

Cuadernos sobre Criminalidad Económica 3

Criptoactivos

CEI EDICIONES UNR

UNR

Cuadernos sobre criminalidad económica 3: Criptoactivos / Laureano Gabriel Brufal ... [et al.]; Compilación de Marina Beatriz Marsili; Narvaja Sebastián R.; Prólogo de Hernán Blanco. - 1a ed. - Rosario: CEI ediciones, 2026.
Libro digital, PDF
Archivo Digital: descarga y online
ISBN 978-631-92038-3-7
1. Delitos Económicos. 2. Criptomonedas. 3. Legislación. I. Brufal, Laureano Gabriel II. Marsili, Marina Beatriz, comp. III. Sebastián R., Narvaja, comp. IV. Hernán Blanco, prolog.
CDD 330

Editor: Lautaro Sappietro
Imagen de tapa creada con inteligencia artificial por Sebastián Narvaja
Diseño de tapa: Cintia Espinosa
Diseño y maquetación: Cintia Corestein
Tipografía: *Saira*, Gatti & Omnibus-Type Team

Sebastián Narvaja y Marina Marsili
Universidad Nacional de Rosario, 2026
Hecho el depósito que marca la ley 11.723

Publicado bajo licencia Creative Commons

Edición y publicación Centro de Estudios Interdisciplinarios, UNR
Director: Prof. Darío Maiorana
Maipú 1065 3° piso of 309, Rosario, Argentina
Tel: (0341) 4802781
Correo electrónico: cei@unr.edu.ar

CENTRO DE ESTUDIOS INTERDISCIPLINARIOS

UNR Universidad Nacional de Rosario

PROGRAMA DE ESTUDIOS INTERDISCIPLINARIOS SOBRE PREVENCIÓN Y PERSECUCIÓN DE LA CRIMINALIDAD ECONÓMICA

- ECOCRIM -

Directores

Sebastián R. Narvaja y Marina B. Marsili

ECO CRIM
Programa de Estudios Interdisciplinarios sobre Prevención y Persecución de la Criminalidad Económica

CUADERNOS SOBRE CRIMINALIDAD ECONÓMICA 3

Índice

Prólogo 7
Hernán Blanco

Introducción 13
Lautaro Sappietro

Cuando la tecnología cambia el mundo del crimen 33
Laureano Brufal y Paula Ronco

Estudio del caso "Lazarte Di Lieto" desde una perspectiva de análisis económico forense en un contexto signado por el uso masivo de criptomonedas en Argentina 51
Walter R. Chiquiar y Lucas Paulinovich

La Criminalidad Económica de Edgar A. Bacchiani y Adhemar Capital SRL 76
Maximiliano Fernández y Lorena Beatriz Varas

El delito de estafa en el ecosistema de los activos virtuales: la modalidad rug pull y el caso $LIBRA en Argentina 97
Ignacio Chiarenza y Manuela Belén Losada

Desafíos de la persecución penal estratégica en materia de criptoactivos. Un Análisis FODA (fortalezas, oportunidades, debilidades y amenazas) 115
Elia Bollecich Masters

Regulación de los PSAV en Argentina: avances formales y desafíos 132
María Alejandra Freire

Fiscalidad internacional de criptoactivos: panorama actual, desafíos normativos y perspectivas 152
Antonella Gervagi y Ana Laura Jaruf

Abordaje del aspecto contable e impositivo de los criptoactivos 173
Jésica Nicol Luisi y Martín Regalini

Stablecoins bajo la lupa: concepto, clasificación y el nuevo orden regulatorio internacional 186
Augusto Lombardo y Nicolás Maletti

No es disrupción, es adaptación: tensiones del ecosistema cripto en Argentina 216
Carlos Emanuel Monzón

Prólogo

Es un orgullo para mí haber recibió la invitación para prologar esta nueva edición de los *Cuadernos sobre criminalidad económica.* Más allá de remarcar que la temática que liga entre sí a todos los trabajos de este número —la confluencia entre las nuevas tecnologías, los delitos económicos y su investigación— resulta de enorme interés y candente actualidad, lo que quiero comenzar destacando es el propósito general que, como se advierte fácilmente, anima estos cuadernos, que es fomentar el análisis académico y científico de cuestiones que hacen al Derecho penal y la problemática de su aplicación en la realidad, pero siempre *orientado a contribuir a la práctica concreta de los operadores del sistema de justicia*.

Celebro esta decisión que apunta a cerrar la que, quizás, sea la principal "grieta" vinculada al Derecho penal y su implementación, que no es la política a la que tanto se alude en la Argentina, sino una de la que se habla poco, pero que persiste desde hace muchos años. Se trata de la que divide a la "teoría" de la "práctica" en materia penal, ubicando en una vereda a los "académicos" del Derecho -con su dogmática penal y su defensa de las garantías constitucionales- y, en la opuesta, a los operadores del sistema judicial encargados de aplicar ese Derecho en la práctica; y que no remite aun a pesar de la cantidad de penalistas que cumplen ambos roles.

Esta dicotomía genera un enorme perjuicio al Derecho penal. Sus efectos se sienten tanto en la elaboración de las normas penales como en su aplicación. De un lado, la renuencia de muchos juristas a hacerse cargo de las preocupaciones de la sociedad (para la que la inseguridad, la corrupción y lo que se percibe como una ausencia de respuestas útiles por parte de la justicia vienen siendo temas prioritarios desde hace muchos años) e involucrarse en la discusión sobre potenciales reformas a la ley penal. Esta actitud ha dado lugar a la aguda crítica de Diez Ripollés a lo que denomina el "inmovilismo" de los defensores del garantismo penal, que considera fundada en

el "olímpico desprecio" de ese sector ideológico hacia todo lo que suponga abandonar "el cómodo hogar de los principios" (evidenciado en el descuido de las aproximaciones empíricas a la realidad del delito y a su capacidad para ignorar ciertas realidades que contradicen sus orientaciones político-criminales), cuyo principal efecto es permitir que la discusión sobre potenciales modificaciones al Derecho penal sea monopolizada por quienes se autoarrogan la representación de los "ciudadanos de bien" y descartan cualquier objeción a la demagogia punitivista, aludiendo peyorativamente al "garantismo".

La misma renuencia se advierte en muchos operadores del sistema de justicia, que se resisten a adoptar un enfoque sistemático en la aplicación del Derecho penal -apoyado en herramientas científicas como la dogmática penal en general o la imputación objetiva en particular-, en aras de asegurarse la posibilidad de diseñar soluciones ad hoc para cada caso concreto, sin reparar en si las mismas se contradicen, o no, entre sí o en si están haciendo, en la práctica diaria, lo contrario a lo que enseñan en los claustros.

Esta "grieta" tiene origen, a mi modo de ver, en el olvido de una cuestión fundamental, que debiera ser central en el pensamiento de unos y otros. Esto es: que *el Derecho penal no es una ciencia abstracta o teórica, sino una cuya finalidad esencial, desde el principio, es ser aplicada en la realidad*, atendiendo a conflictos sociales concretos de los ciudadanos. De allí, que el verdadero propósito de la teoría de la imputación objetiva sea gobernar el juicio de subsunción de acciones u omisiones concretas, y no adornar decisiones judiciales, dictámenes o recursos con citas de autores prestigiosos; y que el objetivo del análisis sobre el alcance de las garantías constitucionales en el marco del Derecho penal no sea otorgar contenido a proclamas altisonantes, sino procurar encontrar el balance más justo entre los derechos de los ciudadanos y el interés del Estado en prevenir y/o castigar los delitos (en cumplimiento de la parte que le toca en el pacto social, que es defender la seguridad de aquellos ciudadanos). En sentido opuesto, recordar siempre que tanto el Derecho penal como el Derecho procesal penal son, ante todo, una ciencia orientada a la práctica permite entender que cuando una determinada teoría o doctrina deja de ser de utilidad en la realidad social concreta en que debe ser aplicada, la misma es susceptible de ser abandonada o revisada; como así también que la aplicación del Derecho penal sin anclaje alguno en el método

científico, por parte de los operadores del sistema judicial, conspira contra la seguridad jurídica, abre paso a la arbitrariedad y contribuye a alimentar la percepción negativa que la sociedad tiene de la justicia.

En este escenario, publicaciones como estos *Cuadernos sobre criminalidad económica* constituyen un paso importante en la dirección correcta, en la medida en que apuntan a analizar los interrogantes que la evolución de la sociedad le plantea al Derecho penal y al modo en que es aplicado, e intenta aportar soluciones que den respuesta a dichos interrogantes. Esto es fundamental en un contexto en el que la velocidad en que se producen los cambios sociales, económicos y -sobre todo- tecnológicos se ha incrementado dramáticamente, poniendo a prueba la capacidad de legisladores, académicos y operadores del sistema judicial para adaptar las leyes, las doctrinas, las políticas criminales y las herramientas a una realidad en continua transformación.

En cuanto atañe a la criminalidad económica, objeto principal de estos cuadernos, casi nadie discute ya que, desde hace varios años, los fenómenos (estrechamente conectados entre sí) de la criminalidad organizada y la criminalidad "de empresa" siembran dudas sobre la vigencia del paradigma "Derecho penal nuclear" y los principios emanados del Iluminismo, todos ellos producto de una época radicalmente diferente a la que nos toca vivir, en la que las agencias de orden público se enfrentan en ocasiones a organizaciones criminales (o a empresas multinacionales) cuyo poder rivaliza con el del propio Estado; en el que la actividad criminal se proyecta más allá de las fronteras y puede tener un alcance global; y en el que el accionar de los grupos criminales remeda y se entrelaza con el de las grandes corporaciones. En este escenario, la máxima "*societas delinquere non potest*" ha pasado de ser (casi) indiscutida a minoritaria, y teorías apoyadas en la protección de intereses colectivos, como el "Derecho penal del riesgo" o la "responsabilidad penal por el producto" han cobrado una preponderancia impensada.

Debido a ello, la investigación criminal de delitos complejos —con el lavado de activos como supuesto emblemático— demanda hoy, a quienes la llevan adelante, conocimientos que no solo incluyen a los últimos desarrollos en materia de dogmática, sino que exceden largamente la esfera del Derecho penal para comprender cuestiones como el funcionamiento del mundo financiero, los sistemas de transferencia

internacional de pagos, los vehículos corporativos en los "refugios fiscales" y otras jurisdicciones, el modo en que funcionan los sectores de la economía vulnerables al blanqueo de capitales, nociones básicas de contabilidad o auditoría forense, etc. A lo que cabe añadir la necesidad de adaptarse también a los efectos de la vertiginosa evolución de las tecnologías de la información y la comunicación (sobre todo en los últimos veinte años). Evolución que impacta tanto en la conducta de las sociedades modernas y el desarrollo de nuevas modalidades delictivas (por ejemplo, todas las vinculadas al fenómeno del "cibercrimen"), como en la aparición de nuevas estrategias y herramientas de investigación que, bien usadas, pueden incrementar en gran medida la eficiencia de las autoridades en la persecución de los nuevos delitos (y también de los tradicionales).

En efecto, se advierte que, por un lado, la consolidación de la Internet como la primera vía de comunicación a nivel mundial, así como la ubicuidad de los dispositivos informáticos como herramienta para la realización de la casi totalidad de las actividades humanas (trabajo, educación, comunicación, información, entretenimiento, etc.) ha dado origen a un nuevo ámbito para la comisión de delitos (el "ciberespacio") y al nacimiento de una nueva categoría de ilícitos (el "cibercrimen"). En esta dirección, y siguiendo la tendencia general de la sociedad de trasvasar gran parte de su actividad al mundo online (tendencia que se profundizó todavía más a partir de la pandemia global del Covid-19), una porción considerable de los delitos tradicionales (fraude, robo, extorsión, amenaza, explotación sexual) se trasladó al ámbito virtual, circunstancia que obligó a las agencias de orden público y los operadores del sistema judicial a seguir el mismo camino, trasladando sus investigaciones al ciberespacio.

En tal contexto, hay un conjunto de nuevos factores que no pueden ser soslayados. Entre ellos, el carácter eminentemente trasnacional y "despersonalizado" de los delitos "ciberdependientes" o "ciberasistidos"; las particulares características de la evidencia digital requerida (casi en exclusividad) para acreditar su comisión y fundar un reproche penal a sus respecto; el surgimiento de herramientas digitales con capacidad "anti forense" (como, por ejemplo, las que facilitan la navegación anónima en Internet o permiten el cifrado de las comunicaciones o de la información almacenada en dispositivos electrónicos) y de un ecosistema virtual que permite efectuar pagos o transferencias de

valores en todo el globo a espaldas del sistema financiero tradicional (el de los criptoactivos); así como la consolidación de nuevos modelos delictivos como el del "cibercrimen como servicio" (CaaS, por sus siglas en inglés). La combinación de estos elementos tiene el triple efecto de reducir las barreras de ingreso al delito, maximizar su capacidad de daño y dificultar su investigación (sobre todo, cuando se la lleva a cabo aplicando los modelos tradicionales de investigación, concebidos para pesquisas que se desarrollan en el mundo físico).

Sin embargo, es preciso reconocer también que, en la actualidad, la labor de los investigadores se ve favorecida por la disponibilidad de una variedad de herramientas tecnológicas de vigilancia y fuentes de información o evidencia (en su mayor parte digital) como nunca antes existió en la historia de la humanidad. De allí, que se aluda a nuestra era como la "edad de oro de la vigilancia", en base a cuestiones como el modelo económico de las grandes empresas tecnológicas —centrado en el minado y explotación de los datos privados de los usuarios para elaborar perfiles de clientes—; la ubicuidad de los "teléfonos inteligentes", en los que se concentra la casi totalidad de la información de sus usuarios (comunicaciones, contactos, fotos, búsquedas en Internet, datos históricos de localización, biométricos y de salud, etc.); la disponibilidad de herramientas de "big data", que permiten el entrecruzamiento y análisis de enormes volúmenes de información; la posibilidad de combinar herramientas de vigilancia miniaturizadas (cámaras, micrófonos, interceptadores del tráfico en Internet, etc.) con dispositivos como los drones o sistemas de identificación biométrica; y la consolidación del modelo de investigación centrado en la cooperación público privada, en cuyo marco los operadores del sistema de justicia o las agencias de orden público pueden contar con los servicios de empresas privadas con conocimientos especializados o herramientas tecnológicas avanzadas, como las que se dedican al análisis de la Blockchain en el ecosistema cripto.

En este escenario, los trabajos que integran la edición de los *Cuadernos sobre criminalidad económica* que me toca prologar interrogan a la realidad descripta en los párrafos precedentes. Sus autores exploran, desde diversos ángulos y perspectivas, muchas de las cuestiones que hacen a la persecución de delitos económicos en esta nueva coyuntura social, económica y tecnológica, con especial énfasis

en el funcionamiento del ecosistema de criptoactivos y el impacto de la inteligencia artificial, tanto en la comisión como en la investigación de los delitos económicos vinculados al ciberespacio.

Tomados en conjunto, estos trabajos constituyen un aporte de enorme valor, en especial por cuanto -como se adelantó- los une la idea de que la investigación académica resulte de utilidad para una gestión más rigurosa, sistematizada y —a la postre— eficaz de las funciones del sistema de justicia en la investigación y juzgamiento de los ilícitos que le toca perseguir. Los invito a disfrutarlos.

Hernán Blanco

Abogado
Secretario Letrado de la Corte Suprema de Justicia de la Nación
Especialista en Delitos Complejos

Introducción

Hacia una respuesta estratégica frente a la criminalidad económica en la era digital

Lautaro Sappietro[1]

El presente número de *Cuadernos sobre criminalidad económica* se publica en un momento de transformación sin precedentes para los sistemas de justicia penal y para las categorías fundamentales del derecho penal patrimonial. Nos encontramos ante un punto de inflexión donde la aceleración de las finanzas digitales, potenciada por la disrupción tecnológica que siguió a la pandemia de COVID-19, ha superado con creces la capacidad de respuesta de los marcos normativos tradicionales. Las instituciones diseñadas en el siglo XX para combatir delitos de cuello blanco convencionales se enfrentan hoy a fenómenos que operan en velocidades, escalas y geografías que desafían su arquitectura jurídica más básica.

La irrupción masiva de los criptoactivos y de la inteligencia artificial (IA) no solo ha rediseñado el ecosistema financiero global, sino que ha puesto en crisis las categorías fundamentales del derecho penal: la noción de «cosa» susceptible de apoderamiento, la territorialidad de la jurisdicción, los mecanismos tradicionales de prueba y la propia definición de sujeto obligado a reportar. La tecnología de registro distribuido (DLT) introduce una paradoja regulatoria: a mayor descentralización, menor es la capacidad del Estado de imponer controles,

1- Abogado egresado de la Universidad Nacional de Rosario. Profesor en Derecho por la Universidad Nacional de Rosario. Especialista en Magistratura UCA. Especialista en Criminología, Políticas de Seguridad y Justicia Penal por la Universidad Nacional del Litoral. Adscripto cátedra Derecho Procesal Penal UNR. Actualmente, se desempeña como Secretario interino de 1era Instancia y Auxiliar Fiscal Federal en el Ministerio Público Fiscal de la Nación.

pero también mayor es la trazabilidad teórica de las transacciones, un activo que la investigación forense aún no explota en toda su potencia.

En Argentina, este fenómeno adquiere una relevancia singular y urgente. La persistente inestabilidad monetaria, con tasas de inflación que en 2023 superaron el 211% anual (INDEC, 2024), y la histórica desconfianza hacia el sistema bancario formal han convertido a las criptomonedas en un refugio económico de adopción masiva. Según datos del Banco Mundial (2022), Argentina es uno de los países con mayor penetración de criptoactivos en América Latina, con aproximadamente un 12 % de la población adulta que ha utilizado o posee algún tipo de activo virtual. Esta adopción acelerada y mayormente informal constituye, al mismo tiempo, un vector de inclusión financiera y un campo fértil para estafas, maniobras de lavado de activos y evasión fiscal de escala sistémica.

Los artículos que integran este volumen no se limitan a describir casos de alto impacto público. Proponen, de manera más ambiciosa, un cambio de paradigma en la investigación penal estratégica: transitar de un enfoque reactivo y atomizado hacia una perspectiva sistémica e interdisciplinaria capaz de anticipar y desarticular estructuras criminales complejas. Como bien advierte Sutherland (1949) en su obra fundacional sobre la criminalidad de cuello blanco, cuya vigencia es hoy más pertinente que nunca, el delito económico no es un fenómeno marginal sino una amenaza central a la confianza en las instituciones y en el orden económico. Sus autores no son marginales sociales sino, frecuentemente, actores con acceso privilegiado a los mecanismos del sistema que defraudan. A continuación, me adentraré, intentando dar una pequeña imagen de cada artículo que compone este volumen imprescindible para comprender la criminalidad económica actual.

1. El nuevo ecosistema del crimen: criptoactivos e inteligencia artificial

La convergencia entre los activos virtuales y la inteligencia artificial define hoy la frontera más dinámica y peligrosa de la criminalidad económica compleja. El surgimiento del Bitcoin en 2008, concebido por el seudónimo Satoshi Nakamoto como respuesta directa a la crisis de las hipotecas subprime y a la desconfianza hacia los intermediarios

financieros institucionales (Nakamoto, 2008), introdujo conceptos radicales que reconfigurarían el paisaje del delito financiero: la descentralización, la inmutabilidad del registro, la seudoanonimidad y la operatividad transfronteriza sin regulación estatal.

El primer artículo de este volumen, de la autoría de Brufal y Ronco, "Cuando la tecnología cambia el mundo del crimen", proporciona el marco histórico y técnico indispensable para comprender esta transformación. Los autores trazan una línea de continuidad entre la criminalidad económica clásica y sus manifestaciones digitales, mostrando que la esencia del delito, la apropiación indebida de recursos ajenos permanece inalterada, aunque sus medios hayan mutado de forma radical. Desde el fraude contable de empresas como Enron hasta las maniobras de ofuscación en redes blockchain de segunda generación, el vector tecnológico actúa como multiplicador tanto del daño como de la impunidad.

Brufal y Ronco advierten sobre la convergencia entre criptoactivos e inteligencia artificial como el escenario más desafiante para la investigación penal contemporánea. La IA ya no es una promesa futura: es una realidad operativa que permite automatizar el proceso de layering en el lavado de activos, detectar y explotar vulnerabilidades en contratos inteligentes, y manipular mercados mediante bots de negociación algorítmica que generan señales falsas en tiempo real. Como señalan Europol e INTERPOL en su informe conjunto sobre crimen organizado digital (Europol, 2023), la capacidad de los grupos criminales para adoptar tecnologías emergentes supera sistemáticamente la velocidad de respuesta de los marcos regulatorios.

Sin embargo, los mismos autores subrayan una contraparte esperanzadora: la tecnología también ofrece herramientas sin precedentes para la investigación. El uso de algoritmos de aprendizaje automático y análisis de grafos transaccionales por parte de agencias como Europol, el FBI y empresas especializadas como Chainalysis o Elliptic ha permitido desarticular redes de lavado de activos que habrían resultado invisibles para las metodologías tradicionales. La paradoja de la blockchain, que oculta identidades, pero registra irreversiblemente cada transacción, es, para el investigador forense bien entrenado, una fortaleza más que una limitación.

Esta interconexión creciente entre tecnología criminal y tecnología de investigación exige que los operadores del sistema de justicia;

jueces, fiscales, defensores, abandonen las metodologías lineales y adopten herramientas de análisis masivo de datos, bajo una impronta de investigación penal estratégica. No se trata únicamente de capacitación técnica, sino de una transformación epistemológica: aprender a pensar en flujos, patrones y redes en lugar de en transacciones individuales.

2. El desafío probatorio en entornos de ofuscación: el fallo «Lazarte Di Lieto»

Uno de los ejes centrales de este volumen es el análisis del desafío probatorio que presentan los entornos de ofuscación deliberada. El fallo "Lazarte Di Lieto", estudiado en profundidad por Walter Chiquiar y Lucas Paulinovich, constituye un hito jurisprudencial de primer orden en la materia, no solo por sus hechos sino por la metodología de análisis que propone para superar los obstáculos técnicos que presentan herramientas como Wasabi Wallet y el protocolo CoinJoin.

