

XIX Jornadas de  
Comunicaciones  
Científicas de la Facultad  
de Derecho y Ciencias  
Sociales y Políticas

UNNE

2023

*En homenaje a la Dra. Hilda Zulema Zárate*

Corrientes - Argentina

XIX Jornadas de Comunicaciones Científicas de la Facultad de Derecho y Ciencias Sociales y Políticas: UNNE / Silvia Alegre... [et al.]; compilación de Martín Chalup; Lucía Sbardella; dirigido por Mario R. Villegas. - 1a ed. compendiada. - Corrientes:

Universidad Nacional del Nordeste. Facultad de Derecho y Ciencias Sociales y Políticas, 2023.

Libro digital, PDF

Archivo Digital: descarga y online  
ISBN 978-987-3619-94-6

1. Derecho. I. Alegre, Silvia. II. Chalup, Martín, comp. III. Sbardella, Lucía, comp. IV. Villegas, Mario R., dir.  
CDD 340.072

# LAS CRIPTOMONEDAS Y EN ESPECIAL EL BITCOIN, ¿SON UN NUEVO OBJETO E INSTRUMENTO DE DELITOS? ¿EXISTEN RESPUESTAS ADECUADAS EN EL ORDENAMIENTO JURÍDICO?

Ferrer Alvarez Filizzola, Ivonne B. de las M.

*Ivonne-ferrer@live.com*

## RESUMEN

El uso de las criptomonedas es cada vez más frecuente. Los rasgos beneficiosos de las transacciones comerciales con criptoactivos, los erigen como instrumentos propicios para la comisión de delitos. La inexistencia de órganos de contralor y la falta de legislación específica que regule su uso son algunos de los déficits que existen para detectar operaciones sospechosas dentro de este mercado. Por ello, la introducción de sujetos que reporten operaciones sospechosas, la capacitación de los operadores jurídicos y la dotación de tecnología adecuada, son algunas de las propuestas para detectar operaciones ilegales. De lo contrario, el entramado normativo construido para luchar contra el blanqueo de dinero, el financiamiento del terrorismo, y otras figuras delictivas, devienen ineficaces.

## PALABRAS CLAVES

Criptoactivos, Herramientas, Ilícitos.

## INTRODUCCIÓN

Al margen de los usos legítimos que puede darse a las criptomonedas, las nuevas tecnologías también pueden ser empleadas en el ámbito delictivo, específicamente en el ámbito del blanqueo de dinero, la defraudación tributaria, medio de pago en el narcotráfico, en las extorsiones, entre otros usos ilícitos. Todos atraídos por el anonimato, la rapidez, la no presencialidad y la transnacionalidad de las transacciones.

En los últimos años, la política antiblanqueo se centró en los bancos multinacionales como puntos centralizados para reportar actividades sospechosas, quedando al margen los sistemas de virtuales descentralizados.

Asimismo, la rapidez de las transacciones en monedas virtuales, señalada como una ventaja, no lo es, ya que, si bien para tener por confirmada una transacción en cripto, deben cerrarse un número mínimo de bloques, la misma queda confirmada en un tiempo muy

acotado. Lo que, sumado al anonimato de las transacciones y de sus titulares, genera el fracaso de la actividad preventiva de monitoreo de actividades sospechosas, sobre todo pensando en su posible bloqueo, así como de la posterior persecución policial.

El problema de las direcciones de IP utilizadas en las transacciones, es que no proporcionan la identificación de los participantes reales ni generan registros del historial asociados a personas o entidades concretas, y aunque la estructura de cadena de bloques, es lo que le da cierta trazabilidad a las transacciones, ello no implica la identificación de los usuarios, afectando las medidas antiblanqueo que vinculan al actor con la operación sospechosa, así como su decomiso.

Por ello, como no hay un órgano de control centralizado, surge la necesidad de incluir sujetos que reporten operaciones sospechosas, y aunque ya existen desarrollos

informáticos que permiten cierto monitoreo e identificación de sujetos y transacciones sospechosas, se produjo evolución mucho más rápida y creciente de las tecnologías base que permiten oscurecer la actividad. Argentina, carece de regulación sobre la materia, únicamente se halla la Resolución N° 300/2014, adoptada por la Unidad de Información Financiera, que obedeció a las pautas elaboradas por el GAFI, que impuso la obligación a determinados sujetos obligados ante la UIF a reportar las operaciones que se realicen con monedas virtuales y prestar atención al volumen de cada una de ellas. Y, además, se elaboraron al menos tres proyectos parlamentarios referidos al universo cripto, en los cuales la autoridad de aplicación es la CNV.

