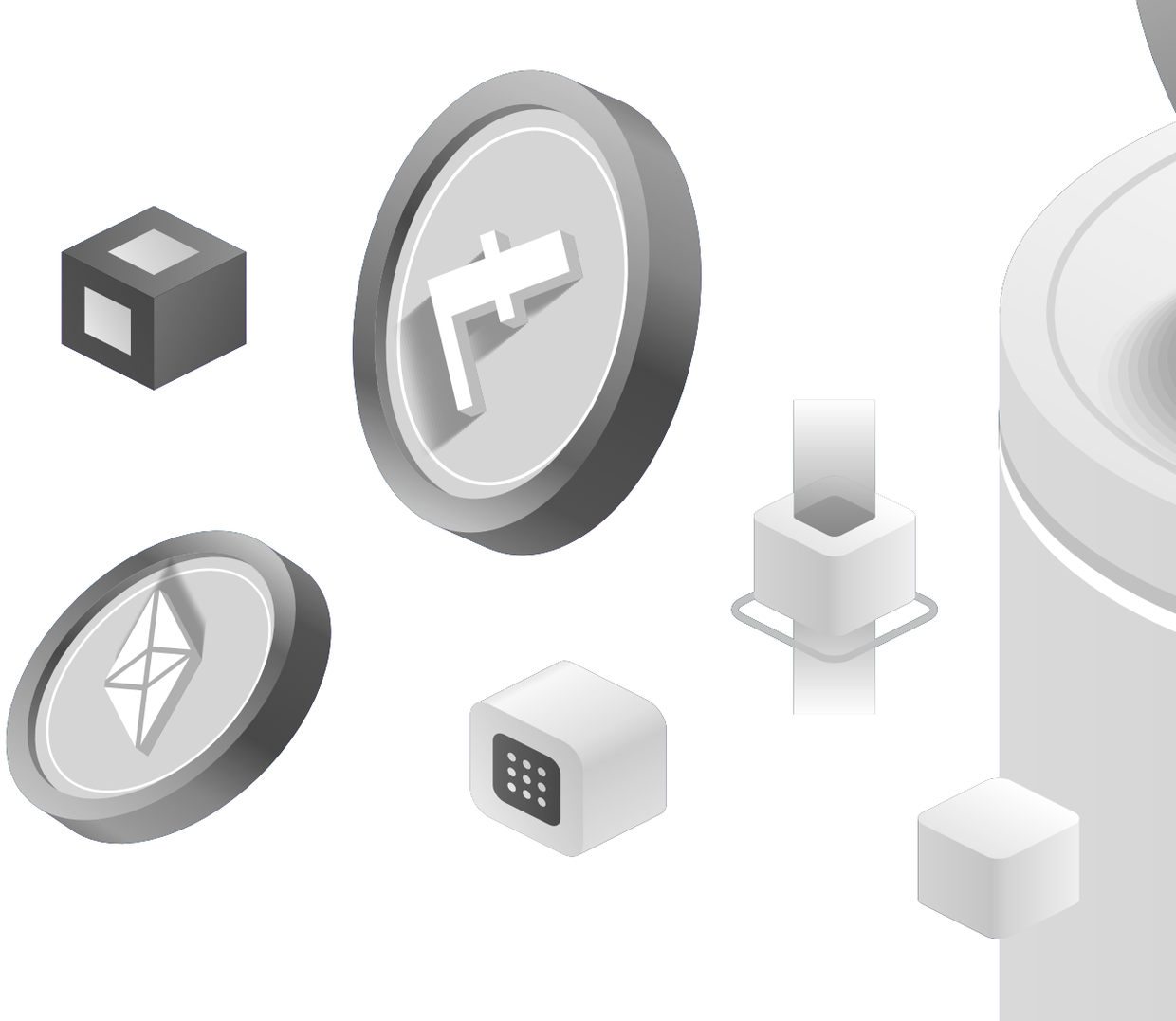
REGISTRO Y **MÁS ALLÁ**

Naturalmente, frente a un panorama lo más cercano al "lejano oeste" digital como el descrito, la introducción de una "Ley Fintech" puede generar las condiciones propicias para reducir el componente delictivo en el comercio con criptomonedas, juntamente con generar un ecosistema seguro para su desarrollo en Chile.

En esta misma línea, la propuesta de la CMF, junto con definir los alcances de las criptomonedas y reconocerlas como instrumento financiero (art. 2° lit. g), establece directamente la obligación de los prestadores de servicios definidos en la Ley, de inscribirse en el Registro de Prestadores de Servicios Financieros que llevará el ente (art. 4°). Lo anterior engloba a plataformas intermediadoras y prestadoras de servicios relacionados con criptomonedas. Ello puede contribuir efectivamente a disminuir el riesgo de fraudes, tales como las ICO fraudulentas, o la apropiación de los fondos por parte de prestadores de servicios de criptomonedas en contra de los usuarios.

Sin perjuicio de lo anterior, la disminución del riesgo de lavado de activos mediante esta clase de instrumentos requiere de medidas adicionales. De acuerdo con la experiencia internacional, ello puede lograrse a través de una especificación de las obligaciones a ser cumplidas por los proveedores. Ya hemos indicado que los traspasos de criptomonedas, particularmente del Bitcoin, se realizan de manera pseudoanónima. Ello se traduce en que cada transacción de la criptomoneda queda registrada en la cadena de bloques mediante el identificador alfanumérico del monedero desde el cual se emite la orden y del que la recibe. En ese entendido, es posible seguir el rastro de los autores de las transacciones, en la medida que se obligue a los prestadores de servicios de criptomonedas a cumplir con deberes de identificación de clientes. Ello se realizó en Japón, donde Ley para la Prevención de Transferencia de Ganancias Delictuales fue modificada el 1° de abril del 2017, para exigir a los proveedores de criptomonedas implementar políticas de identificación de clientes nuevos y mantener registros de los mismos. En el mismo sentido ha transitado la Quinta Directiva de Lavado de Activos de la Unión Europea (Directiva (UE) 2018/843, del 30 de mayo de 2018).

Por lo tanto, estimamos que debe avanzarse en dirección a que cualquier transferencia sospechosa que se realice desde y hacia Chile pueda ser rastreada, lo cual podría permitir, por ejemplo, identificar a sujetos que intenten mover ganancias producto del narcotráfico desde y hacia el extranjero. Dichas medidas deben ser complementadas con cooperación internacional, con el fin de coordinar el trabajo de esclarecimiento de transacciones con reguladores extranjeros y evitar que nuestro país sea usado como plataforma de transferencia de activos obtenidos ilícitamente. De tal forma, será posible contribuir a un ecosistema seguro para el uso de las monedas virtuales en Chile, así como garantizar el desarrollo de esta importante tecnología.



CSIRT

Equipo de Respuesta ante Incidentes
de Seguridad Informática

CSIRT
https://www.csirt.gob.cl/

Teatinos 92 piso 6
Santiago, Chile

CONTÁCTANOS

+(562) 2486 3850

registra un incidente

Síguenos

Twitter de CSIRT
https://twitter.com/csirtgob/

LinkedIn
https://www.linkedin.com/company/csirt-gob/

Youtube
https://www.youtube.com/channel/UCua0E5Jz9V1Rn-VtLHPP4Nw/

Instagram
https://www.instagram.com/csirtgobcl

Ministerio del Interior y Seguridad Pública

Gobierno de Chile

CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

Teatinos 92 piso 6
Santiago, Chile
www.csirt.gob.cl