El caso describe, en su estructura criminológica básica, una maniobra de abuso de confianza de manual: un asesor técnico informal aprovecha el acceso privilegiado a la frase semilla de su cliente, obtenido en el contexto de una migración de wallets legítima, para sustraer fondos en criptomonedas meses después, cuando la relación de confianza ya parecía extinguida. La tipología es la que Sutherland (1949) identificó como característica del delito de cuello blanco: un sujeto con posición de confianza y conocimiento técnico superior que lo utiliza en perjuicio de quien se lo confió.

Lo verdaderamente disruptivo del análisis de Chiquiar y Paulinovich es la propuesta metodológica para superar el obstáculo probatorio central: la fragmentación de la trazabilidad lineal producida por CoinJoin, un protocolo que combina múltiples transacciones de distintos usuarios en una sola operación, haciendo imposible la identificación de qué fracción de los fondos corresponde a qué origen. Frente a esta técnica de ofuscación, los autores proponen abandonar la lógica del "seguimiento de monedas" (coin tracking) y adoptar un análisis de Nivel 4 basado en clústeres y grafos de control económico.

Este enfoque, consistente con los estándares metodológicos desarrollados por el Financial Crimes Enforcement Network (FinCEN, 2021)

en sus directrices sobre activos virtuales, no busca probar que un bitcoin específico sustraído en una fecha determinada reapareció en una wallet particular. En cambio, reconstruye el circuito económico de control: analiza la consistencia operativa global, los patrones de comportamiento del imputado antes y después del hecho, la coincidencia cuantitativa entre montos sustraídos y montos reingresados a wallets bajo su esfera de control, y la proximidad temporal que hace estadísticamente inviable la hipótesis de la coincidencia.

Los autores sostienen, de manera convincente, que esta metodología es no solo técnicamente válida sino jurídicamente suficiente como estándar indiciario para sostener la imputación en etapas procesales complejas. La propuesta se alinea con lo que Reuter y Truman (2004) denominan el "análisis de riqueza inexplicada": cuando la trayectoria económica del imputado no puede explicarse por fuentes legítimas conocidas, la carga probatoria se desplaza hacia la justificación de esos flujos.

3. Estafas sistémicas: del esquema Ponzi al «rug pull» como delito económico-político

3.1. El caso Adhemar Capital: el Ponzi en la era del influencer

La criminalidad económica masiva tiene en los esquemas de tipo Ponzi su manifestación más longeva y socialmente dañina. El artículo de Maximiliano Fernández y Lorena Varas sobre el caso Edgar Adhemar Bacchiani y su firma Adhemar Capital SRL representa una contribución de primer orden al estudio de cómo este esquema clásico se ha reinventado y potenciado en el ecosistema cripto.

Bacchiani construyó su captación fraudulenta sobre tres pilares que los autores identifican con precisión: la mística de los retornos extraordinarios prometidos en dólares (entre el 6% y el 12% mensual), la figura del "Trader God" como autoridad carismática con conocimiento técnico inaccesible para el inversor común, y el efecto de legitimación que produjo la asociación visual y simbólica con el mundo cripto. Como documentan ampliamente Frankel (2012) en la historiografía del fraude, el esquema Ponzi en entornos digitales se beneficia de la opacidad tecnológica para disimular la estructura

fraudulenta durante períodos más prolongados que sus versiones analógicas.

Fernández y Varas realizan una contribución metodológica de alto valor al proponer que la investigación no debe limitarse a la persecución y condena del autor sino que debe orientarse hacia la Investigación del Aspecto Económico del Delito (IAED) como herramienta para el recupero de activos y el resarcimiento de las víctimas. Esta perspectiva, coherente con los Principios de Bruselas sobre Recupero de Activos (UNODC, 2019), propone la utilización sistemática del levantamiento de secretos fiscal y bancario, la auditoría forense y el análisis de patrimonio para reconstruir *la cuantía real del daño* y localizar los activos desviados.

La dimensión social del caso es igualmente relevante: las víctimas de Adhemar Capital no fueron grandes inversores institucionales sino ahorristas individuales, trabajadores y jubilados que confiaron sus ahorros, frecuentemente denominados en dólares para protegerlos de la inflación, en un instrumento que prometía retornos imposibles. Esta dimensión victimológica, que los autores abordan con sensibilidad, refuerza la necesidad de diseñar mecanismos de compensación que el derecho penal tradicional no prevé adecuadamente.

3.2. El caso $LIBRA: cuando el estado legitima el fraude

Si el caso Bacchiani representa la actualización tecnológica de una modalidad criminal centenaria, el análisis del caso $LIBRA desarrollado por Ignacio Chiarenza y Manuela Losada introduce una categoría conceptual de mayor complejidad y perturbación: la del delito económico-político.

El rug pull, o "tirón de alfombra", en traducción libre, es una modalidad de fraude específicamente cripto que consiste en la creación y promoción artificial de un token hasta alcanzar una capitalización de mercado significativa, para luego retirar masivamente la liquidez del pool de intercambio, colapsando el precio y dejando a los tenedores con activos sin valor recuperable. Su ejecución técnica requiere un grado de coordinación y conocimiento de los mecanismos de los protocolos DeFi que lo distingue claramente de una estafa ordinaria.

Lo que hace al caso $LIBRA singularmente grave, y teóricamente relevante, no es la mecánica del fraude en sí, sino la intervención de actores estatales en su legitimación. Chiarenza y Losada recuperan

el concepto de delito económico-político desarrollado por Naucke, quien lo define como aquellas conductas criminales que son fortalecidas, toleradas o directamente habilitadas por el aparato estatal. La promoción pública del token por parte de funcionarios de alto rango del Poder Ejecutivo Nacional, incluyendo referencias directas desde la cuenta presidencial en redes sociales, actuó como señal de legitimidad institucional que indujo a error a miles de inversores minoristas que razonablemente interpretaron ese respaldo como garantía de seriedad.

Los autores construyen un análisis que articula categorías del derecho penal, error esencial de tipo, ardid o engaño, perjuicio patrimonial cuantificable, con el análisis on-chain del comportamiento del pool de liquidez, mostrando la coordinación temporal entre la promoción oficial y el retiro de fondos. Este abordaje interdisciplinario es precisamente el que este volumen propone como estándar metodológico para la investigación de la criminalidad económica compleja. Siguiendo a Naucke, los autores advierten que el delito económico-político no es simplemente más grave que el delito económico ordinario: es cualitativamente distinto, porque erosiona la confianza en el Estado mismo como garante del orden económico.

4. El estado frente al espejo: fortalezas, debilidades y el marco regulatorio

4.1. Análisis FODA de la persecución penal estratégica

La capacidad del Estado para responder eficazmente a la criminalidad económica digital no puede darse por sentada. El trabajo de Elia Bollecich Masters realiza un diagnóstico riguroso mediante el instrumento del análisis FODA (Fortalezas, Oportunidades, Debilidades y Amenazas) aplicado a la persecución penal estratégica en materia de criptoactivos, ofreciendo un mapa institucional cuya honestidad resulta tan valiosa como incómoda.

En el plano de las fortalezas, Bollecich identifica correctamente la trazabilidad inherente a la blockchain como el activo diferencial de la investigación en este campo. A diferencia del efectivo, instrumento predilecto del lavado de activos durante décadas, cada transacción

en la cadena de bloques queda registrada de forma permanente e inmutable. Esta característica convierte a la blockchain en una fuente probatoria de excepcional potencia cuando se cuenta con las herramientas y el conocimiento para explotarla. Como señala el GAFI (2021) en sus directrices sobre activos virtuales, la aplicación del análisis de blockchain al rastreo de activos ilícitos ha permitido recuperar en los últimos años fondos que en esquemas analógicos hubieran resultado irrecuperables.

Sin embargo, las debilidades que Bollecich identifica son estructurales y urgentes. La falta de especialización técnica de los investigadores, jueces, fiscales, peritos, constituye la brecha más crítica. No se trata solo de desconocimiento tecnológico sino de una carencia epistemológica más profunda: la dificultad para formular teorías del caso que integren el análisis económico-forense como elemento central y no como mero anexo técnico. A esto se suma el acceso limitado a herramientas profesionales de análisis on-chain, cuyos costos de licenciamiento resultan prohibitivos para muchas jurisdicciones.

La propuesta central de Bollecich, la creación de fiscalías especializadas en criminalidad económica digital, dotadas de equipos interdisciplinarios permanentes, es consistente con las mejores prácticas internacionales documentadas por el Egmont Group (2022) y con las recomendaciones del GAFI para jurisdicciones de mercados emergentes. La centralización del conocimiento especializado en unidades con recursos, continuidad institucional y protocolos de actuación estandarizados ha probado ser, en experiencias como la del Departamento de Justicia de los Estados Unidos o la Fiscalía Europea (EPPO), un multiplicador significativo de la eficacia investigativa.

4.2. La Ley 27.739: avances formales y desafíos estructurales

El artículo de María Alejandra Freire sobre los avances y desafíos de la regulación de los Proveedores de Servicios de Activos Virtuales (PSAV) en Argentina aborda el marco normativo vigente con una perspectiva crítica que va más allá del análisis exegético.

La Ley 27.739, sancionada en 2024, incorporó a los exchanges y demás PSAV como sujetos obligados ante la Unidad de Información Financiera (UIF) y estableció un registro obligatorio bajo la supervisión de la Comisión Nacional de Valores (CNV). Desde una perspectiva formal, esta norma representa un avance significativo hacia los estándares del

Grupo de Acción Financiera Internacional (GAFI), cuya Recomendación 15 (GAFI, 2019) exige que los países apliquen a los PSAV el mismo régimen de prevención del lavado de activos y financiamiento del terrorismo que rige para las entidades financieras tradicionales.

Sin embargo, Freire identifica con rigor las deficiencias estructurales que comprometen la eficacia real del marco. La primera y más crítica es la falta de coordinación interinstitucional entre la CNV y la UIF: dos organismos con culturas regulatorias distintas, objetivos parcialmente superpuestos y sin mecanismos de coordinación eficaz, generan para los PSAV obligados una carga de cumplimiento duplicada e incoherente que desincentiva la formalización y abre espacios de arbitraje regulatorio. Esta tensión, que Freire documenta con precisión, reproduce en el campo cripto la fragmentación institucional que ha debilitado históricamente la capacidad regulatoria argentina en el sector financiero.

El segundo desafío estructural que señala la autora es la regulación de las plataformas offshore: exchanges internacionales que prestan servicios a usuarios argentinos sin presencia física en el país y, por tanto, fuera del alcance real de la regulación doméstica. Este fenómeno, que el GAFI (2021) denomina "riesgo de elusión por diseño", es especialmente pronunciado en Argentina dado el alto volumen de operaciones peer-to-peer y el uso extendido de plataformas como Binance o Coinbase, registradas en jurisdicciones con regímenes regulatorios menos exigentes.

La tercera debilidad identificada es la implementación de la "Regla de Viaje" (Travel Rule), que exige que en cada transferencia de activos virtuales se transmita información identificatoria del ordenante y del beneficiario. Este estándar, requerido por la Recomendación 16 del GAFI (2019) y ya implementado en la Unión Europea a través del Reglamento de Transferencias de Fondos (EU, 2023), implica costos tecnológicos y operativos significativos que los PSAV locales de menor escala difícilmente pueden afrontar sin apoyo estatal o períodos de implementación gradual.

5. La frontera fiscal: transparencia internacional y desigualdad

La dimensión tributaria de la criminalidad económica vinculada a los criptoactivos es abordada de forma rigurosa y con perspectiva comparada por Antonella Gervagi y Ana Laura Jaruf en el artículo

que cierra este volumen. Su análisis del Marco de Reporte de Criptoactivos (CARF) impulsado por la OCDE (2022) no solo describe el instrumento técnico, sino que inscribe su análisis en una reflexión más amplia sobre justicia fiscal, desigualdad y género.

El CARF, aprobado por la OCDE en 2022 y cuya primera ronda de intercambios está prevista para 2027, establece un sistema de intercambio automático de información sobre transacciones en criptoactivos entre autoridades fiscales de países adherentes, análogo al Common Reporting Standard (CRS) que ya opera para cuentas financieras tradicionales. Su lógica es simple pero poderosa: si los exchanges deben reportar a las autoridades fiscales las transacciones de sus usuarios, el anonimato relativo de los criptoactivos se reduce significativamente para quienes operen a través de plataformas reguladas.

Gervagi y Jaruf identifican, no obstante, las limitaciones estructurales del CARF frente a las operaciones DeFi (Finanzas Descentralizadas). En los protocolos DeFi, los intercambios se producen directamente entre wallets sin intervención de ningún intermediario centralizado que pueda ser objeto de obligaciones de reporte.

La perspectiva de género que aportan las autoras es un elemento de notable originalidad en la literatura especializada sobre criminalidad económica digital. Gervagi y Jaruf documentan cómo la opacidad de los criptoactivos como vector de evasión fiscal no es un fenómeno socialmente neutro: son los sectores con mayor capacidad de inversión y conocimiento tecnológico, predominantemente masculinos y de alto poder adquisitivo, quienes acceden a los mecanismos más sofisticados de evasión. El resultado es una doble inequidad: por un lado, el Estado compensa la menor recaudación presionando sobre los impuestos indirectos que afectan de forma desproporcionada a los sectores de menores ingresos; por otro, las mujeres, sobrerrepresentadas en esos estratos y en la economía de cuidados no remuneradas, soportan de manera regresiva el costo fiscal de la evasión de otros.

El análisis comparado de la región que ofrecen las autoras (Brasil, México, El Salvador y Paraguay) permite contextualizar los desafíos de Argentina y extraer lecciones de política fiscal aplicables. La experiencia de Brasil con la Instrução Normativa RFB 1.888/2019, que impuso obligaciones de reporte a las exchanges antes de que existiera un marco internacional coordinado, demuestra que la acción

unilateral anticipada puede capturar información valiosa, aunque no resuelva el problema de la evasión transfronteriza.

6. El abordaje contable e impositivo de los criptoactivos: la dimensión técnica de la persecución

Si los artículos anteriores abordan la criminalidad vinculada a los criptoactivos desde la perspectiva penal, forense y regulatoria, el trabajo de Jesica Nicol Luisi y Martín Regalini, "Abordaje del aspecto contable e impositivo de los criptoactivos", aporta una dimensión indispensable que con frecuencia queda relegada en la literatura jurídico-penal: la técnica contable e impositiva como herramienta de reconstrucción patrimonial y detección del delito. Su contribución es de notable valor práctico, ya que, sin el dominio de estas categorías, la investigación penal carece de los instrumentos necesarios para cuantificar el daño, probar el enriquecimiento ilícito y orientar las medidas cautelares de recupero.

Los autores parten de un diagnóstico normativo que es, en sí mismo, revelador: la primera aproximación regulatoria argentina a las criptomonedas no provino del Congreso ni del Banco Central, sino de una resolución de la Unidad de Información Financiera (UIF 300/2014), dictada siguiendo los lineamientos del GAFI. Esta progresión, donde el organismo de prevención del lavado antecede al regulador financiero y al legislador, no es accidental: refleja que los criptoactivos ingresaron al radar institucional argentino primariamente como problema de cumplimiento antilavado, y solo después como objeto de derecho tributario, contable y penal. Esta secuencia tiene consecuencias directas sobre los vacíos normativos que el artículo mapea con precisión.

En el plano contable, Luisi y Regalini realizan una contribución técnica de primer orden al clarificar que la clasificación patrimonial de los criptoactivos no es uniforme, sino que depende de la función económica que cumplen para el sujeto que los posee. Siguiendo el marco conceptual de las normas contables profesionales argentinas (RT N.º 16, FACPCE), los autores distinguen cuatro tratamientos posibles: los criptoactivos utilizados como medio de pago se exponen bajo el rubro Caja y Bancos; los mantenidos con fines de rentabilidad

especulativa integran el rubro Inversiones; los que constituyen el objeto de la actividad principal del ente, como ocurre con los exchanges, corresponden a Bienes de Cambio; y los recibidos en calidad de préstamo o depósito configuran un Pasivo. Esta taxonomía, aparentemente técnica, tiene implicancias directas para la investigación penal: la clasificación adoptada por el imputado determina el tipo de auditoría forense aplicable y las normas de valuación que permiten reconstruir el patrimonio real.

En materia impositiva, el artículo sistematiza el tratamiento aplicable en los tres tributos más relevantes para la investigación patrimonial. En el Impuesto a las Ganancias, los resultados de la enajenación de criptoactivos están gravados tanto para personas humanas, con tasas cedulares del 5% o 15% según la denominación de la operación, como para personas jurídicas, a la alícuota progresiva del artículo 73 de la ley. En el IVA, si bien la venta de criptoactivos en sí misma no está alcanzada, por no tratarse de "cosas muebles" en sentido técnico, sí lo está la prestación del servicio de intermediación, lo que convierte a las comisiones de los exchanges en un vector de fiscalización. En el Impuesto sobre Bienes Personales, siguiendo el Dictamen ARCA 2/2022, los criptoactivos se valúan al costo de adquisición ajustado al 31 de diciembre de cada año, con declaración explícita como "monedas digitales, monedas virtuales, criptoactivos o similares".

Uno de los aportes más relevantes del trabajo es el análisis sistemático del régimen informativo de ARCA (ex-AFIP) como fuente de inteligencia patrimonial para la investigación. Las Resoluciones Generales 4614/2019, 4647/2019, 5029/2021, 5348/2023 y 5512/2024 establecen obligaciones de reporte para los exchanges locales que permiten, dentro de sus límites, reconstruir tenencias, detectar inconsistencias en declaraciones juradas y cruzar información fiscal. La más reciente, RG 5804/2025, avanza un paso adicional al exigir la valuación mensual de saldos en criptoactivos y su reporte por usuario, aproximándose al estándar de monitoreo continuo que el CARF de la OCDE busca institucionalizar a nivel internacional. No obstante, los autores son rigurosos al señalar las limitaciones estructurales del sistema: las wallets de autocustodia, los exchanges extranjeros y las operaciones peer-to-peer permanecen fuera del alcance informativo del régimen doméstico, configurando los mismos "puntos ciegos" que Freire identifica desde la perspectiva regulatoria.

La sección sobre recupero y congelamiento de criptoactivos constituye una guía procedimental de alto valor operativo para fiscales e investigadores. Luisi y Regalini detallan con precisión técnica los pasos que deben seguirse: identificación de las personas requeridas con sus datos registrales completos, delimitación temporal del período bajo análisis, levantamiento de secretos fiscal, bancario y bursátil, y solicitud de información coordinada a los exchanges regulados por la CNV (actualmente 82 entidades registradas), a ARCA por vía de sus regímenes informativos y al BCRA mediante comunicación "D" para vincular billeteras virtuales con cuentas bancarias. La advertencia crítica de los autores sobre la necesidad de actuar con rapidez, dada la posibilidad de transferir criptoactivos en segundos hacia direcciones inaccesibles, conecta directamente con los estándares de urgencia que el GAFI (2021) y GAFILAT (2021) han establecido para las medidas cautelares sobre activos virtuales.

El artículo también ilumina una "zona gris" de notable relevancia práctica: el uso de criptomonedas como medio de pago en exportaciones de servicios puede funcionar como mecanismo de elusión del régimen cambiario, al permitir no canalizar ingresos equivalentes a divisas a través del mercado oficial de cambios. Esta tensión entre la validez contable e impositiva de la operación, que genera un ingreso gravado y registrable, y su posible infracción al régimen cambiario pone de manifiesto que la criminalidad económica vinculada a criptoactivos no siempre opera mediante el engaño o la apropiación ilícita directa, sino también a través de la instrumentalización de vacíos normativos que el legislador no anticipó.

En síntesis, el trabajo de Luisi y Regalini cumple una función articuladora dentro de este volumen: si los artículos precedentes diagnostican el problema desde el derecho penal, la criminología y la regulación, este trabajo proporciona el lenguaje contable e impositivo que el investigador necesita para traducir las estructuras criminales en evidencia patrimonial cuantificable, recuperable y judicializable. Como señala Regalini en su trayectoria académica y profesional, la pericia contable no es un auxiliar técnico del proceso penal: es, en la investigación de la criminalidad económica compleja, el núcleo mismo del caso.

7. Las stablecoins bajo la lupa: arquitectura, riesgos y el nuevo orden regulatorio global

Si los artículos precedentes abordan la criminalidad vinculada a los criptoactivos desde la perspectiva penal y forense, el trabajo de Augusto Lombardo y Nicolás Maletti, "Stablecoins bajo la lupa: concepto, clasificación y el nuevo orden regulatorio internacional", introduce una dimensión que resultaba indispensable para completar el mapa conceptual de este volumen: el análisis sistemático de las monedas estables como infraestructura financiera en plena consolidación, con sus propias lógicas de funcionamiento, sus riesgos específicos y los marcos regulatorios que el mundo está construyendo, con urgencia y no sin tensiones, para contenerlas.

Lombardo y Maletti parten de una premisa que este volumen comparte en su conjunto: la comprensión del fenómeno debe preceder a su persecución. En ese sentido, su contribución comienza por despejar la ambigüedad conceptual que rodea al término «stablecoin», recorriendo las definiciones del Banco Central Europeo, del World Economic Forum y de la doctrina especializada, para proponer una síntesis operativa: tipo de criptomoneda diseñada para tener un valor fijo y estable, generalmente vinculado al precio de una moneda fiduciaria o a un activo real. Esta claridad terminológica no es un detalle menor; es el punto de partida para cualquier intervención regulatoria o penal eficaz.

La taxonomía que desarrollan los autores, stablecoins respaldadas por dinero fiat, por activos, por criptoactivos y algorítmicas, tiene una relevancia directa para la investigación penal patrimonial. Cada categoría implica una arquitectura de riesgo diferente: las respaldadas por fiat concentran el poder de congelamiento en un único emisor privado (Tether, Circle), mientras que las algorítmicas, como demostró el colapso de Terra-Luna en 2022, pueden desmoronarse en cuestión de horas cuando la pérdida de confianza activa la "espiral de la muerte". El relato pormenorizado de este episodio que ofrecen Lombardo y Maletti constituye un caso pedagógico de primer orden para entender cómo la ingeniería financiera descentralizada puede generar pérdidas masivas sin que exista un responsable penal claramente identificable bajo los marcos vigentes.