#### MÉTODOS

Se analizó: Ley 25.345, Resolución N° 300/14 de la UIF, Recomendaciones de GAFI, Proyectos existentes en materia de criptomonedas, en Argentina, Ley 14.905/72 de la República Oriental del Uruguay; Ley 27.411, que incorporó a la legislación Argentina el Convenio sobre Cibercriminación del Consejo de Europa. Y se utilizó los métodos: a- Tipo de Estudio: Exploratorio, descriptivo y comparativo; b- Método: Deductivo. Se buscó identificar las dificultades, en las transacciones con monedas virtuales, para la individualización de usuarios y el control de las operaciones. Para ello, se identificó las normas existentes en materia penal y fiscal sobre la materia; y formular propuestas, a partir de normas existentes en otros cuerpos normativos de otras provincias del país y/o de otros países, que permitan regular las transacciones en monedas virtuales, y controlar y monitorear las operaciones que resulten sospechosas.

#### RESULTADOS Y DISCUSIÓN

Este nuevo mercado, sin dudas trae grandes beneficios, ya que no sólo se reduce el costo de las transacciones porque se eliminan los

intermediarios, sino porque también genera mayor celeridad rapidez y fluidez en las transacciones. Pero también, aparece como caldo de cultivo propicio para que los cibercriminales proliferen en este ámbito, y es que, la criptomoneda es una moneda como cualquier otra, pero sin ningún respaldo legal, es decir, no se considera reconocida por ningún Estado, pero por medio de la misma se pueden adquirir bienes y servicios. Y son justamente dichas características, las que permiten que pueda ser empleada con fines lícitos o con fines ilícitos, ya que al no haber una entidad que autorice o regule las transacciones no es fácil controlar las operaciones realizadas en dicho marco.

Las criptodivisas están soportadas en un registro distribuido, no hay un órgano de control central, y ningún ente u organismo puede asumir el rol de supervisor centralizado. Por lo tanto, si se quiere intentar algún tipo de seguimiento y control de las transacciones realizadas con ellas, surge como opción la introducción de nuevos sujetos que reporten operaciones sospechosas. De lo contrario, todo el entramado normativo construido para la lucha contra el blanqueo de dinero, evitar el financiamiento del terrorismo, y otras figuras delictivas que puedan concretarse en este marco, pueden devenir ineficaces.

Y, aunque ya existen desarrollos informáticos que permiten cierto monitoreo e identificación de sujetos y transacciones sospechosas, lo cierto es que las tecnologías base evolucionaron mucho más, permitiendo oscurecer aún más la actividad.

De esta manera, si bien, hay diferentes sistemas que operan en la blockchain cuya finalidad es detectar patrones de operaciones sospechosas que se efectúan allí dentro, para que ello sea posible, "la única forma de llegar a la identidad que está detrás es a través de un análisis eficiente de la blockchain y para acceder y conocerla hay que crear los mismos sistemas que

permiten operar en ella”, lo cual requiere entonces no solo de una mayor capacitación del Ministerio Público Fiscal, de modo de que sus colaboradores puedan comprender cabalmente todo el funcionamiento de la blockchain y de las criptomonedas, sino también es necesario que la Fiscalía u otros órganos que se dediquen al contralor y ciberpatrullaje de las transacciones con criptomonedas, pueda contar con las herramientas adecuadas, sistema, velocidad de navegación etc. De lo contrario intentar identificar o rastrear a ciberdelincuentes sería como buscar una aguja en un pajar. Sin embargo, en mi opinión, si bien aún no existe un acuerdo generalizado en el mundo acerca de cómo controlar y cómo y qué regular de estas transacciones, que día a día crecen de manera exponencial, considero que existe una eficaz herramienta que actualmente ya se aplica en los ciberdelitos vinculados especialmente al delito de pornografía infantil, que podría tomarse de ejemplo. Así, a partir de una iniciativa de la ONG americana NCMEC (Centro Nacional para Niños Desaparecidos y Explotados) empresas como Facebook, Microsoft, Google, están obligadas a reportar cualquier actividad sospechosa en Estados Unidos; lo que luego, a partir de los convenios celebrados con aquellos países del mundo donde la explotación sexual infantil es delito, también se ha extendido la protección a ellos, debiendo reportar cualquier actividad sospechosa de dicha índole, que se detecte como ocurriendo en alguno de dichas jurisdicciones. De esta forma, considero propicio que al igual que sucede para la persecución de la explotación sexual infantil, se pudiera establecerse una entidad capaz de realizar una especie de ciberpatrullaje, a fin de detectar cualquier transacción sospechosa, para lo cual se deberá contar con toda la capacitación y tecnología adecuada, a fin de escarbar en el mundo de las transacciones cripto, e incluso

bucear en la llamada deep web. Pero también se deberá contar con la colaboración de los llamados nodos o mineros, que son quienes en realidad realizan el trabajo de la intermediación para la concreción de las transacciones en cripto; y también con la colaboración de los llamados exchangers, que son los que actúan como puente entre lo virtual y lo real, entre el anonimato y la tangibilidad, aun cuando estos en definitiva no sean poseedores de dichos activos sino meros intermediarios o cambiadores de moneda virtuales (exchangers). Para lo cual, deberán ser incluidos como sujetos obligados al reporte de operaciones sospechosas, todo lo cual requiere una toma de decisión concreta a fin de regular adecuadamente este fenómeno y una inversión adecuada a los requerimientos tecnológicos. Sin dudas, el desafío es adaptarse y conocer adecuadamente este nuevo mercado para poder perseguir a aquellos que se valen de la informalidad y el anonimato para cometer delitos con mayor impunidad.

#### REFERENCIAS BIBLIOGRÁFICAS

- Administración Federal de Ingresos Públicos. (2023). *Unidad de Información Financiera*. <https://www.afip.gob.ar/lavado/unidad-de-informacion-financiera/default.asp>
- Aranguéz Sánchez, C. (2020). El Bitcoin como instrumento y objeto de delitos en *Cuadernos de Política Criminal*, (pp. 75-104.) Segunda Época.
- Bank Magazine. (12 de noviembre de 2020). *Proyecto de regulación de Criptomonedas en Argentina* <https://www.bankmagazine.com.ar/proyecto-de-regulacion-de-criptomonedas-en-argentina/#:~:text=La%20%C3%A1mara%20de%20Diputados%20de%20la%20N>

- aci%C3%B3n%20ya,p%C3%BAlicas%2C%20residentes%20en%20el%20pa%C3%ADs%20o%20el%20exterior.
- Brezo Fernández, F.; Rubio Viñuela, Y. (2017). *Bitcoin. La tecnología Blockchain y su investigación*. Zeroxword computing.
- Cámara de Diputados de la Nación. (s.f.). <https://www4.hcdn.gob.ar/dependencias/dsecretaria/Periodo2020/PDF2020/TP2020/6055-D-2020.pdf>
- GAFI. (junio de 2015). Recuperado el junio 2019, de <http://www.cfatf-gafic.org/>
- González- Menses Robles, M. (2019). *Entender blockchain. Una introducción a la tecnología de registro distribuido*. Thomson Reuters Aranzadi.
- Lambert, H. (8 de septiembre de 2022.). *Criptomonedas, el nuevo paraíso fiscal para el lavado de dinero. Pandasecurity*. [https://www.pandasecurity.com/es/mediacenter/tecnologia/cryptomonedas-lavado-dinero/?gclid=CjwKCAiA2L-dBhACEiwAu8Q9YCIMLUxO8-bvbyWknuaE09HCbJOyJgNIMvsqwZnadGbcY-HdF8chMhoC42QQAvD\\_BwE](https://www.pandasecurity.com/es/mediacenter/tecnologia/cryptomonedas-lavado-dinero/?gclid=CjwKCAiA2L-dBhACEiwAu8Q9YCIMLUxO8-bvbyWknuaE09HCbJOyJgNIMvsqwZnadGbcY-HdF8chMhoC42QQAvD_BwE)
- Linares, M. B. (11 de julio de 2019). *Criptomonedas y lavado de activos*. Derecho al día. <http://www.derecho.uba.ar/derechoaldia/notas/cryptomonedas-y-lavado-de-activos/+7603>
- Navarro Cardoso, F. (2019). *Criptomonedas (en especial bitcoin) y blanqueo de dinero. Revista Electrónica de Ciencia Penal y Criminología, 21*.
- Santillan, Francisco G. y Sarquis, A. (2020). *Criptomonedas: un desafío inminente del Derecho Penal*. Rubizal Culzoni.
- Silvera Mendez, C. (2020). *Los desafíos ante la presencia de nuevos bienes jurídicos con especial atención en las criptomonedas*. Thomson Reuters.
- Skalany, E. G. (2019). "Criptomonedas" y Derecho Penal en Argentina. Introducción a la "blockchain", el "bitcoin" y más allá. *Revista de Derecho Penal, 2*, pp. 1574-2020.
- Vanella, C. A. (septiembre de 2021). Los avatares del negocio con criptomonedas y el peligro de estafa. *Erreius online*. <https://idcar.com.ar/wp-content/uploads/2022/09/Vanella-Carolina-A.-Los-avatares-del-negocio-con-cryptomonedas-y-el-peligro-de-estafa.pdf>
- Viña, G. A. (2021). Los criptoactivos a la luz del derecho argentino: estado de la situación ante incipientes desafíos. Primera parte. *El Derecho, 9*. <https://idcar.com.ar/wp-content/uploads/2022/09/Vina-Gonzalo-Ariel-Los-criptoactivos-a-la-luz-del-derecho-argentino-estado-de-la-situacion-ante-incipientes-desafios.pdf>
- Viña, G. A. (2021). Los criptoactivos a la luz del Derecho Argentino: Estado de situación ante incipientes desafíos. Segunda Parte. *El Derecho*. <https://idcar.com.ar/wp-content/uploads/2022/09/Vina-Gonzalo-Ariel-Los-criptoactivos-a-la-luz-del-derecho-argentino-estado-de-la-situacion-ante-incipientes-desafios.pdf>

EJE TEMÁTICO DE LA  
COMUNICACIÓN  
Derecho Y Nuevas Tecnologías

FILIACIÓN

AUTOR 1: Docente - Trabajo libre de  
cátedra