El recorrido regulatorio comparado que realizan los autores, Reglamento MiCA europeo, Ley GENIUS norteamericana, regulaciones de Rusia, China y Reino Unido, y el vacío normativo argentino, pone de manifiesto una carrera entre la innovación y la respuesta institucional que ningún país ha ganado todavía con claridad. Para el fiscal o el juez que trabaja con activos virtuales en Argentina, este panorama comparado ofrece algo más que erudición: ofrece una brújula para anticipar qué estándares internacionales llegarán a nuestro ordenamiento y qué argumento de derecho comparado puede sustentar una estrategia de litigio innovadora. La regulación argentina, limitada aún al encuadre de los proveedores de servicios (PSAV) mediante la Ley 27.739 y la Resolución 994/24 de la CNV, aparece en este contexto como un primer paso necesario pero insuficiente frente a la envergadura del fenómeno.

El artículo de Lombardo y Maletti cumple, así, una función análoga a la que en el derecho penal clásico tiene la tipificación: antes de perseguir, hay que saber qué se persigue. En un ecosistema donde Tether concentra más del 60% del volumen total de stablecoins en circulación y donde cinco de las veinte criptomonedas de mayor capitalización son monedas estables vinculadas al dólar, este conocimiento deja de ser teórico y se convierte en una herramienta operativa imprescindible.

8. No es disrupción, es adaptación: las tensiones estructurales del ecosistema cripto en argentina

El artículo de Carlos Emanuel Monzón, "No es disrupción, es adaptación: tensiones del ecosistema cripto en Argentina", aporta al volumen una perspectiva que ninguno de los trabajos precedentes abordaba con la misma profundidad: la dimensión socioeconómica y estructural del fenómeno cripto en el contexto específico de la economía argentina. Lejos de presentar a los criptoactivos como una revolución tecnológica que transforma el paisaje financiero desde afuera, Monzón sostiene una hipótesis más incómoda y más precisa: el ecosistema cripto en Argentina no es disruptivo, es adaptativo. No cambia las lógicas estructurales del sistema; las replica en un nuevo entorno tecnológico.

El diagnóstico de Monzón parte de una paradoja que este volumen en su conjunto también documenta: los instrumentos que permiten

a los ciudadanos escapar de las restricciones del sistema financiero local, la inflación, el cepo cambiario, la desconfianza institucional, son precisamente aquellos que implican mayor dependencia de actores externos y centralizados. Las stablecoins más utilizadas en Argentina, USDT y USDC, no son descentralizadas en ningún sentido operativo relevante: su emisión, su respaldo y su gobernanza dependen de Tether y Circle, empresas privadas que operan bajo jurisdicciones extranjeras y que pueden congelar fondos unilateralmente. La "autonomía financiera" que el ecosistema promete es, en los hechos, una redistribución de dependencias: se abandona la dependencia del banco central local para asumir la dependencia de un emisor privado global.

Desde la perspectiva de la criminalidad económica, el análisis de Monzón sobre la tensión entre trazabilidad técnica y opacidad operativa es particularmente valioso. El autor identifica con precisión una asimetría regulatoria que afecta directamente a la eficacia de la persecución penal: la regulación se concentra en los intermediarios (los PSAV), que son los puntos donde la supervisión resulta operativamente viable, pero los activos en sí mismos circulan en gran medida fuera de control directo. Controlar la entrada al sistema no equivale a controlar lo que ocurre dentro. Esta observación tiene consecuencias prácticas inmediatas: permite entender por qué esquemas de lavado de activos sofisticados pueden utilizar stablecoins para fragmentar el rastro patrimonial incluso cuando el punto de entrada y el de salida están registrados.

El trabajo también cuestiona con rigor empírico la narrativa de la inclusión financiera como promesa democratizadora de los criptoactivos. Monzón documenta que el uso de stablecoins en Argentina no se distribuye de manera homogénea, sino que se concentra en usuarios ya integrados al sistema financiero formal, con acceso a tecnología, conectividad y educación financiera suficiente. Lejos de incorporar a los sectores excluidos, el ecosistema tiende a optimizar las estrategias de quienes ya operaban dentro del sistema, reforzando desigualdades preexistentes bajo el ropaje de la innovación.

Para el investigador penal o el regulador, el artículo de Monzón ofrece un marco conceptual de alto valor estratégico: el ecosistema cripto argentino no es un espacio de ruptura que exige herramientas

completamente nuevas, sino un campo híbrido donde conviven lógicas de descentralización con estructuras centralizadas, innovaciones tecnológicas con prácticas históricas de informalidad y dolarización, y promesas de inclusión con nuevas formas de segmentación. Comprender esta hibridez es el primer paso para diseñar respuestas institucionales que no fallen por exceso de literalidad tecnológica ni por déficit de sofisticación jurídica.

Conclusión: la interdisciplinariedad como imperativo estratégico

Los trabajos reunidos en este volumen convergen en un diagnóstico compartido: la lucha contra la criminalidad económica en la era digital no es, en primera instancia, un problema de capacidad técnica, aunque la carencia técnica sea real y urgente, sino fundamentalmente un problema de estrategia institucional, de voluntad política y de renovación epistemológica.

Las fortalezas de la blockchain, su trazabilidad, su inmutabilidad, su transparencia radical, se ven sistemáticamente amenazadas por el uso de mixers, bridges entre redes, protocolos de privacidad y la transnacionalidad de las maniobras. Pero esta amenaza no es invencible: es, ante todo, una brecha de conocimiento y de coordinación. Cuando las autoridades de investigación cuentan con las herramientas, el entrenamiento y los marcos normativos de cooperación internacional adecuados, la blockchain se convierte, paradójicamente, en el registro más honesto y exhaustivo que haya existido para documentar la actividad económica ilícita.

La respuesta efectiva que estos trabajos proponen no es la hiperregulación que ahogue la innovación ni el abandono regulatorio que deje el campo libre a la impunidad. Es, en cambio, una respuesta calibrada que integre tres dimensiones: la pericia informática y el análisis de datos como herramientas estándar de la investigación penal; una sólida teoría del caso económico que trascienda el punitivismo tradicional para priorizar el recupero de activos y la reparación a las víctimas; y una cooperación internacional genuina, construida sobre estándares comunes de intercambio de información financiera y asistencia judicial.

Como señala el GAFI en su evaluación mutua más reciente de Argentina (GAFI, 2023), el país presenta avances técnicos normativos significativos pero una eficacia operativa todavía insuficiente en la aplicación de esos marcos a casos complejos. Esta brecha entre la norma y su eficacia es precisamente el espacio que este volumen busca iluminar con evidencia, metodología y propuestas concretas.

Este número de los *Cuadernos sobre criminalidad económica* invita a jueces, fiscales, reguladores y académicos a repensar el derecho penal desde una perspectiva sistémica e interdisciplinaria. No podemos enfrentar delitos del siglo XXI con estructuras burocráticas del siglo XX. Los trabajos aquí reunidos demuestran que, con las herramientas adecuadas y la voluntad institucional necesaria, las huellas inmutables que todo delincuente deja en la blockchain pueden ser leídas, interpretadas y llevadas al estrado judicial. Solo mediante la actualización constante de nuestras capacidades, técnicas, jurídicas e institucionales, y la cooperación internacional efectiva podremos evitar que la innovación tecnológica se convierta, simplemente, en una nueva forma de impunidad.

Referencias bibliográficas

Administración Federal de Ingresos Públicos [AFIP]. (2019). *Resolución General N.º 4614/2019. Régimen informativo de operaciones con criptoactivos*. Boletín Oficial de la República Argentina.

Agencia de Recaudación y Control Aduanero [ARCA]. (2022). *Dictamen N.º 2/2022 DI ALIR: Impuesto sobre los bienes personales. Criptomonedas. Naturaleza jurídica. Gravabilidad*. Ministerio de Economía de la Nación Argentina.

Agencia de Recaudación y Control Aduanero [ARCA]. (2024). *Resolución General N.º 5512/2024*. Boletín Oficial de la República Argentina.

Agencia de Recaudación y Control Aduanero [ARCA]. (2025). *Resolución General N.º 5804/2025*. Boletín Oficial de la República Argentina.

Banco Mundial. (2022). *The Global Findex Database 2021: Financial Inclusion, Digital Payments, and Resilience in the Age of COVID-19*. Banco Mundial.

Chainalysis. (2023). *The Chainalysis 2023 Crypto Crime Report*. Chainalysis Inc.
Comisión Nacional de Valores [CNV]. (2024). *Resolución General N.º 994/2024. Registro de Proveedores de Servicios de Activos Virtuales*. Boletín Oficial de la República Argentina.
Egmont Group. (2022). *Annual Report 2021-2022*. Egmont Group of Financial Intelligence Units.
European Union. (2023). *Regulation (EU) 2023/1113 on information accompanying transfers of funds and certain crypto-assets*. Official Journal of the European Union.
Europol. (2023). *Internet Organised Crime Threat Assessment (IOCTA) 2023*. Europol.
Federación Argentina de Consejos Profesionales de Ciencias Económicas [FACPCE]. (2000). *Resolución Técnica N.º 16: Marco Conceptual de las normas contables profesionales*. FACPCE.
Financial Crimes Enforcement Network [FinCEN]. (2021). *FinCEN Guidance on Convertible Virtual Currency Mixing*. U.S. Department of the Treasury.
Frankel, T. (2012). *The Ponzi Scheme Puzzle: A History and Analysis of Con Artists and Victims*. Oxford University Press.
GAFILAT. (2021). *Guía sobre aspectos relevantes y pasos apropiados para la investigación, identificación, incautación y decomiso de activos virtuales*. Grupo de Acción Financiera de Latinoamérica.
Grupo de Acción Financiera Internacional [GAFI]. (2019). *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*. FATF/OECD.
Grupo de Acción Financiera Internacional [GAFI]. (2021). *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*. FATF/OECD.
Grupo de Acción Financiera Internacional [GAFI]. (2023). *Anti-Money Laundering and Counter-Terrorist Financing Measures: Argentina*. Mutual Evaluation Report. FATF/OECD.
Instituto Nacional de Estadística y Censos [INDEC]. (2024). *Índice de Precios al Consumidor: Resultados del año 2023*. Ministerio de Economía de la Nación Argentina.
Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. https://bitcoin.org/bitcoin.pdf

Naucke, W.-R. (2015). *El concepto de delito económico-político: Una aproximación* (E. Sarrabayrouse, Trad.). Marcial Pons.
OCDE. (2022). *Crypto-Asset Reporting Framework and Amendments to the Common Reporting Standard*. OECD Publishing. https://doi.org/10.1787/1d0c89fd-en
Proceeds of Crime Act [POCA]. (2002). *Part 8: Investigations*. UK Parliament.
Reuter, P., & Truman, E. M. (2004). *Chasing Dirty Money: The Fight Against Money Laundering*. Institute for International Economics.
Sutherland, E. H. (1949). *El delito de cuello blanco*. BdeF. Colección: Memoria Criminológica Nº 6. 2009.
Unidad de Información Financiera [UIF]. (2024). *Resolución 49/2024: Obligaciones de reporte para Proveedores de Servicios de Activos Virtuales*. Boletín Oficial de la República Argentina.
UNODC. (2019). *The Brussels Principles on the Recovery of Corruption Proceeds*. United Nations Office on Drugs and Crime.

Cuando la tecnología cambia el mundo del crimen

Laureano Brufal[1] y Paula Ronco[2]

Resumen

El presente trabajo examina la convergencia entre criptoactivos e inteligencia artificial y su incidencia en la evolución de la criminalidad compleja, en particular en el ámbito del cibercrimen y del lavado de activos. En primer lugar, se desarrolla una aproximación histórica y técnica al fenómeno de los criptoactivos, abordando el surgimiento de Bitcoin en el contexto de la crisis financiera de 2008, la expansión del ecosistema blockchain, el funcionamiento de billeteras, tokens, mecanismos de consenso, protocolos DeFi, bridges, mixers y otras herramientas propias del entorno descentralizado. En segundo término, se presenta una reseña histórica de la inteligencia artificial, desde sus antecedentes conceptuales hasta su masificación reciente con los modelos generativos, destacando sus capacidades de automatización, análisis y producción de contenido. Sobre esa base, se analiza la interrelación entre ambas tecnologías en el marco del delito económico contemporáneo, identificando usos criminales como el lavado automatizado de fondos, la explotación de vulnerabilidades en contratos inteligentes, la manipulación de mercados y la sofisticación

1- Bachiller Universitario en Derecho, Universidad Nacional de Rosario, 2015; Diplomado en Blockchain, Bitcoin y Criptomonedas, Secretaría de Extensión Universitaria, Bienestar Estudiantil y Desarrollo Sustentable de la Facultad de Ciencias Económicas de la Universidad de Buenos Aires y la ONG Bitcoin, 2024. Programa Ejecutivo Blockchain & Criptomonedas, Universidad Torcuato Di Tella, 2022. Trabaja en Ministerio Publico de la Acusación de la Provincia de Santa Fe desde 2016. Correo: laureanobrufal@gmail.com

2- Abogada de la Universidad Nacional de Rosario; Diplomada en Análisis Económico Forense, Universidad Nacional de Rosario. Especialización en Derecho Penal, Universidad Nacional de Rosario (en curso). Trabaja en el Ministerio Público de la Acusación de la Provincia de Santa Fe desde 2021. Correo: paulasronco@gmail.com

de fraudes digitales. Asimismo, se examina el empleo de inteligencia artificial en tareas de prevención, monitoreo e investigación por parte de organismos públicos y empresas especializadas en análisis blockchain. Finalmente, se sostiene que la transformación tecnológica plantea desafíos significativos para los sistemas de persecución penal, pero también ofrece nuevas herramientas para fortalecer la trazabilidad, la cooperación internacional y la capacidad institucional frente a formas cada vez más complejas de criminalidad económica.

1. Introducción

Desde el ladrón a pie en un mercado egipcio, pasando por bandidos a caballo y sujetos que asaltaban camiones blindados hasta los actuales ciberdelincuentes que en un par de segundos vacían cuentas, podemos ver cómo fue cambiando el delito en sus formas y medios, pero en esencia sigue siendo la apropiación ilegal de bienes ajenos.

Los cambios tecnológicos impactan en todos los ámbitos de la sociedad, no estando ajeno a estos cambios el mundo del crimen.

Las últimas décadas del siglo XX y la primera década del siglo XXI mostraron cambios vertiginosos a nivel tecnológico a partir de la adopción masiva de internet que nos mostró un mundo interconectado en tiempo real, pasando por la aparición de las redes sociales que modificaron las formas de relacionarnos y percibir la realidad. En ese proceso de transformación tecnológica observamos la irrupción creciente en nuestras vidas de dos fenómenos disruptivos como son las criptomonedas y la inteligencia artificial.

Los sellos postales de Carlo Ponzi se han actualizado en esquemas que involucran criptomonedas y publicidad generada por IA, el dinero de origen ilícito no necesita ser transportado o almacenado de manera física, o pasar por las viejas lavanderías, ni requiere de un complejo sistema de sociedades; basta con el uso de algún criptoactivo que en segundos lo transfiere a otra parte del mundo o aprovechándose de vacíos legales se puede incorporar al circuito legal.

Frente a ello, se vuelve necesario examinar cómo estas tecnologías se desarrollaron, qué lógicas técnicas las sustentan y de qué

manera intervienen en la configuración actual del delito complejo. En el presente trabajo se analizará, en primer lugar, desde una mirada histórica y técnica el fenómeno de los criptoactivos; seguidamente se abordará desde la misma perspectiva el surgimiento de la inteligencia artificial, con breves referencias a delitos y la investigación de los mismos. Posteriormente se examinará la interconexión entre los criptoactivos y la inteligencia artificial en el marco del avance de la criminalidad compleja en la actualidad. Finalmente, se presentarán algunas conclusiones orientadas a comprender el alcance y las implicancias de esta convergencia tecnológica.

2. Historia y aspectos técnicos de los criptoactivos

2.1. Reseña histórica de las criptomonedas

El 15 de septiembre de 2008 el banco Lehman Brothers presentaba la quiebra (Reuters, 2008). Fue el momento icónico de la crisis financiera de las subprime, bautizada así en honor al activo financiero que se había convertido en una burbuja que puso en jaque a la economía mundial. La crisis puso en tela de juicio el accionar de Wall Street, las calificadoras de riesgo y los bancos en todo el mundo. En aquel momento Facebook tenía 4 años[3] y aparecían los primeros smartphones[4] y el mundo ya se comunicaba por mensajería móvil.

En ese contexto, el 31 de octubre de 2008 Satoshi Nakamoto envió un correo electrónico a un grupo de criptógrafos que decía “He estado trabajando en un nuevo sistema de efectivo electrónico que es completamente entre pares, sin necesidad de un tercero de confianza”, adjuntando un documento titulado “Bitcoin: Un Sistema de Efectivo Electrónico Entre Pares”.[5] Al referirse a un tercero de confianza, Nakamoto hacía alusión a las instituciones financieras que eran las prota-

3- Meta. (s.f.). *About company info*. https://www.meta.com/es-la/about/company-info/
4- Apple Newsroom. (2008). *Apple introduces the new iPhone 3G*. https://www.apple.com/newsroom/2008/06/09Apple-Introduces-the-New-iPhone-3G/ | Google Blog. (2008). First Android-powered phone. https://googleblog.blogspot.com/2008/09/first-android-powered-phone.html
5- Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. https://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html

gonistas de la crisis y a los gobiernos del mundo, principalmente el de EE.UU., que estaban saliendo a rescatar a los bancos en problemas.

Como describiera Vitalik Buterin:

> Cuando Satoshi Nakamoto puso en marcha por primera vez la blockchain de Bitcoin en enero de 2009, estaba introduciendo simultáneamente dos conceptos radicales y no probados. El primero es el 'bitcoin', una moneda digital descentralizada de igual a igual (peer-to-peer) que mantiene un valor sin ningún respaldo, valor intrínseco ni emisor central [...] Sin embargo, también existe otra parte, igualmente importante, del gran experimento de Satoshi: el concepto de una blockchain basada en Proof of Work (prueba de trabajo), que permite alcanzar un acuerdo público sobre el orden de las transacciones. (2014)

El 3 de enero de 2009, se minó el primer bloque de Bitcoin, el genesis block, con un mensaje dentro del bloque que aún resuena como una crítica a las instituciones tradicionales, el titular del diario *The Times* de ese día: "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks.", donde se anuncia un nuevo salvataje al sistema bancario.

Bitcoin nació como una blockchain con el objetivo de realizar transacciones de manera descentralizada, siendo descentralizada tanto la emisión de la moneda —bitcoin— como la transacción al ser entre pares sin intermediarios. Además, presentaba una característica diferencial con respecto a la emisión de moneda fiduciaria por parte de los Estados: la emisión de bitcoin está limitada a un máximo de 21 millones de unidades.

El 22 de mayo de 2010 se dio un hito en la historia de Bitcoin que hasta el día de hoy se sigue celebrando. El programador Laszlo Hanyecz compró dos pizzas de Papa John's a un forista de BitcoinTalk, por un total de 10.000 bitcoins, naciendo el denominado Bitcoin Pizza Day. Este hecho tuvo un doble efecto: por un lado, demostró que el sistema funciona para una transacción persona a persona y, por el otro, le dio un precio de referencia a bitcoin al establecerse que 10.000 bitcoins valían 41 dólares.

En 2013 salió a la luz "The Silk Road", un marketplace en la darkweb creado por Ross Ulbricht en el año 2011, donde se podían adquirir estupefacientes y otros productos prohibidos, pagándose con bitcoin. A partir de este caso, bitcoin empieza a ser conocido para el público en

general. Representó el primer gran caso de utilización de bitcoin para fines criminales, situación que manchó a bitcoin al quedar señalado como moneda utilizada por delincuentes.

En diciembre de 2014, Vitalik Buterin vislumbró un futuro donde la blockchain podría usarse para mucho más que registrar transacciones monetarias y publicó "Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform", un whitepaper proponiendo una plataforma que soportara contratos inteligentes y aplicaciones descentralizadas. El objetivo era claro: pasar de una red diseñada únicamente para transacciones a una plataforma programable que pudiera ejecutar cualquier tipo de aplicación descentralizada.

El fenómeno de las criptomonedas o criptoactivos no se puede explicar simplemente con Bitcoin; es necesario reconocer que la aparición de Ethereum abrió el panorama a la creación de los millones de tokens y criptomonedas que existen actualmente, los contratos inteligentes, las finanzas descentralizadas (DeFi), los NFT (Token No Fungibles), las DAO (Organizaciones Autónomas Descentralizadas), DEX (Exchange Descentralizado), casas de apuestas descentralizadas y consecuentemente todo un sinfín de posibilidades nuevas para la comisión de ilícitos.

2.2. Aspectos técnicos

Para entender el fenómeno es necesario describir algunos conceptos técnicos que operan como base de su funcionamiento. Comencemos con las definiciones de criptomoneda y blockchain.

Se entiende por criptomoneda aquel medio digital de intercambio que utiliza la criptografía para asegurar sus transacciones financieras, controlar la creación de nuevas unidades y verificar la transferencia de activos.

A su vez, la tecnología blockchain, o tecnología de registro distribuido (DLT, sus siglas en inglés), es una base de datos que permite almacenar información de manera descentralizada, segura y transparente, y se basa en una red de computadoras (nodos) que mantienen y validan un registro compartido de transacciones o datos. Este registro no está controlado por una entidad central, lo que lo hace resistente a manipulaciones y ataques.

Algunas de las características principales de la tecnología blockchain son:

- Descentralización: no depende de un servidor central. La información se distribuye entre todos los participantes de la red.
- Transparencia: todos los usuarios tienen acceso al registro, lo que facilita la verificación de transacciones o datos.
- Inmutabilidad: una vez que se registra una transacción en un bloque y este se añade a la cadena, no se puede modificar sin alterar todos los bloques subsiguientes, lo que garantiza la seguridad del sistema.
- Seguridad: utiliza criptografía para asegurar la identidad de los participantes y la integridad de las transacciones.

Un aspecto central es la noción de red distribuida como característica clave de las blockchain, en contraste con las monedas fiduciarias, ya que operan sin intermediarios y confían en el propio sistema sin depender de nodos centrales o hubs con roles de control superior.

Es importante aclarar que las características reseñadas se corresponden con Bitcoin, pero que en su totalidad o mayoría han sido adoptadas por otras blockchain. Sin embargo, pueden existir blockchain privadas como Monero, o blockchain centralizadas o poco descentralizadas, lo que representa un riesgo para los usuarios porque quien controle la mayoría de los nodos podría manipular la red.

Mecanismos de consenso

Comprender cómo funcionan las criptomonedas y la tecnología blockchain requiere conocer cuáles son los procedimientos que se utilizan para validar y agregar transacciones en una cadena de bloques, los cuales son llamados mecanismos de consenso. La validación de las transacciones mediante estos mecanismos produce el cierre del bloque y, en recompensa, quienes producen esa validación reciben una compensación en el token nativo de esa blockchain.

Los mecanismos más utilizados son la prueba de trabajo (Proof of Work, PoW) y la prueba de participación (Proof of Stake, PoS):

- Prueba de trabajo (PoW): mecanismo introducido por primera vez con Bitcoin. Los mineros compiten para resolver un problema matemático complejo (un hash). El primer minero en resolver

el problema agrega un bloque de transacciones a la cadena y recibe una recompensa. Este problema es difícil de resolver pero sencillo de verificar, lo que garantiza que todos puedan validar el trabajo realizado.

- Prueba de participación (PoS): alternativa que supera el alto consumo energético del PoW. Se utiliza en Ethereum 2.0 y Cardano, entre otras. En lugar de depender del poder computacional, PoS selecciona validadores de manera proporcional a la cantidad de criptomonedas que poseen y bloquean (staking) como garantía. Si el validador actúa deshonestamente, pierde parte o todo el capital en staking, lo que desincentiva los comportamientos maliciosos.

Billeteras o Wallets

Los criptoactivos siempre se alojan en la blockchain, por lo cual se requiere de un puente de acceso para interactuar con ella. Esos instrumentos se conocen como billeteras o wallets, los cuales poseen direcciones públicas para recibir transferencias y una clave privada contenida en la denominada frase semilla o seed phrase, que permite abrir o recuperar la billetera en cualquier dispositivo. Quien posea la frase semilla puede acceder a los criptoactivos vinculados a esa wallet.

Las billeteras pueden ser centralizadas o descentralizadas. En el primer caso, el titular delega la custodia en un tercero, generalmente un exchange. En el segundo caso, el usuario es poseedor de la frase semilla y responsable de la custodia de los fondos. De acuerdo a datos de la empresa Ledger, se estima que hay entre 2,3 y 3,7 millones de bitcoins perdidos por haber extraviado u olvidado la frase semilla (Ledger Academy, s/f).

La distinción entre billeteras frías o calientes (cold o hot wallet) se refiere a la necesidad de mantenerse conectado a internet para acceder. La distinción entre software o hardware wallet hace referencia a la utilización o no de un dispositivo físico como capa adicional de seguridad.

Tokens

Un token es una representación de valor, por lo cual abarca, pero no se limita, a las criptomonedas. Toda blockchain tiene un token nativo (por ejemplo, Bitcoin/bitcoin, Ethereum/Ether, etc.) con el cual se transacciona dentro de la misma.[6] A través de contratos inteligentes se pueden crear tokens con diferentes utilidades.

La diferencia entre criptomoneda y token es relevante: la criptomoneda es el token nativo de una blockchain y tiene como función utilizarse para pagar los costos o tarifas de transacción (Gas Fee), mientras que el token es un contrato inteligente creado dentro de una blockchain determinada. Este punto es fundamental tenerlo presente en el marco de un secuestro o decomiso de criptoactivos en billeteras descentralizadas, porque de no tener saldo suficiente de la criptomoneda de la blockchain utilizada no se puede realizar el secuestro o decomiso.

Una cantidad importante de tokens se lanzaron a través de ICOs (Initial Coin Offerings). El período 2017-2018 fue destacado por una gran cantidad de fraudes relacionados con ICOs, ya que numerosos proyectos fraudulentos aprovecharon la falta de regulación y el entusiasmo de los inversores para cometer estafas.

Las criptomonedas y tokens pueden clasificarse de la siguiente manera:

- Por emisión: de emisión limitada o ilimitada. Bitcoin tiene una emisión máxima de 21 millones; Ether tiene emisión ilimitada.
- Fungibilidad: fungibles o no fungibles. Los no fungibles son los NFT (Non Fungible Token), por ejemplo el arte digital.
- Stablecoins: criptoactivos con mecanismo de estabilización de precio, referenciados en moneda fiat o activo financiero como el dólar o el oro.
- Memecoins: criptomonedas creadas como broma o meme. La pionera y más conocida es Dogecoin.

6- La recompensa que reciben los mineros o stakers por mantener la blockchain se paga en criptomoneda; por ejemplo, los mineros de Bitcoin reciben bitcoin y los stakers de Ethereum reciben ether.

- Utility tokens: tokens que proporcionan acceso a un producto o servicio. Incluyen los tokens de gobernanza, que se utilizan para proponer y votar cambios en un protocolo.
- Security tokens: tokens que representan derechos de propiedad en un activo subyacente como acciones, bonos o bienes raíces.
- Orientados a la privacidad: criptomonedas diseñadas para proporcionar transacciones más privadas o seguras. Monero (XMR) es un ejemplo, donde no se pueden ver públicamente las transacciones de la blockchain.

En particular sobre los NFT (Non Fungible Token) cabe señalar que representan un mundo amplio y en constante crecimiento: cualquier actividad que requiera un token único e irrepetible puede ser considerado un NFT. Además de su conocido uso en arte digital y juegos, podrían ser NFT documentos como diplomas, escrituras u oficios judiciales.

Bridge o puente

El puente o bridge en el ecosistema cripto es una conexión que permite la transferencia de tokens y/o datos de una cadena a otra. Las blockchain en el entorno descentralizado no interactúan entre sí —por ejemplo, no se puede enviar bitcoin desde la blockchain de Bitcoin hacia la de Ethereum—, pero el puente proporciona una forma compatible de interoperar de forma segura en ambos lados.

Esto dificulta la trazabilidad de las transacciones por más que la blockchain sea pública. Para clarificar la idea: es como cambiar de libro contable, debiendo ir a buscar el asiento contable correspondiente a otro libro, con el detalle de que no hay reglas contables estandarizadas, ya que cada blockchain tiene sus propias reglas.

Mixers o mezcladores

En el ecosistema de las criptomonedas existen servicios diseñados para aumentar la privacidad y el anonimato de las transacciones

llamados **mixers o mezcladores** (también conocidos como coin join o tumbling services). El funcionamiento consiste en mezclar las transacciones de diferentes usuarios para dificultar o hacer imposible rastrear el origen y el destino. Si bien estas herramientas tienen aplicaciones legítimas en la protección de la privacidad, también han sido utilizadas en actividades ilegales, como el lavado de dinero o la evasión de sanciones (Santos, 2021).

DeFi o Finanzas Descentralizadas

Los **protocolos de finanzas descentralizadas** (DeFi por su sigla en inglés) presentan un serio desafío desde el punto de vista de la contabilidad y la normativa por la complejidad y amplitud del fenómeno. Según el sitio defillama.com, se listan más de 6.300[7] protocolos o proyectos DeFi, con una amplia gama de objetivos: préstamos y ahorro, exchanges descentralizados, juegos NFT y otras categorías.

Destacamos dos formas de DeFi con amplia difusión: los protocolos de préstamos y los exchanges descentralizados.

En el caso de los protocolos de préstamos, el usuario debe dejar una cierta cantidad de tokens como garantía para que se otorgue un préstamo de valor inferior a la garantía. Si el valor de mercado del token disminuye y la garantía no alcanza a cubrir el monto del préstamo, se procede a la liquidación automática. Al ser un sistema automatizado por contratos inteligentes, no existe un margin call en formato de correo electrónico, con lo cual es responsabilidad de cada usuario monitorear el estado de su garantía.

Por otro lado, los exchanges descentralizados (DEX) premian a quienes proporcionan liquidez con tasas de interés y comisiones sobre las transacciones realizadas. También pueden otorgar nuevos tokens que representan ese aporte al pool de liquidez y pueden ser utilizados para generar ganancias en el mismo protocolo o en otros dentro de la misma blockchain. Esta última maniobra de enlazar activos en diferentes protocolos DeFi se conoce como “DeFi lego”.

7- A la fecha del 11/04/2026.

DAO (Decentralized Autonomous Organization) u Organización Autónoma Descentralizada

Una DAO es una organización que funciona de manera completamente automatizada y democrática, donde los participantes toman las decisiones a través de su voto. Un ejemplo histórico es MakerDAO[8], la creadora de la stablecoin DAI.

Sin embargo, la primera DAO fue "The DAO", un proyecto innovador lanzado en mayo de 2016 en la blockchain de Ethereum. Los participantes podían comprar tokens (llamados DAO tokens) a cambio de Ether (ETH) y votar sobre las propuestas de inversión. Era una idea revolucionaria, ya que permitía a los inversores participar directamente en decisiones importantes sin intermediarios.

Sin embargo, The DAO tenía una vulnerabilidad en el código del contrato inteligente que permitía retirar ETH varias veces antes de que se actualizara el saldo. Esa vulnerabilidad fue utilizada por un hacker para retirar millones de dólares en ETH. Este hackeo abrió un debate sobre la inmutabilidad de la blockchain. La decisión mayoritaria de la comunidad de Ethereum fue violar la inmutabilidad con el objetivo de fortalecer la confianza, generando una bifurcación donde Ethereum borró el hackeo de su historia y por el otro lado nació Ethereum Classic, que tiene dentro de su registro el hackeo a The DAO.

2.3. Pseudonimato y globalización: características desafiantes del ecosistema cripto

Si bien la blockchain es pública y cualquier persona puede conocer su contenido, las transacciones y billeteras están denominadas en números alfanuméricos, no identificables, configurándose lo que se conoce como el pseudoanonimato: se conoce la existencia de una billetera y se pueden rastrear todos sus movimientos, pero se desconoce la identidad de su titular y de las personas con quienes transacciona.

La capacidad de realizar transacciones de manera relativamente anónima o bajo seudónimos puede atraer a individuos que buscan ocultar actividades ilícitas, como lavado de dinero o financiamiento

8- Actualmente cambió de nombre a Sky. El whitepaper original de MakerDAO está disponible en: https://makerdao.com/es/whitepaper/

del terrorismo. Dentro de este punto debe señalarse el uso malicioso de los bridges y mezcladores con el fin de ocultar el destino de fondos obtenidos por actividades ilícitas.

A su vez, el entorno digital y descentralizado borra las fronteras de los Estados, dando como resultado que el ecosistema cripto opere de manera global las 24 horas, los 365 días del año. Este ecosistema global dificulta la persecución porque la víctima puede estar en un país A, la plataforma o software ser de un país B y el criminal estar en un país C con una nacionalidad D. Se pueden plantear como dificultades en la investigación la necesidad de librar exhortos a otros países, comunicaciones virtuales con plataformas no registradas en Argentina y conflictos de competencia.

Tornado Cash

El caso de Tornado Cash ha sido emblemático. Tornado Cash es un protocolo de privacidad construido en la blockchain de Ethereum que actúa como un mezclador descentralizado. Se descubrió que hackers y grupos criminales, como el grupo Lazarus, usaban Tornado Cash para lavar grandes cantidades de criptomonedas robadas. Un caso destacado es el ataque al Ronin Bridge (el puente del juego Axie Infinity), donde los hackers utilizaron Tornado Cash para ocultar parte de los 625 millones de dólares sustraídos.

En agosto de 2022, el Departamento del Tesoro de los Estados Unidos, a través de la Oficina de Control de Activos Extranjeros (OFAC), incluyó a Tornado Cash en la lista de entidades sancionadas, prohibiendo a los ciudadanos y empresas estadounidenses interactuar con el protocolo.

Las sanciones impuestas por la OFAC generaron un debate significativo en la comunidad criptográfica sobre la privacidad y la descentralización. Muchos defensores argumentaron que sancionar un protocolo descentralizado es problemático, ya que el código es de código abierto y puede ser utilizado por cualquier persona en el mundo, sin intervención de sus creadores originales. En agosto de 2022, las autoridades neerlandesas arrestaron a uno de los desarrolladores de Tornado Cash, acusándolo de ayudar a facilitar el lavado de dinero mediante el protocolo.

3. Reseña histórica de la Inteligencia Artificial

La empresa IBM (IBM, s/f) ha publicado una definición de Inteligencia Artificial (en adelante IA) en la que la describe como "una tecnología que permite a ordenadores y máquinas simular las capacidades humanas de aprendizaje, comprensión, resolución de problemas, toma de decisiones, creatividad y autonomía. Las aplicaciones y dispositivos equipados con IA pueden ver e identificar objetos, comprender y responder al lenguaje humano, aprender de nueva información y experiencia, hacer recomendaciones detalladas a los usuarios y expertos, y actuar de forma autónoma —por lo que no es necesaria la inteligencia o intervención humana—."

El desarrollo de esta tecnología fue conocido a nivel mundial a partir del 30 de noviembre de 2022 cuando la empresa OpenAI lanzó al mundo ChatGPT, un modelo de inteligencia artificial generativa, que rápidamente se masificó; tanto es así que "ChatGPT" pasó a formar parte de nuestro lenguaje cotidiano como lo era "Googlear".

Sin embargo, la historia de la IA se remonta a mediados del siglo XX. Como señala John McCarthy: "Después de la Segunda Guerra Mundial, varias personas comenzaron a trabajar de forma independiente en máquinas inteligentes. El matemático inglés Alan Turing fue posiblemente el primero. Dio una conferencia sobre el tema en 1947. También fue posible que fuera el primero en decidir que la mejor manera de investigar la IA era programando computadoras en lugar de construyendo máquinas. A finales de la década de 1950, había muchos investigadores en IA, y la mayoría basaba su trabajo en la programación de computadoras" (McCarthy, s/f).

En la cultura popular la idea de la IA se fue desarrollando a través de la ciencia ficción, siendo dos ejemplos 2001: Odisea del espacio de Stanley Kubrick y Terminator de James Cameron. Un símbolo del avance de la computación sobre el ser humano se dio cuando en 1997 el programa Deep Blue, desarrollado por IBM, derrotó al campeón mundial de ajedrez Gary Kasparov.

A diferencia del mundo de las criptomonedas, desde la aparición de ChatGPT hasta el momento, la adopción de la IA para la vida cotidiana creció de manera vertiginosa. Al tener una forma de acceso muy sencilla a través de una charla, la IA nos asiste en nuestra vida

diaria respondiendo preguntas, creando imágenes a partir de simples instrucciones y agilizando las tareas laborales.

Para iniciar una primera aproximación al fenómeno de la IA relacionada a la criminalidad compleja o económica, es importante tomar en cuenta lo señalado por Europol en el año 2023: "Además de generar lenguaje similar al humano, ChatGPT es capaz de producir código en distintos lenguajes de programación [...] Una de las áreas delictivas en las que esto podría tener un impacto significativo es el cibercrimen. Con la versión actual de ChatGPT ya es posible crear herramientas básicas para diversos fines maliciosos [...] esto ya representa un punto de partida para el cibercrimen, ya que permite que alguien sin conocimientos técnicos pueda aprovechar un vector de ataque contra el sistema de una víctima" (Europol 2023).

4. Interconexión entre criptoactivos e inteligencia artificial en el marco de la criminalidad compleja

Una vez revisados los aspectos históricos y técnicos que explican el surgimiento y funcionamiento tanto de los criptoactivos como de la inteligencia artificial, resulta necesario observar cómo estas tecnologías, originalmente diseñadas para fines legítimos, han sido progresivamente incorporadas al accionar delictivo en el entorno digital. La combinación de sistemas descentralizados con herramientas de automatización y análisis avanzado ha ampliado las posibilidades operativas del cibercrimen, dando lugar a modalidades más complejas, veloces y difíciles de rastrear.

4.1. Criptoactivos y el uso de IA en el cibercrimen

Si bien Europol en diversos informes señala al phishing y el ransomware como los principales ciberdelitos en los cuales se utiliza IA, en este trabajo se pretende mostrar someramente la utilización más sofisticada de las herramientas de IA y el uso de criptoactivos como objeto del delito, mostrando la amplitud del entorno digital.

La integración de criptoactivos con inteligencia artificial ha permitido a los delincuentes mejorar la sofisticación de sus técnicas de lavado de dinero, hackeos, manipulación de mercado y fraude. La naturaleza anónima de las criptomonedas y la capacidad de la IA para

analizar grandes volúmenes de datos y automatizar transacciones ha dado lugar a nuevos riesgos en el ámbito del cibercrimen.

TRM Labs (s/f) plantea una serie de ciberdelitos generados u optimizados por la IA, siendo los más relevantes los siguientes:

- Servicios automatizados de blanqueo y mezcla de dinero: los algoritmos basados en IA están aumentando la eficacia de las técnicas de blanqueo de criptomonedas. Los delincuentes utilizan mezcladores impulsados por IA para ocultar los rastros de las transacciones mediante el análisis de patrones de blockchain y el ajuste dinámico de los flujos de transacciones para evadir la detección. Estas estrategias basadas en IA dificultan cada vez más el seguimiento de los fondos ilícitos.
- Explotación de Smart Contracts y piratería basada en IA: la IA está acelerando el descubrimiento y la explotación de vulnerabilidades en smart contracts y los protocolos DeFi. Las herramientas automatizadas escanean las redes blockchain en busca de fallos y ejecutan los exploits más rápido que los hackers humanos, provocando cuantiosas pérdidas financieras.
- Robots de IA para manipular el mercado: los robots de negociación basados en IA pueden manipular los mercados de criptomonedas mediante prácticas como el lavado de operaciones, la suplantación de identidad y el front-running. Estos bots analizan las tendencias del mercado en tiempo real y realizan miles de operaciones por segundo para crear falsas señales de mercado.

Reportes de Chainalysis señalan que durante 2023 el volumen de transacciones vinculadas a actividades ilícitas superó los 22.000 millones de dólares a nivel global (Chainalysis, 2024).

La inteligencia artificial en la prevención e investigación de la criminalidad con criptoactivos

La IA en el análisis forense de criptoactivos está evolucionando rápidamente, y las autoridades internacionales están empezando a utilizar algoritmos avanzados de aprendizaje automático para rastrear las transacciones ilícitas. Europol e Interpol, en su colaboración con agencias de seguridad cibernética y reguladores financieros, han comenzado a utilizar IA para desarrollar sistemas más robustos de monitoreo de blockchains y detectar patrones de transacciones sospechosas. En 2024, Europol informó que una de las tendencias emergentes en los mercados de criptoactivos es el uso

de plataformas descentralizadas para lavar dinero, una práctica que se está facilitando con la incorporación de IA en las transacciones (Europol 2024).

El uso de la IA en la lucha contra el crimen financiero ha demostrado ser invaluable. Empresas como Chainalysis han implementado tecnologías basadas en IA para rastrear transacciones vinculadas a actividades ilícitas. Según su informe de 2025, la compañía ha identificado un aumento en el uso de criptomonedas en actividades delictivas, y cómo sus sistemas avanzados de análisis han ayudado a las autoridades a seguir el rastro de fondos ilegales y desmantelar operaciones criminales.

En Estados Unidos, organismos regulatorios como la Securities and Exchange Commission (SEC) han comenzado a integrar la IA en sus investigaciones de fraudes financieros dentro del mercado de criptoactivos (2025). La detección de esquemas Ponzi y estafas piramidales se ha vuelto más precisa mediante el uso de algoritmos de aprendizaje automático que pueden analizar flujos de transacciones de manera más rápida y eficiente que los métodos tradicionales.

5. Conclusión: la tecnología como desafío continuo en la lucha contra el crimen

A lo largo de este trabajo, se ha intentado recorrer, necesariamente de manera introductoria, un fenómeno que se encuentra en plena transformación: la convergencia entre criptoactivos, tecnologías descentralizadas y herramientas avanzadas de procesamiento de datos, en su vínculo con la criminalidad económica. En ese recorrido, se advierte que el lavado de activos ya no puede pensarse únicamente desde las categorías tradicionales, sino que exige ser comprendido dentro de un ecosistema digital caracterizado por la velocidad, la fragmentación y la descentralización.

En efecto, la tecnología blockchain y las finanzas descentralizadas han habilitado nuevas formas de circulación del valor que, al mismo tiempo que generan oportunidades económicas, ofrecen también escenarios propicios para la ocultación y disimulación de activos de origen ilícito. La posibilidad de transferir fondos a través de múltiples direcciones, redes y servicios, en cuestión de segundos, desafía las

lógicas clásicas de trazabilidad y pone en tensión las herramientas investigativas disponibles.

En este contexto, la irrupción de tecnologías emergentes —entre ellas, la inteligencia artificial en sus diversas aplicaciones— contribuye a profundizar la sofisticación de estas dinámicas, ya sea mediante la automatización de operaciones, el análisis masivo de datos o la optimización de estrategias de ocultamiento. Así, el delito económico se desplaza hacia formas cada vez más complejas, menos visibles y más difíciles de aprehender desde los marcos tradicionales.

Sin embargo, el problema no reside únicamente en la evolución de las prácticas delictivas, sino también en las capacidades estatales para enfrentarlas. En el caso argentino, las diferencias en recursos tecnológicos, formación especializada y desarrollo institucional entre el nivel nacional y los ámbitos subnacionales revelan un escenario heterogéneo, en el cual la respuesta frente a este tipo de criminalidad resulta, en muchos casos, fragmentaria e insuficiente.

No obstante, el mismo proceso que complejiza el problema ofrece también herramientas para su abordaje. La posibilidad de analizar transacciones en blockchain, reconstruir flujos financieros y articular mecanismos de cooperación internacional abre nuevas perspectivas para la investigación del lavado de activos. En este sentido, el desafío no es meramente normativo, sino fundamentalmente estratégico: comprender las tecnologías, incorporarlas críticamente y desarrollar capacidades institucionales acordes a su nivel de complejidad.

Todavía es posible, en este escenario, construir respuestas eficaces. Pero esa posibilidad se encuentra directamente condicionada por la decisión de actuar con anticipación, invertir en conocimiento y asumir que la evolución tecnológica no es un fenómeno futuro, sino una realidad presente. En esa tensión entre cambio e inercia se juega, en definitiva, la capacidad del sistema penal para responder a las formas contemporáneas de la criminalidad económica y evitar que la innovación tecnológica se traduzca, simplemente, en nuevas formas de impunidad.

Bibliografía

Buterin, V. (2014). *Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform*. Ethereum Foundation.

Chainalysis. (2024). *Crypto Crime Report 2024*. Chainalysis Inc.

Chainalysis. (2025). *Crypto Crime Report 2025*. Chainalysis Inc.

DeFi Llama. (2026). *Listado de protocolos DeFi*. https://defillama.com/

Europol. (2023). *Tech Watch Flash: ChatGPT – The impact of Large Language Models on Law Enforcement*. Europol.

Europol. (2024). *Common Challenges in Cybercrime 2024*. Europol.

IBM. (s.f.). *¿Qué es la inteligencia artificial?* https://www.ibm.com/es-es/think/topics/artificial-intelligence

Ledger Academy. (s.f.). *How many Bitcoin are lost?* https://www.ledger.com/academy/topics/economics-and-regulation/how-many-bitcoin-are-lost-ledger

MakerDAO. (s.f.). *MakerDAO Whitepaper*. https://makerdao.com/es/whitepaper/

McCarthy, J. (s.f.). *What Is Artificial Intelligence?* Stanford University.

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. https://bitcoin.org/bitcoin.pdf

Reuters. (2008). *Fall of Lehman*. https://www.reuters.com/news/picture/fall-of-lehman-idUKRTR27V57/

Santos, M. (2021). *Mixers y mezcladores en criptomonedas*. [Referencia interna].

Securities and Exchange Commission. (2025). *Press Release 2025-42*. https://www.sec.gov/newsroom/press-releases/2025-42

TRM Labs. (s.f.). *AI-enabled crime*. https://www.trmlabs.com/es/glossary/ai-enabled-crime

Estudio del caso “Lazarte Di Lieto” desde una perspectiva de análisis económico forense en un contexto signado por el uso masivo de criptomonedas en Argentina

Walter R. Chiquiar[1] y Lucas Paulinovich[2]

Resumen

El trabajo analiza el fallo “Lazarte Di Lieto” (CCC 60100/2022/CA1), que confirma el procesamiento de un asesor en criptoactivos acusado de apropiarse de 24,5 BTC de su cliente. Durante una asistencia presencial en junio de 2022, el imputado migró los bitcoins de la víctima a una billetera física (Ledger Nano) y, según la acusación, conservó después el acceso a la frase semilla. En agosto de 2022 los fondos pasaron por Wasabi Wallet y CoinJoin, se dispersaron entre cientos de direcciones y, entre el 12 y el 29 de agosto, reingresaron a una cuenta Binance a nombre del imputado por 22,47 BTC, un volumen casi idéntico al sustraído. Los autores sostienen que la Cámara acierta al reconocer a los criptoactivos como bienes inmateriales susceptibles de apropiación y

1- Contador Público (UBA). Licenciado en Administración (UBA). Docente autorizado (UBA). Magister en Contabilidad Internacional (UBA). Doctor de la Universidad de Buenos Aires, Área Ciencias Económicas. Subárea Contabilidad. Profesor Titular UBA, UNQ y UNLP. Profesor de posgrado en universidades nacionales y Profesor invitado en universidades del exterior. Perito Oficial, Cuerpo de Peritos del Poder Judicial de la Nación, Especializados en Casos de Corrupción y Delitos contra la Administración Pública, dependiente de la Corte Suprema de Justicia de la Nación. Correo: wchiquiar@yahoo.com.ar

2- Ha desarrollado estudios en diversos niveles dentro de las áreas de criminología, seguridad, defensa, inteligencia, economía y finanzas. Cuenta con una trayectoria de más de 13 años desempeñándose como redactor y editor en diferentes medios de comunicación. En la actualidad, desarrolla tareas de consultoría tanto en el ámbito público como en el privado. Correo: lpaulinovich@gmail.com

al fundar el procesamiento en un conjunto de indicios convergentes (coincidencia cuantitativa, proximidad temporal, uso de mezcladores y actividad previa casi nula), sin exigir una trazabilidad lineal perfecta.

Sin embargo, el estudio señala omisiones que debilitan la motivación del fallo: no se analiza el historial patrimonial previo del imputado, no se examinan clústeres ni grafos transaccionales pese a la dispersión en cientos de direcciones, y no se evalúan con detalle hipótesis alternativas, como el acceso de un tercero a la frase semilla o la posible coincidencia fortuita generada por un mezclador. Como aporte metodológico, proponen integrar en la investigación penal económica una teoría del caso explícita, una matriz de consistencia patrimonial, series temporales de flujos y análisis de clústeres y grafos, de modo que la prueba indiciaria resulte más sólida y controlable en instancias revisoras.

1. Introducción

El fallo Lazarte Di Lieto (CCC 60100/2022/CA1) se dicta en un contexto social signado por el uso masivo de criptomonedas en Argentina como refugio económico en un entorno de alta inestabilidad monetaria; una alta incidencia de estafas y ciberdelitos vinculados a criptoactivos como efecto a la proliferación de oportunidades ligadas a las brechas técnicas y de conocimiento; vacíos normativos que obligaban a los jueces a reconceptualizar jurídicamente los criptoactivos; preocupación creciente por el lavado de dinero mediante técnicas de anonimización (mixers[3] y coinjoin[4]); emergencia

3- Un mixer es un servicio en línea que reúne criptomonedas de varios usuarios y luego les envía criptomonedas "limpias" en diferentes cantidades, para ocultar el rastro de auditoría de los fondos contaminados. Estos servicios tienen como objetivo impedir que las criptomonedas fraudulentas sean rastreadas hasta su origen o hasta su destino final, ocultando el rastro de las transferencias potencialmente identificables. Estructurar las transacciones de esta manera dificulta que las fuerzas del orden y los investigadores de blockchain puedan rastrear eficazmente el flujo de fondos provenientes de esquemas fraudulentos y actividades delictivas. Disponible en: https://www.fraudinvestigation.net/cryptocurrency/tracing/mixers-and-coinjoin [consultado el 15/03/2026].

4- CoinJoin es una transacción de Bitcoin que mejora la privacidad, ya que combina las aportaciones de numerosos usuarios y devuelve múltiples salidas con valores idénticos. A diferencia de otros servicios de mezcla, los usuarios conservan la custodia de sus fondos durante todo el proceso. Disponible en: https://www.fraudinvestigation.net/cryptocurrency/tracing/mixers-and-coinjoin [consultado el 15/03/2026].

de servicios de “expertos” informales en temas cripto y creación de dependencia técnica de usuarios; y aceleración de la vida financiera digital postpandemia.

El fallo refleja, en esencia, la necesidad del Poder Judicial de adaptar categorías jurídicas tradicionales a nuevas formas de criminalidad digital y patrimonial, en un país donde la economía cripto creció más rápidamente que su marco normativo. El desarrollo de los criptoactivos como forma de inversión, medio de pago y reserva de valor ha complejizado la criminalidad económica tradicional: operaciones de alto impacto patrimonial pueden ejecutarse en minutos, desde un dispositivo doméstico y mediante herramientas de pseudonimato que tensionan los esquemas clásicos de control.

Por otra parte, muchas personas sin conocimientos técnicos recurren a “asesores cripto” informales (como ocurrió en el caso del querellante) presentando una vulnerabilidad relacionada al control de las operaciones. Esta realidad social, habilitó nuevas formas de fraude, donde las víctimas dependían del conocimiento técnico de terceros, tal como se describe en la causa.

González Busquin (2023) señala con claridad que el vertiginoso desarrollo de las tecnologías de la información y la comunicación ha tensionado profundamente los cimientos sobre los que se asienta la dogmática penal, comprometiendo el alcance y la operatividad de los tipos penales tradicionales, los cuales resultan crecientemente insuficientes frente a una realidad tecnológica que evoluciona a un ritmo sin precedentes.

Cabe advertir que en 2023 aún no existía normativa penal o civil específica sobre criptoactivos, por lo cual el fallo evidencia este vacío regulatorio y el debate doctrinario y jurisprudencial. Esto es, no se encontraba zanjada la discusión sobre si los criptoactivos son “cosas” u “objetos” en el sentido del Código Penal, su inclusión como bienes inmateriales según el art. 16 del CCyC y su clasificación a efectos del delito de hurto, estafa o apropiación indebida. La propia sentencia dedica varios párrafos a fundamentar por qué los bitcoins deben considerarse bienes susceptibles de tenencia y, por lo tanto, objeto de delitos patrimoniales. Todo lo cual muestra un contexto jurídico transicional, donde los tribunales estaban construyendo criterios interpretativos frente a nuevas tecnologías.

Así pues, los conflictos penales vinculados a la apropiación de criptomonedas ponen a prueba la capacidad del sistema de justicia para traducir categorías como "cosa", "apoderamiento", "engaño" y "perjuicio patrimonial" a un entorno técnico y económico radicalmente distinto.

El caso Lazarte Di Lieto se inscribe en ese punto de fricción. Un asesor en criptoactivos, convocado para asistir a la víctima en la migración de sus bitcoins desde una plataforma de intercambio hacia una billetera fría, es acusado de haber aprovechado ese acceso técnico privilegiado para sustraer, tiempo después, la totalidad de los fondos.

El problema central no es solo la relación entre asesor y cliente, sino la posibilidad de reconstruir, con estándares de racionalidad probatoria aceptables, la secuencia económica del hecho y la trazabilidad de operaciones realizadas en una blockchain pública, pero sometidas a técnicas de ofuscación y dispersión que complejizan la atribución de autoría.

El propósito del trabajo es doble. Por un lado, analizar críticamente el razonamiento del fallo: su reconstrucción fáctica, el uso de la prueba técnica, la calificación jurídica propuesta y las decisiones implícitas sobre la naturaleza de los criptoactivos como bienes penalmente relevantes. Por otro, formular aportes metodológicos desde el análisis económico-forense para mejorar la investigación y el litigio en casos análogos, especialmente en lo relativo a la identificación de señales patrimoniales sospechosas, el uso sistemático de la trazabilidad en blockchain y la articulación coherente de indicios económicos en el marco del estándar probatorio aplicable a la etapa de procesamiento.

A partir de esto, el trabajo se organiza en torno a tres preguntas guía: si la combinación de coincidencias cuantitativas y trayectorias técnicas resulta suficiente en esa fase procesal para sostener la imputación; qué deficiencias u omisiones pueden detectarse en la investigación y en la explotación de la evidencia económica y tecnológica disponible; y qué aporta el fallo al tratamiento de los criptoactivos en el derecho penal económico contemporáneo.

Lejos de ser una rareza tecnológica, Lazarte Di Lieto condensa rasgos clásicos que encajan en la criminología clásica del delito de cuello blanco (Edwin Sutherland), es decir, delitos cometidos por personas que aprovechan una posición de confianza, conocimiento especializado que otorga asimetrías informativas para obtener un beneficio económico relevante a través de una maniobra técnica y

posición social/funcional, más que la violencia física, todo ello en un entorno tecnológico que exige modelos de análisis más sofisticados.

2. Marco conceptual y antecedentes doctrinarios

El análisis del caso Lazarte Di Lieto requiere articular derecho penal económico, teoría del delito patrimonial, criminalidad tecnológica y análisis económico-forense. No alcanza con examinar la imputación desde la dogmática clásica: es necesario comprender cómo se combinan el abuso de confianza, la arquitectura técnica de la blockchain y la lectura de los flujos patrimoniales generados por la maniobra.

La aproximación de Sutherland al delito de cuello blanco resulta especialmente pertinente. Para el autor, este tipo de criminalidad se caracteriza por el aprovechamiento de una posición de confianza, la disponibilidad de información privilegiada y el uso de capacidades técnicas que permiten producir un perjuicio económico difícil de detectar. Lazarte replica este patrón: el imputado es convocado por su expertise, accede a información crítica —la frase semilla— y utiliza esa ventaja informativa para operar sobre el patrimonio de la víctima sin su conocimiento.

Autores como Klaus Tiedemann y Wolfgang Naucke amplían esta visión al destacar que los delitos económicos trascienden el daño individual y erosionan expectativas institucionales básicas de seguridad, previsibilidad y confianza. En un entorno donde los criptoactivos ocupan un lugar creciente como forma de inversión y reserva de valor, la manipulación de claves privadas o dispositivos de resguardo adquiere una dimensión sistémica: afecta no solo a la víctima, sino a la credibilidad del ecosistema económico que habilita esas transacciones.

En el plano local, los trabajos de Carrara, König y Marsili han contribuido a consolidar una metodología de investigación centrada en la reconstrucción patrimonial, el análisis de flujos y la identificación de señales económicas sospechosas. Este enfoque sistémico —que evalúa cada indicio en relación con el comportamiento económico global del imputado— resulta particularmente adecuado para investigar maniobras con criptoactivos, donde la evidencia directa suele ser limitada y la inferencia se apoya en patrones económicos, técnicos y contextuales.

Como antecedentes jurisprudenciales se releva: a) el primer fallo (2019) de Cripto-Fraude en el Nordeste: "P. H. M. S/ DEFRAUDACIÓN INFORMÁTICA EN CONCURSO REAL CON VIOLACIÓN DE SECRETOS Y DE LA PRIVACIDAD", Expte. Nº 40134/2017-1 de la Provincia del Chaco, donde se consideró que el objeto del delito eran las criptodivisas mismas y se analizaron aspectos probatorios propios del ecosistema blockchain; y b) La sentencia del 02/06/2021, de la Cámara Nacional de Apelaciones en lo Criminal y Correccional, de la C.A.B.A. Sala 05. Jueces: Hernán Martín López — Ricardo Matías Pinto. Id SAIJ: FA21060030. En esta última se confirma el sobreseimiento de la presunta comisión del delito de estafa del imputado, que se dedicaba a realizar trading de criptomonedas prometiendo una rentabilidad bimestral, y que fue denunciado por un inversor cuando la operación comenzó a perder rentabilidad, al considerar que no se apreciaba un supuesto con aristas delictivas, sino una inversión de alto riesgo dado por su carácter virtual y la falta de regulación legal. Agrega que no puede desecharse un obrar negligente de parte del querellante, quien pudo haber conocido de antemano los avatares del negocio, o simplemente un actuar voluntario guiado por la ganancia de la operación, lo que impide considerar tipificada la figura penal invocada.

Como caso internacional relevante (España) se observa el primer juicio por una macro estafa vinculada con inversiones en criptomonedas, centrado en la denominada trama Arbistar, operativa entre mayo de 2019 y septiembre de 2020. La Audiencia Nacional (Sección Tercera) juzga a Santiago Fuentes, fundador de Arbistar 2.0 —con prisión preventiva—, a quien se solicitan casi 30 años de cárcel por estafa agravada, organización criminal y falsificación documental, junto con otros seis integrantes de la estructura. Según la investigación del juez, la plataforma prometía rentabilidades del 8% al 15% sin realizar operaciones reales con activos digitales. El caso inicialmente estaba radicado en un juzgado de Tenerife, y luego pasó a la Audiencia Nacional por la magnitud del fraude y su carácter transnacional, con miles de afectados en Europa y América. El perjuicio se estimó inicialmente en 92 millones de euros, aunque la Fiscalía lo elevó a casi 1.900 millones calculando el valor de los casi 30.000 bitcoins incautados según su cotización en 2024. Arbistar reproducía mecanismos típicos de estafas piramidales, como el "plan amigo", altas rentabilidades prometidas y una intensa promoción pública. Al colapsar

el esquema en 2020, los responsables desviaron masivamente los fondos a cuentas personales, generando uno de los mayores fraudes cripto investigados en España[5].

3. Naturaleza jurídica y económica de los criptoactivos

Uno de los ejes conceptuales del fallo es la determinación del estatuto jurídico de los criptoactivos. La Cámara adopta la posición dominante: aunque no constituyan moneda de curso legal, las criptomonedas son bienes inmateriales con valor económico, encuadrables en el art. 16 del Código Civil y Comercial como objetos patrimoniales susceptibles de apropiación.

Esta interpretación es consistente con la normativa y los criterios administrativos vigentes. La UIF, en la Resolución 300/2014, define a las monedas virtuales como representaciones digitales de valor aptas para actuar como medio de intercambio, unidad de cuenta o reserva de valor. La UFECI, en su Guía de 2023, refuerza esta perspectiva al reconocer que la ausencia de corporeidad no excluye a los criptoactivos del concepto de "bien", dado que su control —mediante claves privadas— tiene efectos patrimoniales directos.

El razonamiento también converge con los estándares internacionales del GAFI (2015 y 2019), que consideran a los activos virtuales como valores transferibles con usos económicos equiparables a los de otras formas de inversión o de pago. Este consenso global consolida su aptitud para integrar el patrimonio, ser objeto de apropiación ilegítima y generar un perjuicio patrimonial jurídicamente relevante.

Si bien la jurisprudencia argentina aún es incipiente, las investigaciones y decisiones técnicas de UFECI en casos de phishing y sustracción de criptomonedas, así como algunos conflictos civiles vinculados a la pérdida o apropiación de frases semilla, coinciden en

5- Con fecha 11/03/2026, la Audiencia Nacional elevó las penas al fundador de la plataforma de criptomonedas Arbistar y a su socio, por estafa y por pertenencia a una organización criminal. Entendió que llevaron a cabo una actividad defraudatoria prolongada y sistemática. Fue singularmente agravada habiendo afectado a un gran número de inversores (32.000) con un perjuicio patrimonial de magnitud de 200 millones de euros entre 2019 y 2020. Disponible en: https://www.rtve.es/noticias/20260311/audiencia-nacional-duplica-penas-duenos-plataforma-criptomonedas-arbistar/16975777.shtml

reconocer que la privación del acceso a un wallet constituye un daño real y cuantificable.

En conjunto, estos antecedentes afirman una línea interpretativa clara: los criptoactivos son bienes económicamente relevantes y su apropiación no consentida configura un perjuicio patrimonial susceptible de tutela penal.

4. Reconstrucción económica del hecho

El fallo Lazarte Di Lieto gira en torno a una maniobra de apropiación de criptoactivos ejecutada mediante el aprovechamiento del acceso técnico que el imputado obtuvo durante una asistencia legítima.

La resolución de la Cámara ofrece una base sólida para reconstruir el itinerario delictivo presunto. El punto de partida es una relación de asesoramiento en criptoactivos. El imputado, M. E. Lazarte Di Lieto, fue contactado por la víctima, M. H. H., a través de un tercero (M. T.), quien le había brindado referencias positivas sobre su experiencia en el manejo de wallets y procedimientos de migración de activos digitales.

El trabajo encomendado consistía en migrar 24,5 BTC desde una plataforma virtual (X.V. Ltd.) hacia un dispositivo físico tipo hardware wallet (Ledger Nano), adquirido también a través del imputado. Esta operación es altamente sensible, porque involucra la generación y resguardo de la frase semilla —las 24 palabras que permiten acceso total e irrestricto a la billetera— y el establecimiento del PIN de acceso.

La asistencia se desarrolló presencialmente, en el domicilio de la víctima, entre el 22 y 23 de junio de 2022, momento en el que se completaron tres operaciones de transferencia:

- 22/06/2022 – 10:39 h.
- 22/06/2022 – 23:22 h.
- 23/06/2022 – 16:24 h.

Estas transferencias consolidaron la migración de la totalidad de los bitcoins a la billetera física controlada por la víctima. La Cámara destaca un punto central: luego de esa reunión, la víctima nunca volvió a utilizar la billetera, ni compartió las claves con ninguna otra persona. Este dato se vuelve crucial cuando se analizan posteriormente los movimientos de salida.

El damnificado recién advierte la desaparición de sus criptoactivos el 4 de noviembre de 2022, cuando un conocido le informa que el imputado había sido detenido en otra causa por estafa informática. Al abrir su Ledger Nano, comprueba la ausencia total de fondos.

Esta distancia temporal —entre junio (migración legítima), agosto (movimientos de extracción) y noviembre (descubrimiento)— es característico de defraudaciones basadas en acceso técnico: el autor retiene la semilla o el control del dispositivo, permitiendo ejecutar la apropiación con posterioridad y sin riesgo perceptible para la víctima. Es decir, se da una disociación temporal entre el acto inicial de confianza y la sustracción final.

El punto más relevante en términos económicos es la reconstrucción del movimiento de los fondos luego de la migración. La sentencia describe con precisión la secuencia siguiente:

4.1. Desvío hacia Wasabi y uso de CoinJoin

El 3 de agosto de 2022, los BTC fueron transferidos desde la billetera de la víctima hacia una dirección vinculada al servicio Wasabi Wallet, conocido por implementar CoinJoin, una técnica de mezcla (mixing) diseñada para ofuscar la trazabilidad de las transacciones.

La dirección inicial identificada es:
bc1qjxkgh6cke83ef8rpz0s0jv2wxn874q0jnch3xj

Wasabi y CoinJoin permiten que múltiples usuarios combinen sus transacciones en una sola operación, generando una matriz de entradas y salidas que impide identificar qué fondos corresponden a qué usuario. Desde una perspectiva forense, esto no elimina toda inferencia posible, pero sí reduce la claridad del flujo contable directo.

4.2. Redistribución hacia dos direcciones nuevas

El 9 de agosto de 2022, desde la dirección utilizada en Wasabi se generan dos transferencias:

- A la dirección: bc1qxx4hyfl0pt0acc0mls4hcur660atuhp0xvg680
- A la dirección: bc1qkuh40rx5c8fhdwt7etq7mkw5l2auuzty7erqpd

El fallo destaca dos elementos técnicos de interés:

- Una de las direcciones recibe un monto con un solo decimal,
- La otra recibe un monto con ocho decimales —el máximo permitido en la red Bitcoin—.

Estos patrones suelen ser relevantes para análisis heurísticos: las transacciones con muchos decimales pueden corresponder a saldos residuales o a operaciones automatizadas en mezcladores.

4.3. Vinculación con cuentas identificadas

La Cámara señala que una porción de los BTC fue enviada, ese mismo 9 de agosto, a la dirección 1Gh6WMSq73C2FArDCazPTnjMzmdFNwB2Nz, perteneciente a una cuenta Binance a nombre de J. C. Rojas Prieto. Esto da el primer indicio claro de que los fondos sustraídos entran en contacto con identidades verificables, porque Binance exige validación KYC[6] (Know Your Customer) para operar.

4.4. Dispersión masiva

El 11 de agosto de 2022, desde la dirección bc1qkuh40rx5c8fhdwt7e-tq7mkw5l2auuzty7erqpd, se ejecuta una operación que involucra:

- 315 direcciones de origen,
- 379 direcciones de destino.

Esta maniobra es altamente indicativa del uso de mixers avanzados, típicos en procesos de ofuscación para dificultar la trazabilidad.

4.5. Reingreso de fondos a wallets asociadas al imputado

El núcleo económico del caso —y la base de la imputación— surge al reconstruir el reingreso de los fondos hacia direcciones vinculadas a Lazarte.

La Cámara verifica que entre el 12 y el 29 de agosto de 2022, la dirección bc1qukw20jqn2lktkhav6f0zzxaecm2akalvpqq8sh recibió fondos provenientes de direcciones previamente sometidas a CoinJoin.

En ese mismo período, la billetera Binance a nombre de M. E. Lazarte Di Lieto recibió 22,47 BTC, un volumen prácticamente idéntico al total sustraído de la billetera de la víctima. La diferencia mínima es atribuida a las tarifas de transacción. Además, el tribunal verifica que otra porción menor de los fondos llegó a una wallet asociada a B. Mur, quien mantenía una relación personal con el imputado.

6- KYC: Know Your Customer o "Conoce a tu Cliente" es el conjunto de políticas y procedimientos obligatorios que utilizan bancos y empresas para verificar la identidad de sus clientes, evaluando sus riesgos y legitimidad para prevenir delitos como el fraude, el lavado de dinero y la financiación del terrorismo.

5. Evaluación económica de la coincidencia cuantitativa y temporal

Desde una perspectiva forense, tres elementos adquieren especial relevancia:

- Coincidencia casi perfecta en el volumen total: la suma reingresada se aproxima a los 24,5 BTC sustraídos.
- Coincidencia temporal: los movimientos de ingreso en Binance ocurren inmediatamente después de la dispersión realizada mediante CoinJoin.
- Patrón de actividad anómalo: la wallet de Lazarte tenía escaso movimiento previo y recibe, de manera súbita, un volumen extraordinariamente elevado de activos.

6. Modelo económico del delito

El comportamiento del imputado sigue una estructura típica de fraude tecnológico con conversión patrimonial digital:

- Etapa de captación: Venta y configuración de la billetera fría. Acceso a claves privadas (valor económico digital).
- Etapa de transferencia opaca: Uso de mixer. Destrucción del vínculo directo entre víctima y beneficiario.
- Etapa de recomposición patrimonial: Consolidación del total de BTC en wallets controladas por Lazarte. Beneficio patrimonial equivalente al total sustraído.
- Etapa de diseminación secundaria: Distribución de pequeñas fracciones a terceros. Estrategia de dispersión para dificultar la recuperación.

7. La posición del tribunal

La Cámara sostiene que existe un vínculo técnico y económico suficiente entre la asistencia prestada por el imputado durante la migración del wallet y la posterior sustracción de los fondos. Considera que los movimientos posteriores —incluido el reingreso de un volumen prác-

ticamente idéntico al sustraído hacia wallets vinculadas al imputado— son compatibles con la hipótesis de apropiación ilegítima, y que el uso de servicios de ofuscación como Wasabi/CoinJoin refuerza esa lectura, pues constituye un comportamiento típico de quien procura ocultar el origen de los fondos.

Desde la dogmática penal, el análisis exige revisar la aplicabilidad de las figuras de estafa (art. 172 CP), hurto y defraudación informática (art. 173 inc. 16). En materia de estafa, la estructura típica —engaño, error, disposición patrimonial, perjuicio y nexo causal— enfrenta un desafío particular en delitos con criptoactivos: el acceso inicialmente permitido (entrega de dispositivo, revelación de la frase semilla o asistencia técnica) puede habilitar una apropiación diferida, sin un acto de disposición clásico. Permitir el acceso a la frase semilla es conceptualmente equivalente a habilitar un control patrimonial que el autor explota ulteriormente.

Respecto del hurto, la postura que el fallo adopta es que la falta de corporeidad no impide calificar a los criptoactivos como objetos patrimoniales susceptibles de apoderamiento, pues integran el patrimonio y su sustracción genera un perjuicio real. En cuanto al art. 173 inc. 16, la Cámara lo menciona como alternativa razonable: la manipulación de claves privadas podría constituir alteración maliciosa de un sistema o dato informático, aunque no fija una subsunción definitiva dada la etapa procesal.

La evaluación de los flujos en blockchain requiere una mirada técnica particular. La doctrina internacional distingue entre trazabilidad directa, trazabilidad ofuscada (uso de mixers) y análisis probabilístico contextual. La literatura especializada —como la desarrollada en el ámbito de Chainalysis[7]— coincide en que CoinJoin reduce la precisión de la reconstrucción, pero no elimina la posibilidad de inferencias basadas en patrones cuantitativos, temporales y relacionales.

La Cámara reconoce que no es posible reconstruir cada eslabón del circuito, pero afirma que la combinación de: (i) coincidencia cuantitativa casi exacta, (ii) proximidad temporal de los movimientos y (iii) recepción final en direcciones asociadas al imputado, conforma un conjunto indicia-

7- Chainalysis es una plataforma de datos blockchain, que proporciona datos, software, servicios e investigación a agencias gubernamentales, exchanges, instituciones financieras y empresas de seguros y ciberseguridad en más de 70 países. Sus datos impulsan softwares de investigación, cumplimiento (compliance) e inteligencia de mercado que se han utilizado para resolver algunos de los casos criminales más mediáticos del mundo y para aumentar el acceso seguro de los consumidores a las criptomonedas.

rio suficiente para fundar un procesamiento. Esta posición se alinea con la jurisprudencia comparada en delitos tecnológicos complejos, donde no se exige una trazabilidad lineal perfecta, sino una valoración integral de los indicios económicos disponibles.

Cabe advertir que el núcleo del análisis no se debiera agotar en transacciones aisladas o vínculos directos, sino en la reconstrucción de un circuito económico caracterizado por:

- Múltiples intervinientes;
- Diversidad de vehículos de canalización (personas, cuentas, instrumentos);
- Fragmentación de ingresos y egresos; y
- Dificultad para identificar un beneficiario final único mediante un seguimiento lineal.

Pues, transforma al caso en un supuesto típico de insuficiencia de la trazabilidad de Nivel 1–2, y lo vuelve especialmente apto para un enfoque de Nivel 4 (clústeres + grafos).

El enfoque de Nivel 4, permite abandonar la mirada centrada exclusivamente en personas o cuentas individuales y reconstruir: a) Clúster A: conjunto de cuentas, instrumentos o intermediaciones vinculadas a su esfera de control económico; b) Clúster B: conjunto equivalente, aunque formalmente separado; y c) Clústeres satélite: terceros recurrentes, intermediarios o vehículos instrumentales. Con esta mirada, el interés probatorio no reside en cada elemento aislado, sino en el patrón de coordinación estable entre ellos, permitiendo sostener que:

La reiteración estructural de vínculos económicos sustituye la necesidad de prueba directa de dominio individual; y

El control se acredita por consistencia operativa, y no por titularidad formal.

Creemos que esto es particularmente relevante en Lazarte – Di Lieto, donde la defensa tiende a fragmentar responsabilidades.

Modelado del grafo transaccional del caso

a) Nodos y aristas en clave judicial

Nodos:

- Clústeres de control económico.

- Entidades intermediarias recurrentes.
- Destinos finales de acumulación.

Aristas:
- Flujos de fondos reiterados.
- Secuencias temporales coordinadas.
- Relaciones de dependencia económica.

Es importante destacar que el grafo no procura "descubrir" un hecho nuevo, sino visualizar y explicar lo que ya está en la causa.

b) Métricas relevantes en Lazarte – Di Lieto

Centralidad de intermediación

Permite identificar:
- Nodos que no concentran grandes montos, pero articulan el sistema; y
- Puntos donde la maniobra podría interrumpirse.

Detección de comunidades

Permite mostrar:
- Sub-estructuras relativamente autónomas; y
- División funcional de tareas económicas.

Análisis de convergencia final

Permite evaluar si:
- La dispersión inicial converge en uno o pocos centros de decisión económica; y
- La aparente atomización es solo una fase de layering.

Podemos afirmar que el análisis por grafos permite sostener —sin forzar la prueba— que:
- El beneficiario final no necesita ser identificado como una cuenta o persona única.

Basta con demostrar:
  - Capacidad de disposición.
  - Dirección estratégica del flujo.
  - Aprovechamiento económico sistemático.

Esto es coherente con la lógica del fallo y con estándares en criminalidad económica compleja.

En la búsqueda de la neutralización de la defensa fragmentaria, el enfoque por clústeres debilita la estrategia defensiva que se basa en:

- "Yo solo intervine en esta operación".
- "Esa cuenta no es mía".
- "No hay transferencia directa".

El grafo demuestra que la suma de intervenciones adquiere sentido unitario.

Como síntesis, aplicar explícitamente este enfoque permitiría:

- Reforzar la motivación de la decisión;
- Reducir el margen de arbitrariedad;
- Alinear el fallo con estándares modernos de análisis financiero-criminal; y
- Mejorar su resistencia en instancias revisoras.

Si bien la jurisprudencia argentina[8] no utiliza vocabulario técnico de análisis de grafos, sí reconoce y valora los análisis estructurales de relaciones, funciones y patrones persistentes en causas complejas de lavado de activos y asociación ilícita. Ese reconocimiento es metodológicamente compatible con la técnica de trazabilidad por clústeres y grafos, y en muchos casos alimenta la robustez probatoria de decisiones condenatorias.

8. Análisis crítico del fallo

El fallo Lazarte Di Lieto constituye un intento de adaptar las categorías del derecho penal patrimonial y el criterio de aplicabilidad de estándares probatorios tradicionales a un entorno técnico —blockchain, mixers, claves privadas— que desafía los modelos clásicos de atribución y prueba. La Cámara confirma el procesamiento sobre la base de

8- Fallo de la Cámara Federal de Casación Penal – Báez, Lázaro: El tribunal de alzada articula la prueba de un esquema complejo de lavado a partir de múltiples conductas, relaciones societarias, y roles diferenciados de los imputados. Esto es un ejemplo de evaluación estructural de la maniobra en vez de considerar a los hechos de forma aislada (disponible en: https://www.mpf.gob.ar/procelac-lavado/files/2023/12/Fallo-de-C%C3%A1mara-Federal-de-Casaci%C3%B3n-Penal-B%C3%81EZ-LAZARO-2023.pdf); Casos en los cuales el sistema penal federal articula la conexión entre hechos distribuidos en múltiples expedientes, la valoración de relaciones funcionales y las estructuras de participación: a) Hotesur - Causa penal 11352/2014 (disponible en: https://www.pensamientopenal.com.ar/system/files/fallos89693_0.pdf); y b) Causa Hotesur-Los Sauces – Cámara Federal de Casación Penal (disponible en https://www.pensamientopenal.com.ar/fallos/90996-casacion-sobre-causa-hotesur-sauces-fallo-completo).

un conjunto de indicios económicos y técnicos coherentes, aunque su razonamiento presenta vacíos metodológicos que limitan el alcance del precedente.

Entre los aciertos, se destaca el reconocimiento claro de las criptomonedas como bienes inmateriales con valor económico en los términos del art. 16 del Código Civil y Comercial. El tribunal integra correctamente la normativa administrativa (UIF, UFECI) y los estándares internacionales (GAFI), despejando cualquier duda sobre la aptitud del criptoactivo para ser objeto de apropiación y para generar un perjuicio patrimonial cierto. Pues, evita soluciones anacrónicas, armoniza con la doctrina comparada, y se alinea con la Guía UFECI y estándares internacionales (GAFI).

Asimismo, la Cámara valida la trazabilidad mediante blockchain forensics, y construye un razonamiento indiciario compatible con la lógica de los delitos económicos complejos, donde la prueba directa suele ser escasa. La coincidencia cuantitativa entre lo sustraído y lo reingresado, la cercanía temporal de los movimientos y la actividad previa casi nula del wallet vinculado al imputado constituyen señales patrimoniales relevantes. El tribunal también interpreta adecuadamente el uso de Wasabi/CoinJoin como indicio de ocultamiento, evitando la premisa errónea de que la ofuscación vuelve irrelevante toda inferencia.

El fallo reconoce que en delitos con criptoactivos el "ardid" no siempre se manifiesta en forma clásica, sino que puede derivar de una asimetría informacional y técnica entre autor y víctima. Esta visión se considera moderna y correcta, pues la criminalidad tecnológica se basa justamente en esa desigualdad de conocimiento.

Otro punto relevante es el reconocimiento de que, en contextos de acceso técnico legítimo, la comisión del delito puede diferirse sin que ello rompa la lógica del apoderamiento. Esta lectura evita aplicar mecánicamente categorías pensadas para bienes físicos y refleja una comprensión adecuada de la criminalidad digital contemporánea.

Sin embargo, el fallo presenta omisiones significativas. La Cámara menciona que la wallet del imputado tenía poca actividad previa, pero no profundiza en un análisis patrimonial completo: no examina volúmenes históricos, patrones de trading, origen posible de los fondos o consistencia económica del reingreso. Este déficit es relevante, porque afecta la robustez del razonamiento económico.

También se omite un análisis integral de la operatoria en blockchain. Aunque la sentencia identifica cuatro direcciones relevantes, la maniobra incluyó cientos de direcciones de entrada y salida. La ausencia de un análisis de clústeres, nodos de dispersión o patrones temporales reduce la potencia explicativa de la reconstrucción.

Otro punto débil es la falta de análisis sobre la posible participación de terceros. El fallo menciona que Rojas Prieto y Mur recibieron fondos, pero no evalúa si existe un vínculo económico previo, si esa recepción es compatible con coautoría o receptación, o si forma parte de un patrón de dispersión deliberado. Esta omisión debilita la reconstrucción de la estructura delictiva.

En suma, su fuerza metodológica queda limitada por la ausencia de una teoría del caso económico integral, la subexplotación de la evidencia técnica disponible y la falta de un examen explícito de alternativas razonables. Estos déficits no invalidan la decisión en la etapa de procesamiento, pero sí muestran la necesidad de incorporar herramientas más sofisticadas en futuras investigaciones.

9. Aportes desde el análisis económico-forense

La criminalidad económica vinculada a criptoactivos exige herramientas analíticas distintas a las utilizadas tradicionalmente en delitos patrimoniales. Los criptoactivos no son solo bienes digitales: funcionan como sistemas económicos completos, con dinámicas propias de circulación, anonimización y dispersión que obligan a reconstruir los hechos desde una lógica económica, no meramente técnica ni exclusivamente jurídica.

Todo análisis económico-forense parte de una pregunta central: ¿cuál es la lógica económica del hecho? La teoría del caso debe integrar, de modo coherente, tres hipótesis:

- acceso, que explique cómo el imputado obtuvo control técnico sobre la frase semilla;
- apoderamiento, que detalle la operatoria de sustracción y los mecanismos de ofuscación utilizados;
- destino, que reconstruya cómo los activos sustraídos se integraron al patrimonio del imputado o de terceros.

El fallo aborda parcialmente estos ejes, pero no los articula en una teoría del caso económico integral que permita

interpretar cada indicio dentro de una secuencia delictiva continua. En esta clase de investigaciones la herramienta más eficaz es la matriz de consistencia patrimonial, que evalúa simultáneamente:

- la capacidad económica previa del imputado;
- el historial legítimo de sus operaciones;
- los flujos relevantes al momento del hecho; y
- las anomalías que surgen del contraste temporal.

Aplicada al caso, la matriz debería haber incluido:

- Reconstrucción del perfil económico anterior al período investigado:
    - Actividad económica declarada.
    - Historial bancario previo.
    - Patrimonio inicial.
    - Capacidad de ahorro razonable.

Esta línea de base permitiría responder la pregunta central: "¿Qué volúmenes de operación eran compatibles con la historia económica del imputado?"

La actividad previa de Lazarte en exchanges, volúmenes habituales de trading, egresos e ingresos del wallet y su comportamiento económico anterior a agosto de 2022.

Ese contraste permite evaluar la razonabilidad de eventos atípicos, como un ingreso súbito de varios cientos de miles de dólares o la recepción de fondos provenientes de un mixer en una cuenta verificada a su nombre. Este tipo de análisis cuantitativo aumenta la capacidad explicativa del razonamiento penal.

Cabe advertir que en casos donde el imputado invoca operaciones de trading, inversión o especulación como fuente lícita, el análisis debió incluir:

- Antigüedad real de la actividad.
- Regularidad o intermitencia.
- Volúmenes promedio operados.
- Relación entre capital inicial y ganancias alegadas.
- Instrumentos utilizados (cripto, acciones, derivados, etc.).

Pues, un trader genuino presenta curvas de actividad consistentes, no picos aislados. El crecimiento abrupto sin fase de acumulación previa es indicio de origen exógeno del capital.

Las series temporales de flujos, a diferencia del análisis de puntuales, permiten construir:

- Series mensuales o trimestrales de ingresos y egresos.
- Evolución del capital operativo.
- Relación entre entradas y salidas.
- Persistencia del flujo.

Lo cual en definitiva posibilita la identificación de rupturas estructurales, inyecciones extraordinarias, y fases de acumulación y dispersión.

La comparación cuantitativa de los volúmenes habituales vs. volúmenes investigados arroja desproporciones no explicadas que hacen perder consistencia a los argumentos defensivos. Con los datos del caso elaboramos el cuadro siguiente:

Cuadro: Serie temporal de flujos

VARIABLE	HISTORIAL PREVIO	PERIODO INVESTIGADO
Volumen promedio operado	Bajo o inexistente	Elevado
Frecuencia de las operaciones	Esporádicas	Intensivas
Capital	Limitado	Elevado
Riesgo asumido	Bajo	Alto

Fuente: Elaboración propia en base al caso

La blockchain ofrece, además, niveles crecientes de trazabilidad: desde la simple identificación de direcciones (nivel 1) y las heurísticas de co-gasto (nivel 2), hasta la inferencia probabilística basada en patrones temporales (nivel 3) y el análisis de clústeres (nivel 4), que permite identificar direcciones satélites, nodos de dispersión y estructuras de control comunes. El fallo se apoya fundamentalmente en los dos primeros niveles, pero prescinde de los restantes, que son los que permiten reconstruir movimientos complejos como los generados por CoinJoin. Un grafo transaccional completo, con pesos y centralidades, habría permitido evaluar si las direcciones asociadas al imputado actuaban como nodos dentro del circuito de dispersión.

Otro elemento esencial es el análisis temporal fino: correlacionar los movimientos del wallet de la víctima, las operaciones del

mixer, los ingresos en las direcciones del imputado y los envíos a terceros. Si estas operaciones se concentran en la misma ventana temporal, la probabilidad de coincidencia accidental disminuye drásticamente.

Finalmente, un análisis económico-forense completo exige considerar hipótesis alternativas. El fallo descarta implícitamente que un tercero haya accedido a la frase semilla, pero lo hace sin una evaluación explícita. Tampoco explora si un mixer pudiera generar coincidencias fortuitas entre fondos ilícitos y direcciones del imputado. Explorar estos contrafácticos muestra que la hipótesis acusatoria es la única capaz de explicar el conjunto de datos sin recurrir a supuestos improbables o inconsistentes.

10. El concepto de "señales patrimoniales sospechosas"

La literatura contemporánea en delitos económicos subraya la utilidad de identificar señales patrimoniales sospechosas, entendidas como patrones atípicos de comportamiento económico que, evaluados en conjunto, permiten inferir la existencia de una operatoria ilícita aun cuando la evidencia directa sea limitada. En casos basados en criptoactivos, estas señales adquieren especial relevancia por la estructura técnica de las transacciones y por la frecuente utilización de mecanismos de ofuscación.

En Lazarte Di Lieto, las señales relevantes incluyen:

- ingreso abrupto de fondos de alto valor;
- proximidad temporal con la sustracción;
- actividad previa mínima o inexistente;
- uso inmediato de mixers;
- derivación de fondos hacia wallets de terceros vinculados;
- coincidencia cuantitativa casi perfecta entre lo sustraído y lo recibido.

En conjunto, este patrón es altamente sugestivo de apropiación ilegítima. El fallo identifica varias de estas señales, pero no las conceptualiza como un marco analítico integrado, lo que reduce la claridad metodológica del razonamiento.

La implementación de servicios de ofuscación impone una necesaria reevaluación del criterio de aplicabilidad del estándar probatorio. En entornos donde la tecnología fragmenta deliberadamente

los flujos, la trazabilidad lineal deja de ser un parámetro viable de acreditación. El análisis económico-forense propone, en su lugar, un criterio de aplicación del estándar basado en:

- coherencia sistémica (la hipótesis debe explicar todos los indicios);
- parsimonia (la explicación más simple y consistente es preferible); y
- poder predictivo (la hipótesis debe anticipar correctamente los comportamientos observados).

Desde esta perspectiva, la investigación de criptodelitos requiere ciertas prácticas metodológicas mínimas: análisis de clústeres, recuperación de logs, reconstrucción patrimonial histórica, identificación de wallets vinculadas, elaboración de líneas de tiempo, exploración de hipótesis alternativas y diseño temprano de una teoría del caso económico que integre los indicios técnicos con los patrimoniales. El aporte central del análisis económico-forense es transformar un conjunto disperso de transacciones en una secuencia económica coherente.

El análisis patrimonial histórico permite evaluar:

- Si los flujos siguen una lógica económica reconocible;
- Si existe una progresión compatible con aprendizaje o crecimiento; y
- Si, por el contrario, los fondos aparecen ya "optimizados", fragmentados o listos para circular.

Este último supuesto es típico de capitales de origen externo; esquemas de interposición; y maniobras de lavado en fase de integración.

El análisis patrimonial histórico no compite, sino que se potencia con el análisis estructural[9], pues: a) El historial económico define qué volumen sería razonable; b) El grafo muestra cómo se movió efectivamente el dinero; y c) La divergencia entre ambos aporta inferencias sólidas sobre el origen y el control.

La falta o déficit de este tipo de análisis podría implicar:

- Subvaloración de indicios económicos.
- Aceptación acrítica de explicaciones defensivas genéricas ("era trading").
- Pérdida de oportunidad para demostrar capacidad económica irreal.

9- Por ejemplo, en el análisis de un imputado sin historial relevante, surgen operaciones en volúmenes similares a los de operadores profesionales, pero los grafos muestran que esos fondos ingresan desde clústeres externos, determinando indicios fuertes de no-autonomía económica.

Por el contrario, su incorporación refuerza la motivación de la decisión, mejora la razonabilidad probatoria, y alinea la investigación con estándares actuales de criminalidad económica.

11. Conclusiones

El caso Lazarte Di Lieto revela el desafío central que enfrentan los sistemas de justicia ante la criminalidad económica digital: traducir categorías clásicas del derecho penal patrimonial a un entorno dominado por criptoactivos, mecanismos de ofuscación y trazabilidad probabilística. El fallo acierta al reconocer a las criptomonedas como bienes inmateriales con valor económico y, por lo tanto, susceptibles de apropiación ilegítima. Ese reconocimiento despeja obstáculos formales y consolida la aptitud del criptoactivo como objeto de tutela penal.

Hemos afirmado que el eje no se encuentra únicamente en el perjuicio individual sufrido por la víctima, sino en el aprovechamiento de una posición funcional de confianza, sustentada en una asimetría informativa y técnica, que habilita una apropiación difícilmente detectable por los mecanismos ordinarios de control. Pues, en el plano probatorio, la Cámara adopta un enfoque razonable para una etapa de procesamiento en un contexto de opacidad técnica. Así, asume que no es exigible una trazabilidad lineal absoluta y se apoya en un conjunto de indicios convergentes —coincidencia cuantitativa, proximidad temporal, uso de mixers, actividad previa casi nula— interpretados como señales patrimoniales consistentes con una maniobra de apoderamiento. Esta aproximación es coherente con la jurisprudencia contemporánea en delitos tecnológicos complejos.

Sin embargo, la ausencia de una teoría del caso económico explícita, la escasa explotación del análisis patrimonial del imputado, la falta de un examen profundo sobre direcciones satélite y clústeres transaccionales, y la débil consideración de hipótesis alternativas reducen la fuerza inferencial de la decisión. Estos déficits no invalidan la conclusión adoptada en esta fase, pero muestran la necesidad de incorporar herramientas más completas de análisis económico-forense.

En suma, Lazarte Di Lieto es un fallo relevante porque reconoce la naturaleza patrimonial de los criptoactivos y legitima el uso de razonamientos indiciarios complejos en escenarios de ofuscación.

Pero también evidencia el camino aún pendiente hacia investigaciones mejor estructuradas: mapas patrimoniales integrales, análisis de patrones, reconstrucciones transaccionales avanzadas y evaluación explícita de alternativas.

La consolidación de estos estándares permitirá que la respuesta penal frente a criptodelitos se apoye en metodologías replicables y conceptualmente sólidas, más que en intuiciones fragmentarias ante fenómenos tecnológicos en rápida evolución.

Desde otra frontera, el caso ofrece un terreno fértil para profundizar en lo relativo a la interacción entre delitos precedentes y conductas compatibles con el lavado de activos en entornos digitales. Si bien el proceso no gira formalmente en torno a una imputación por lavado, la operatoria analizada presenta rasgos típicos de las fases de ocultamiento y dispersión. La utilización de mixers y técnicas CoinJoin, la fragmentación de fondos y su posterior reingreso a wallets asociadas directa o indirectamente al imputado reproducen patrones ampliamente documentados en la literatura especializada sobre lavado de activos con criptoactivos. Esto permite comprender que no toda maniobra compatible con lavado será jurídicamente imputada como tal, pero su identificación resulta clave para comprender la racionalidad económica del delito.

El caso permite consolidar y reforzar la idea de que la investigación penal en criminalidad económica debe ser concebida como un proceso planificado, guiado por una teoría del caso explícita y sostenida en el manejo intensivo de datos. Si bien hemos señalado múltiples herramientas propias del análisis económico-forense —matrices de consistencia patrimonial, análisis de clústeres, correlaciones temporales y evaluación de hipótesis alternativas—, resulta pertinente integrarlas en la práctica de manera más explícita en una estructura de planificación de investigación preliminar. Todo lo cual lleva a ordenar los indicios no sólo como elementos probatorios aislados, sino como partes de una secuencia lógica orientada a la verificación o refutación de hipótesis.

Desde esta perspectiva, el caso evidencia la necesidad de integrar pericia informática, análisis de datos y razonamiento económico en un único dispositivo analítico, capaz de traducir grandes volúmenes de información técnica en inferencias jurídicas racionales y controlables.

Finalmente, en investigaciones de esta naturaleza, la planificación debería contemplar el pasaje desde niveles básicos de trazabilidad (direcciones individuales y coincidencias cuantitativas) hacia análisis de clústeres y grafos transaccionales, que permiten reconstruir estructuras de control, nodos de dispersión y potenciales beneficiarios finales entre cientos de direcciones involucradas. Esto hubiera requerido incorporar un análisis patrimonial histórico del imputado, incluyendo volúmenes habituales de trading, frecuencia operativa, flujos previos, capacidad económica declarada y consistencia entre ingresos históricos y los montos involucrados en la maniobra.

Bibliografía

Corti, A. H. M. (s.f.). *Algunas reflexiones sobre los mecanismos de exacción de la renta impositiva nacional. A propósito de las ficciones de contratos al interior de los conjuntos económicos*. Doctrina.

Gils Carbó, A. M., & Vásquez, M. G. (2007). Evasión fiscal a través de la utilización fraudulenta de sociedades extranjeras. *Revista del Instituto*, AFIP, 100-109.

González Busquin, F. R. (mayo de 2023). Criptoactivos, depósitos bancarios y el hurto informático. *Revista Pensamiento Penal*, (468). https://www.pensamientopenal.com.ar/

Ministerio Público Fiscal de la Nación. (2023). *Guía práctica para la identificación, trazabilidad e incautación de criptoactivos: Consideraciones teórico-prácticas sobre activos virtuales basados en la tecnología de cadena de bloques y su investigación penal*. MPF. Dirección de Comunicación Institucional.

König, C., Marsili, M., & Carrara, F. (s.f.). ¿Cómo organizar la investigación del aspecto económico del delito? En *Delitos económicos. Caja de herramientas para quienes investigan, litigan y juzgan*. PROCELAC / INECIP.

Marsili, M. (2023). *Crimen, complejidad y economía*. Ediciones Didot.

Marsili, M., & Radyna, C. (s.f.). Alertas sospechosas y análisis económico del delito. En M. Marsili, *Crimen, complejidad y economía*. Ediciones Didot.

Morcillo, N. (10 de marzo de 2025). *La 'macroestafa' piramidal de Arbistar, a juicio: la Audiencia Nacional celebra la primera vista*

sobre criptomonedas. Cinco días. https://cincodias.elpais.com/mercados-financieros/2025-03-10/la-macroestafa-piramidal-de-arbistar-a-juicio-la-audiencia-nacional-celebra-la-primera-vista-sobre-criptomonedas.html

Naucke, W.-R. (2015). *El concepto de delito económico-político: Una aproximación* (E. Sarrabayrouse, Trad.). Marcial Pons.

Unidad de Información Financiera. (2014). *Resolución 300/2014. Prevención del Lavado de Activos y de la Financiación del Terrorismo*. https://servicios.infoleg.gob.ar/infolegInternet/anexos/230000-234999/231930/norma.htm

Ministerio Público Fiscal. (12 de mayo de 2023). *Resolución PGN N.º 33/23*.

Silva, G., & Marsili, M. (s.f.). ¿Cómo desarrollar una investigación en criminalidad económica a partir de metodologías de las ciencias sociales? En *Delitos económicos. Caja de herramientas para quienes investigan, litigan y juzgan*. PROCELAC / INECIP.

Sutherland, E. H. (s.f.). *El delito de cuello blanco*. BdeF.

Tiedemann, K. (1983). El concepto de derecho económico, de derecho penal económico y de delito económico. *Revista Chilena de Derecho*, 10(1), 59–82.

La Criminalidad Económica de Edgar A. Bacchiani y Adhemar Capital SRL

Maximiliano Fernández[1] y Lorena Beatriz Varas[2]

Resumen

El presente trabajo expondrá los hechos, evidencias y derecho sobre las acciones desplegadas por Edgar Adhemar Bacchiani, el influencer que se hacía llamar "Trader God", quien junto a otros "colaboradores" y detrás de Adhemar Capital SRL estafaron a cientos de personas de distintas localidades del país.

Esta investigación gira en torno al fallo de autos caratulado "Bacchiani, Edgar Adhemar p.s.a. Estafa Reiterada", dictado por la Cámara en lo Criminal y Correccional de la 10° Nominación, tribunal integrado por los Dres. Carlos Palacio Laje, Mario Walter Centeno y Juan José Rojas Moresi, de la Provincia de Córdoba, en fecha 03 de abril de 2025.

1- Abogado por la Universidad de Belgrano. Auxiliar administrativo en MPF de la Nación. Ex Gerente Operativo de Administración y Control de Gestión de Obras y Servicios en Ministerio de Salud GCABA (2021-2024) y Ex Gerente Operativo de Programas Especiales en Ministerio de Hábitat y Desarrollo Humano GCABA (2016-2020). Correo: maximilianoferz@gmail.com.
2- Bachiller Universitario en Ciencias económicas de la facultad de ciencias económicas de la UNL. Estudiante avanzada de la carrera de Contador Público de la facultad de ciencias económicas de la UNL. Técnica Universitaria en Administración y Gestión Tributaria de la facultad de ciencias económicas de la UNL. Diplomatura superior en tributos de la Provincia de Santa Fe y Convenio Multilateral de la facultad de ciencias económicas de la UNL. Diplomatura en análisis económico forense del programa de estudios interdisciplinarios sobre prevención y persecución de la criminalidad económica de la UNR. Desempeño laboral en la Administración Provincial de Impuestos de la Provincia de Santa Fe en la Delegación Esperanza. Correo: lore_vara@hotmail.com

1. El caso

Se trató de una estafa piramidal donde Edgar Adhemar Bacchiani —valiéndose de la inexperiencia de sus víctimas— cometió actos que atentaron contra el patrimonio individual, como así también con el orden económico y financiero nacional, a través de operaciones que entendía como lícitas cuando en realidad no lo eran. Amparándose en una estructura que supo formar y mantener por al menos dos años (03-2020 al 03-2022), captaba ahorristas que le daban grandes sumas de dinero con la promesa de obtener retornos extraordinarios simulando su inversión en el mercado de criptomonedas.

El caso contempla sólo cincuenta (50) hechos probados, por un valor estimado en dólares un millón (USD 1.000.000) y con damnificados en las provincias de Buenos Aires, Catamarca, Córdoba, La Rioja y Tucumán.

El caso de Bacchiani fue caratulado y resuelto como delito de estafa, aunque analizando el modus operandi posiblemente se trate de una estafa piramidal o bien un esquema Ponzi, que por la declaración de los damnificados se asemeja a este último tipo.

En el esquema clásico de "pirámide", los participantes intentan ganar dinero únicamente reclutando nuevos participantes, generalmente cuando:

- el promotor promete una alta rentabilidad en un corto período de tiempo;
- no se vende realmente ningún producto o servicio genuino; y
- el énfasis principal está en reclutar nuevos participantes.

Todos los esquemas piramidales eventualmente colapsan y la mayoría de los inversores pierden su dinero.

Los estafadores suelen promover esquemas piramidales a través de redes sociales, publicidad en internet, sitios web de empresas, presentaciones grupales, conferencias telefónicas, videos de YouTube y otros medios. Los promotores del esquema hacen todo lo posible para que el programa parezca un negocio legítimo. Sin embargo, los estafadores utilizan el dinero pagado por los nuevos reclutas para pagar a los inversores iniciales. En algún momento, los esquemas se vuelven demasiado grandes, el promotor no puede recaudar suficiente dinero de los nuevos inversores para pagar a los primeros, y los inversores pierden su dinero.

Un esquema Ponzi es un fraude de inversión que paga a los inversores existentes con fondos recaudados de nuevos inversores. Los organizadores suelen prometer invertir su dinero y generar altos rendimientos con poco o ningún riesgo. Pero en muchos esquemas Ponzi, los estafadores no invierten el dinero; en cambio, lo utilizan para pagar a quienes invirtieron anteriormente y pueden quedarse con una parte. Con escasas o nulas ganancias legítimas, los esquemas Ponzi requieren un flujo constante de dinero nuevo para sobrevivir.

2. El fallo

Al tratarse de hechos idénticos pero independientes, el fallo hace referencia a que debiera aplicarse el concurso real de delitos donde la pena máxima podría ser la derivada de la suma aritmética de las penas máximas correspondientes a los diversos hechos de estafa.

En oportunidad de los alegatos y últimas palabras, el fiscal de cámara hizo expresa mención de que se ha convenido a una pena de tan sólo diez años de prisión, por 50 hechos de estafa en concurso real, expresando que la escala penal tiene un mínimo de un mes y un máximo de 300 años, aunque la ley establece un límite de 50 años. Sin embargo, según el art. 55 in fine CP: "esta suma no podrá exceder de (50) cincuenta años de reclusión o prisión".

Así las cosas y considerando los atenuantes evaluados por los magistrados, el tribunal resolvió:

> "Declarar por unanimidad a Edgar Adhemar Bacchiani, ya filiado, autor penalmente responsable del delito de estafa reiterada —50 hechos— en concurso real (arts. 45, 172 y 55 CP) e imponer por unanimidad, para su tratamiento penitenciario, la pena de nueve (9) años de prisión de cumplimiento efectivo, con más las accesorias de ley y costas, (arts. 5, 9, 12, 29 inc. 3, 40 y 41 del CP; arts. 412, 415, 550 y 551 del CPP; art. 1 Ley Nac. 24.660 y art. 1 Ley Prov. 8.878)."

3. Perspectiva federal

Con una mirada reduccionista del conflicto social, el caso en el fuero provincial ha comenzado y finalizado con el delito de estafa. Sin embargo, de acuerdo a la figura penal señalada cabe destacar que se han cumplido todos los recaudos para arribar a la sentencia. Se destaca que ante la cantidad de hechos, similares todos, se observa una descripción clara de los mismos, una cronología correcta y un abordaje prolijo al respecto. Las víctimas han confiado su patrimonio y en reiteradas ocasiones han vuelto a confiar en quien les hacía creer que gestionaba sus inversiones con diligencia.

La teoría general del derecho nos enseña una clasificación de delitos donde el bien jurídico protegido resulta ser la vida y la integridad física de las personas, diferenciándose de aquellos delitos de contenido estrictamente patrimonial, ya sea en perjuicio de particulares o del Estado. Dentro de esta segunda especie encontramos los siguientes delitos:

3.1. Delitos contra el patrimonio de particulares

El caso en estudio se centró en el delito de estafa, figura penal por excelencia junto al delito de daños, que protegen el patrimonio de los particulares. Sin embargo, resultan figuras de ánimo punitivista, cuando a raíz de una visión moderna del derecho, debemos procurar el resarcimiento del daño, el recupero de activos y velar por la resolución del conflicto.

3.2. Delitos contra la hacienda pública y la seguridad social

Para la protección de ese bien jurídico, se encuentra vigente el Régimen Penal Tributario, cuya Ley 27.430 ha sido recientemente modificada mediante Ley 27.799. Este ordenamiento contiene la evasión fiscal y de los recursos de la seguridad social. Una nota distintiva es que la infracción a este régimen no admite la aplicación del instituto de la suspensión del juicio a prueba (probation) ya que así lo establece el art. 76 bis del Código Penal. Ahora bien, desde el punto de vista procesal, en estos casos suelen suspenderse la acción penal puesto que el contribuyente evasor se adhiere a un plan de pagos en razón de una ley de blanqueo fiscal —moratoria— cuya excepción se ha vuelto la regla en nuestro sistema tributario.

En el caso en cuestión, la financiera al no contar con la debida autorización para llevar a cabo su actividad comercial no emitía comprobantes fiscales por su labor de asesoramiento, gestoría y afines a favor de sus clientes.

3.3. Delitos cambiarios

Este delito es llevado a cabo por quienes operan con moneda extranjera en forma ilegal en una "cueva financiera", "arbolito", "casa de cambios" o "mercado negro de divisas". Consiste en no contar con la debida autorización de la autoridad competente: el Banco Central de la República Argentina. El bien jurídico protegido es el orden económico financiero del Estado y la política monetaria de la Nación.

Este régimen tiene por objeto promover la liquidez, el buen funcionamiento del crédito y la conservación del valor de la moneda, por tal motivo sanciona a quienes infrinjan la regulación del mercado de cambios.

La normativa sanciona: toda negociación de cambio que se realice sin intervención de institución autorizada; operar en cambios sin estar autorizado; toda falsa declaración relacionada con las operaciones de cambio; la omisión de rectificar las declaraciones producidas; toda operación de cambio que no se realice por la cantidad, moneda o al tipo de cotización, en los plazos y demás condiciones establecidos por las normas en vigor; y todo acto u omisión que infrinja las normas sobre el régimen de cambios.

Al presente —enero de 2026—, esta materia se encuentra regulada en la Ley N.º 19.359 y sus modificatorias ("Ley de Régimen Penal Cambiario, texto ordenado 1995"). El Anteproyecto de Código Penal (CIPCE 2019) incorpora este delito bajo el Título XVIII Delitos Cambiarios en los arts. 379 a 391 CP, derogándose la Ley 19.359. La principal modificación consiste en la exigencia de los elementos subjetivos "a sabiendas" o "pudiendo causar perjuicio", lo que a nuestro entender dificulta la tesis probatoria y podría dar lugar a un error de prohibición o un caso atípico.

Bacchiani realizaba sus actividades en pesos y en dólares, y al no contar con la autorización por parte del Banco Central de la República Argentina para ello, infringía el Régimen Penal Cambiario establecido en la Ley 19.359.

3.4. Delitos contra el orden económico y financiero

Actualmente regulados en el Título XIII del CP en los arts. 303 a 313, fueron completados por la Ley 26.733 que, de acuerdo a la opinión de Raúl R. Saccani, tuvo como finalidad satisfacer las demandas del GAFI[3] a la Argentina en el marco de las 40 Recomendaciones para combatir el lavado de activos, la financiación del terrorismo y su proliferación, y asegurar la transparencia y la cooperación internacional, protegiendo así la integridad del sistema financiero.

- Las figuras que comprende dicho Título son:
- Lavado de activos
- Abuso de información privilegiada o insider trading
- Manipulación de valores negociables
- Intermediación financiera y captación de ahorros públicos no autorizados
- Contabilidad falsa
- Cohecho financiero
- Responsabilidad penal de las personas jurídicas

1. Lavado de activos

En primer lugar, el lavado consistirá en todas aquellas operaciones realizadas para que los bienes de origen ilícito se inserten en la economía legal y formal, aparentando un origen lícito (Carrara, 2017). De acuerdo a una concepción clásica, el lavado presenta tres etapas: a) colocación, b) estratificación y c) integración.

En la colocación, el dinero de un ilícito ingresa al sistema formal bancario o financiero. Esas sumas son depositadas a nombre de tal o cual persona física o jurídica, y su fuente aparente legal sería una donación, un préstamo o un premio obtenido.

En la estratificación, se busca distanciar a los bienes de su origen ilícito. Si el dinero proviene del juego clandestino, se realizarán operaciones que nada tienen que ver con ese rubro, por ejemplo una inversión inmobiliaria. Con avanzado asesoramiento legal y contable se suelen constituir sociedades en el extranjero, especialmente en paraísos fiscales donde el secretismo es una regla en beneficio de los inversores que lavan activos.

3- Grupo de Acción Financiera Internacional.

En la integración ya no quedan rastros que vinculen a los bienes espurios de las operaciones posteriores. Se habrán adquirido bienes muebles, inmuebles, derechos y otras acreencias, inclusive a través de sociedades o interpósitas personas, desvirtuando toda posibilidad de trazabilidad.

Sebastián R. Narvaja propone un modelo de análisis distinto al convencional. Este autor prefiere el modelo dado por el investigador británico Stephen Platt en la obra *Criminal Capital* ya que entiende que el modelo anterior contiene etapas donde no necesariamente todas ellas se verifican en un caso.

En segundo lugar, el delito de lavado de bienes mutó a lavado de activos, incluyendo así un concepto más abarcativo como objeto del delito. Inicialmente su tipificación estaba vinculada al delito de narcotráfico con alusión al bien jurídico protegido salud pública (Ley 23.737/1989). Seguidamente, este delito se vinculó al encubrimiento de un ilícito cometido por otro y con miras en la protección del bien jurídico administración pública (Ley 25.246/2000). Finalmente, el delito de lavado de activos adquiere plena autonomía con la incorporación al Código Penal del artículo 303 protegiendo jurídicamente al orden económico y financiero (Ley 26.683/2011).

Notas distintivas del delito:

- Las acciones típicas son muy diversas y cerradas (Argibay Molina, 2021), aunque con la mención a o de cualquier otro modo, es una figura que desde antaño es atacada de inconstitucional atento a transgredir el principio de legalidad penal (art. 18 CN).
- Su tipo básico se encuentra en el inc. 4.º del art. 303 sancionado con pena de multa.
- Si bien se valora una sentencia condenatoria previa con relación al delito precedente, sólo se requerirá que el hecho previo sea típico y antijurídico, no así declarado culpable y punible.

En nuestro caso de estudio se visualiza la configuración del autolavado[4], es decir, el delito precedente fue cometido por el mismo autor de quien lava sus bienes. Esto en concordancia con el precedente "Córdoba, Segundo Pantaleón s/inf. art. 303 inc. 3 del CP", donde se ha establecido que de acuerdo a la sana crítica racional del juez al valorar la prueba y al ver que el imputado no podría justificar el

4- Ares. Autolavado de activos en el Código Penal Argentino.

dinero, se configura que son provenientes de varias infracciones de naturaleza penal cometidas en el pasado.

2. Intermediación financiera y captación de ahorros públicos no autorizados

Podría decirse que este tipo penal es el de los más controvertidos del orden económico y financiero. Gustavo Aboso y Raúl R. Saccani coinciden en que resulta una figura excesivamente difusa, abierta, confusa y amplia, que transgrede el principio de máxima taxatividad de la ley penal y por ende el principio de legalidad (art. 18 CN). Sin embargo, Fontán Balestra no comparte dicha opinión, ya que entiende que el concepto de intermediador financiero es un elemento normativo del tipo que está bien delineado (Spessot).

El Código Penal actual versa: "En igual pena incurrirá quien captare ahorros del público en el mercado de valores o prestare servicios de intermediación para la adquisición de valores negociables, cuando no contare con la correspondiente autorización emitida por la autoridad competente."

Al respecto, el Proyecto de Código Penal 2025 versa: "Al que captare ahorros del público para la adquisición de valores negociables o prestare servicios de intermediación para la adquisición de valores negociables, si no contare con la correspondiente autorización emitida por la autoridad competente."

El Anteproyecto de Código Penal (2019) analiza este cambio y concluye en que su modificación resulta negativa, ya que deja afuera la penalización de captación de ahorros para la adquisición de valores que no sean negociables y además puede que los valores sean negociables pero que en los instrumentos se incluyan cláusulas que lo vuelven innegociables.

Siguiendo una concepción amplia de intermediación financiera, alcanzaría a toda persona que actúe como banco sin contar con la autorización por parte del Banco Central de la República Argentina, realizando entre otras actividades: otorgar préstamos o recibir depósitos.

En nuestro fallo, según declaraciones de víctimas, éstas realizaban depósitos a favor de Adhemar Capital SRL y/o Edgar Adhemar Bacchiani, mediante contrato de mutuo contra pagarés. El fallo comenta que el Fiscal de Cámara en su alegato de clausura destacó el informe de la Comisión Nacional de Valores del cual surgió que ni Adhemar Capital SRL ni Edgar Adhemar Bacchiani se encontraban inscriptos

en calidad de agentes de la comisión y que se los intimó para que cesaran en su actividad.

> "Aquí quien estaba ofreciendo esta actividad tan rentable era alguien que no tenía ningún tipo de autorización para hacerlo y había sido intimado para que cesara en esa actividad".

El agente fiscal agregó que el Banco Central también informó que Adhemar Capital ni tampoco Bacchiani estaban incluidos en la nómina de entidades financieras autorizadas a funcionar.

> "Que la actividad de asesoramiento en materia de mercado de capitales desde el momento en que se hace pública se convierte en un acto de intermediación previsto por nuestra ley y las normas (N.T. 2013 y mod.), que necesariamente debe contar con autorización de la Comisión Nacional de Valores (en adelante 'CNV') y debe reunir la idoneidad exigida por el organismo, exigida a quienes desempeñen las actividades de venta, promoción o prestación de cualquier tipo de asesoramiento al público inversor, para garantizar que cuentan con el nivel de competencia e integridad requerido. Que el derecho del mercado de capitales se inserta dentro de la función tuitiva de los derechos del consumidor financiero (conf. Art. 42 de la Constitución Nacional) toda vez que el bien jurídico tutelado por el Estado —a través de esta CNV— es el ahorro público".

3. Contabilidad falsa

En el hipotético caso de llevar una contabilidad ordenada por parte de Adhemar Capital SRL, se colige que la única forma de asentar sus movimientos contables y a su vez poder hacer frente a los compromisos asumidos sería insertando en sus libros datos falsos, hechos inexistentes, operaciones crediticias activas y pasivas o de valores negociables con la intención de obtener un beneficio o causar un perjuicio para sí o para terceros, en los términos del art. 311 del Código Penal.

La contabilidad en el caso

a) Los registros contables y la insolvencia

Un análisis de los registros contables y en forma resumida de los estados contables podría haber advertido la iliquidez o insolvencia

de la firma Adhemar Capital SRL. Se podía visualizar con un simple cálculo la liquidez mirando los activos corrientes y pasivos corrientes.

También prestando atención a las cuentas del activo que integran el rubro de Caja y Bancos como así también el rubro Inversiones, ya que son los rubros que le darían origen a los fondos que la empresa devolvía como capital o rendimiento de sus aportes.

b) La documentación respaldatoria

Habitualmente la empresa Adhemar Capital SRL entregaba documentos respaldatorios de la operación que realizaba con sus clientes. Firmaba contratos de mandato de inversión donde el cliente autorizaba a la empresa a realizar las inversiones acordadas, firmaba boletos de compraventa cuando recibía inmuebles como forma de pago de las inversiones, firmaba pagarés cuando recibía fondos de sus clientes.

Se tuvo que solicitar a las oficinas de rentas provinciales y municipales para que informen si se ha abonado el Impuesto de Sellos correspondiente a los documentos y/o contratos firmados para darle validez al momento de la concreción de los instrumentos señalados.

4. Responsabilidad penal de las personas jurídicas en el lavado de activos

El art. 313 Código Penal se dirige a penar a las personas jurídicas con remisión al art. 304 Código Penal. Este artículo especifica las sanciones que caben a la persona jurídica que de algún modo participó en el lavado de activos (art. 303 CP). La sanción más gravosa está en el art. 304 inc. 4: Cancelación de la personería cuando hubiese sido creada al solo efecto de la comisión del delito, o esos actos constituyan la principal actividad de la entidad.

Asimismo, debería analizarse la aplicación de la Ley 27.401 de Responsabilidad Penal de las Personas Jurídicas Privadas a la luz del inc. e) Balances e informes falsos agravados, previsto por el artículo 300 bis del Código Penal, previo a verificar si se han configurado los delitos del art. 258 y 258 bis CP, esto es cohecho activo y tráfico de influencias activo o soborno transnacional. A decir del fallo, se descarta esta posibilidad puesto que Bacchiani era reacio a las relaciones con agentes del gobierno.

Por lo expuesto, no cabe dudas de que tanto a Adhemar Capital SRL como a Bacchiani les cabe las figuras penales desarrolladas, en concurso real —y en algunos casos ideal— de delitos.

4. Criptomonedas

Criptomonedas, criptodivisas, criptoactivos: todas estas denominaciones se refieren a un bien intangible y virtual que previo cambio en un mercado especial puede derivar en un billete físico, pero la idea principal radica en un activo virtual, diferenciado de las monedas tradicionales de la humanidad y de la forma en que concebimos al dinero y su valor.

Desde su presentación en sociedad en el año 2008, el Bitcoin se constituyó como dinero virtual evitando su paso por las instituciones financieras de los Estados. Como toda moneda tiene dos caras: una buena que obedece a la evolución de la humanidad en materia tecnológica y otra mala ligada a la desnaturalización de su finalidad o canalización de fondos provenientes de actividades ilícitas.

Hay criptos que poseen valores nominativos propios, fluctuante internamente de acuerdo a su oferta y demanda, mientras que otros tienen un valor atado a la cotización del dólar u otras monedas gubernamentales, compartiendo ambas clases ciertos grados de volatilidad. La temática resulta sumamente desafiante ante una administración pública y de justicia con escasos conocimientos en la blockchain o cadena de bloques.

A continuación se brindan las definiciones empleadas en la Guía Práctica para la identificación, trazabilidad e incautación de criptoactivos del Ministerio Público Fiscal de la Nación:

El Grupo de Acción Financiera Internacional (GAFI) define a los activos virtuales como “una representación digital de valor que se puede comercializar o transferir digitalmente y se puede utilizar con fines de pago o inversión. Los activos virtuales no incluyen representaciones digitales de monedas fiduciarias, valores y otros activos financieros que ya están cubiertos en otras partes de las Recomendaciones del organismo”.

La UIF, en línea con el GAFI, define a las “monedas virtuales” como la representación digital de valor que puede ser objeto de comercio

digital y cuyas funciones son la de constituir un medio de intercambio, y/o una unidad de cuenta, y/o una reserva de valor, pero que no tienen curso legal, ni se emiten, ni se encuentran garantizadas por ningún país o jurisdicción.

Por su parte, el "criptoactivo" es la denominación que recibe cierto tipo de activos virtuales que se diferencian de los demás por cómo son implementados, es decir, por funcionar sobre una plataforma que se vale del uso de técnicas criptográficas y de una base de datos constituida sobre un sistema de cadena de bloques.

El término "criptomoneda" se refiere a los activos nativos de plataformas basadas en técnicas criptográficas y que se valen de una base de datos constituida bajo el sistema de cadena de bloques.

Los "tokens" son activos no nativos que funcionan sobre plataformas como las descriptas, desplegados e implementados por medio de programas informáticos conocidos como "contratos inteligentes". Son susceptibles de presentar funcionalidades similares a las de las criptomonedas, aunque su creación enfrenta menos obstáculos.

Los Altcoins refieren a cualquier criptoactivo basado en la tecnología "blockchain" que no sea Bitcoin, término que surge de la abreviatura de "alternativa a Bitcoin". Ejemplo: Ether, la criptomoneda nativa del sistema denominado Ethereum. Otras altcoins: DAI, Tether, Num ARS, USD Coin, Fartcoin, Hyperliquid, BitPRO, Binance Coin, Solana, etc.

Finalmente, las Exchanges son plataformas privadas que proveen servicios de arbitraje y/o compraventa de criptoactivos. Se encargan de administrar los activos y registran en sus bases de datos los movimientos de las cuentas de sus usuarios.

Resumiendo, es un universo complejo caracterizado por su constante expansión, volatilidad, anonimato, huidizo de las investigaciones estatales, carentes de atención personalizada por parte de las plataformas, carentes de oficinas comerciales físicas e inclusive virtuales, entre otras características ligadas a la tecnología.

4.1. Breve reseña normativa

Ley N.º 25.246/2000. Encubrimiento y Lavado de Activos de origen delictivo. Unidad de Información Financiera (creación, organización, competencia, facultades). Deber de informar. Sujetos obligados. Régimen Penal Administrativo. Ministerio Público Fiscal.

Art. 4 bis (Ley 27.739, marzo-2024). Activos virtuales: representación digital de valor que se puede comercializar y/o transferir digitalmente y utilizar para pagos o inversiones. En ningún caso se entenderá como activo virtual la moneda de curso legal en territorio nacional y las monedas emitidas por otros países o jurisdicciones (moneda fiduciaria).

Art. 20 (Ley 27.739, marzo-2024). Están obligados a informar a la Unidad de Información Financiera (UIF), entre otros, los siguientes sujetos: 13. Los proveedores de servicios de activos virtuales.

Resolución UIF N.º 70/2011. Apruébese el "Sistema de Reporte de Operaciones —Manual del Usuario— III. RSM".

Resolución UIF N.º 300/2014. Los Sujetos Obligados enumerados en el artículo 20 de la Ley N.º 25.246 y sus modificatorias deberán prestar especial atención al riesgo que implican las operaciones efectuadas con monedas virtuales y establecer un seguimiento reforzado respecto de estas operaciones, evaluando que se ajusten al perfil del cliente que las realiza. A los efectos de la presente resolución se entenderá por "Monedas Virtuales" a la representación digital de valor que puede ser objeto de comercio digital y cuyas funciones son la de constituir un medio de intercambio, y/o una unidad de cuenta, y/o una reserva de valor, pero que no tienen curso legal, ni se emiten, ni se encuentran garantizadas por ningún país o jurisdicción.

Asimismo, los sujetos obligados deberán informar, mensualmente, hasta el día quince (15) de cada mes, todas las operaciones efectuadas con monedas virtuales, a partir del mes de septiembre de 2014, conteniendo la información correspondiente a las operaciones realizadas en el mes calendario inmediato anterior.

Como se puede visualizar, la UIF si bien en los años 2011 y 2014 intentó incluir a los exchanges como sujetos obligados a reportar operaciones sospechosas, recién en 2024 con la sanción de la Ley 27.739, los proveedores de servicios de activos virtuales (PSAV) comenzaron a estar alcanzados por la normativa de reporte de operaciones.

Un punto no menor radica en que esos proveedores deben informar todas las operaciones efectuadas con monedas virtuales. Entendemos que tuvo que establecerse un mínimo de umbral, ya que sin él el sistema se vuelve burocrático. Un mínimo de umbral utilizado con frecuencia es el índice SMVM (salarios mínimos, vitales y móviles).

En cuanto a la Comisión Nacional de Valores (CNV), este organismo adaptó su normativa mediante la Resolución General CNV N.º 994/2024 (25/03/2024), modificada por Resolución General CNV N.º 1058/2025 (14/03/2025). Así, quedó establecida la obligatoriedad de registro de los PSAV ante dicho organismo, su alcance, el régimen informativo y los requisitos de idoneidad, integridad y solvencia para operar en el mercado de capitales.

Quedan exceptuados de la obligación de inscripción en el Registro los PSAV cuyas actividades u operaciones no superen, de manera agregada, un monto equivalente a UVA 35.000 por mes calendario. Al 31/01/2026 (Valor UVA $1.752,97), esas UVAs equivalen a pesos $61.353.950.

En cuanto a la Agencia de Recaudación y Control Aduanero (ARCA), mediante la Resolución General N.º 4.614 (24/10/2019), modificada por la Resolución General N.º 5.804/2025 (24/12/2025), se fijó un régimen de información. Los sujetos que administran, gestionan, controlan o procesan movimientos de activos a través de plataformas de gestión electrónicas o digitales, por cuenta y orden de personas humanas y jurídicas residentes en el país o en el exterior, incluidos los Proveedores de Servicios de Pago (PSP), deberán cumplir con un régimen de información sobre la nómina de cuentas de clientes y los montos totales de ingresos, egresos y/o saldo final mensual. Dicha información se suministrará respecto de aquellos usuarios cuyos ingresos o egresos totales resulten iguales o superiores a $50.000.000 para personas humanas y $30.000.000 para personas jurídicas.

En definitiva, resulta reciente la obligatoriedad de proporcionar información (nombres, direcciones, teléfonos, e-mails, direcciones de IP) sobre las transacciones de criptoactivos que permitieran avanzar en una investigación criminal.

En estas operaciones reina el pseudoanonimato, con lo cual si bien no es imposible detectar quién está detrás de cada transacción, resulta una tarea ardua y compleja. Incluso ya existen sistemas y plataformas que buscan frustrar la trazabilidad a través de la utilización de un procedimiento llamado coinjoin o servicios denominados mixers o tumblers.

Sin embargo, también existen plataformas que analizan criptoactivos y poseen buscadores que detectan en forma automática a cuál de ellas podría pertenecer una dirección determinada; estos sitios son: Blockchair, Blockcypher, Blockchain.com, BTC.com.

Volviendo al fallo, se puede leer que "criptomoneda equivalentes a aproximadamente 2,5 Bitcoins a un nuevo contrato de inversión mediante el cual Bacchiani se comprometía a abonar en concepto de rentabilidad mensual un porcentaje del capital de entre el 7% y 22% cada una…", que "Bacchiani y/o Adhemar Capital SRL, a través de su apoderado García Alaimo, se comprometía falsamente a operar en el mercado de criptomonedas con los fondos de la mandante", y que "en el mes de enero del 2022 hubo información del dueño de que tenían que bajar de golpe las tasas porque el mercado de cryptomonedas 'se estaba amesetando'".

Lo expuesto deja entrever que Bacchiani aprendió conceptos propios del mundo cripto. Se fondeaba con los capitales aportados y distribuía los intereses. El capital se iba consumiendo porque tales ganancias extraordinarias no las obtenía, entonces llegaba el momento de defaultear su deuda, reestructurando contratos, aplicando quitas, disminuyendo las tasas y en definitiva no pagar lo que se había comprometido a pagar.

Se verificó una estafa solapada en inversiones de criptoactivos. Así lo manifiesta el fallo: Bacchiani habría diseñado una maniobra consistente en captar fondos de particulares y, bajo la promesa de invertir dichas colocaciones en criptomonedas y fondos de inversión, ofrecía retornos con rentabilidad extraordinaria, a sabiendas que en función de la naturaleza y la volatilidad de dichas operaciones no podría satisfacer los compromisos pactados tanto con relación a la restitución del capital como al pago de sus respectivos intereses.

5. Investigación del aspecto económico del delito

5.1. La investigación del aspecto económico del delito (IAED)

En cuanto a finalidad del proceso, en nuestro caso observamos que se ha perseguido una condena por el delito de estafa. El bien jurídico protegido es la propiedad, el patrimonio, y un elemento característico es el canal que usa el autor para cometer el ilícito: el engaño, el ardid, inducir a error a su víctima para que le otorgue bienes de su propiedad.

La teoría del caso se ha centrado en la persona del autor. Sin embargo, desde la redacción original del Código Penal del año 1921,

quedó establecido en el art. 23 que la condena importa la pérdida de los instrumentos del delito, los que, con los efectos provenientes del mismo, serán decomisados.

Posteriormente, con la reforma del CP según la Ley 25.188 del año 1999, el art. 23 establece que en todos los casos en que recayese condena la misma decidirá el decomiso de las cosas que han servido para cometer el hecho y de las cosas o ganancias que son el producto o el provecho del delito, en favor del Estado nacional, de las provincias o de los municipios, salvo los derechos de restitución o indemnización del damnificado y de terceros.

A raíz de ese cambio, se pasó a considerar al decomiso como una herramienta orientada al recupero de activos provenientes del delito que procura impedir que el autor del ilícito penal pueda seguir disfrutando de lo que por él obtuvo.

Cabe mencionar que a partir de la Ley 26.683 del año 2011 se incorporó al Código Penal el decomiso sin condena o "decomiso anticipado", respecto de los delitos contra el orden económico y financiero. Con ello, se consolidó el pasaje de la concepción tradicional de decomiso in personam (sanción dirigida al condenado) hacia un decomiso in rem (atendiendo al origen de los bienes y su producido).

Con relación a la investigación misma, parece ser unidireccional y localizada, es decir, enfocada en demostrar la responsabilidad penal del autor. Notamos ausencia de trabajo interdisciplinario. El siglo pasado estuvo marcado por las garantías hacia el reo —debido proceso, plazo razonable, trato humanitario— mientras que ahora sobresale una protección especial a las víctimas, y el recupero de activos para procurarles una reparación requiere de una buena IAED.

En ese sentido, puede resultar muy útil la conformación de una mesa de trabajo conjunto de distintas jurisdicciones judiciales sobre un caso específico, tal como lo prevé el art. 123 del reciente Código Procesal Penal Federal:

> ARTÍCULO 123.- Investigaciones conjuntas y cooperación de Ministerios Públicos provinciales y de la Ciudad Autónoma de Buenos Aires. Si fuera necesario investigar hechos llevados a cabo en más de una jurisdicción, el representante del Ministerio Público Fiscal podrá coordinar la investigación con las autoridades de otras jurisdicciones. A este efecto podrá formar equipos de investigación.

En sintonía con ello, y si del caso pudiera apreciarse que la organización o el particular tuviese puntos de contacto con el extranjero, puede recurrirse a la conformación de un Equipo Conjunto de Investigación (ECI) impulsado por el Ministerio Público Fiscal de la Nación, que brinda herramientas de cooperación internacional frente a la delincuencia organizada transnacional.

5.2. Investigación en el caso

Para efectivizar las técnicas de investigación forense (Fontán) de las personas en cuestión, será necesaria la búsqueda permanente de información, por lo que se deberá solicitar al juez de garantías que ordene el levantamiento del secreto fiscal (art. 101, 3º párrafo de la Ley 11.683), bancario (art. 39 inc. a de la Ley de Entidades Financieras N.º 21.526), bursátil (art. 25 de la Ley 26.831) y el financiero previsto en el art. 22 de la Ley 25.246 y Ley 27.260.

Posterior a ello, se solicitarán informes para identificar parentescos, bienes —muebles, inmuebles, derechos— propios y de terceros conectados, movimientos bancarios, etc.

En forma concomitante, las técnicas de auditoría forense (Saccani) a aplicar para determinar la real cuantía del fraude podrían ser:

- Técnicas de verificación ocular: observación, comparación y rastreo de bienes patrimoniales tanto del acusado como los que están registrados a nombre de la empresa. Bacchiani publicaba en las redes sociales toda su vida, mostrándose en viajes y en fiestas con famosos y exhibiendo los lujos que se daba, como conducir un automóvil marca Ferrari.
- Técnicas de verificación verbal: la indagación a los damnificados, a los empleados que tenía la financiera, asesores contables y jurídicos, gestores y escribanos que participaban de las operaciones diarias.
- Técnicas de verificación documental: comprobando los comprobantes existentes que identifican los bienes aportados en forma de pago.
- Técnicas de verificación física: inspeccionando las oficinas de la empresa en la provincia de Córdoba, Catamarca y Tucumán.
- Técnicas de verificación informática: de aquí se desprende el concepto de evidencia digital. Por ejemplo: los datos obtenidos por el hacker, el registro de la conversación telefónica intervenida,

correos electrónicos, conversaciones por medio de redes sociales, transferencias de fondos dinerarios o el pago por internet.

La Comisión Nacional de Valores (CNV) para el caso en concreto aplicaría las siguientes funciones:

- Supervisión y Regulación: controla a las entidades, agentes de bolsa, fondos comunes de inversión y mercados, asegurando el cumplimiento de la normativa vigente.
- Protección al Inversor: vela por la transparencia del mercado, garantizando igualdad de trato y acceso a información veraz y clara.
- Capacidad Sancionadora: posee facultades para investigar y sancionar conductas contrarias a las normas en el mercado de valores.

En concreto, la CNV en virtud de la recepción de diversas denuncias de carácter anónimo contra Adhemar Capital SRL inició una investigación por medio de la cual se puso en conocimiento de la Gerencia de Inspecciones e Investigaciones sobre el dudoso accionar de dicha razón social.

Del relevamiento realizado en internet se detectó la presencia del sitio web http://www.adhemarcapital.com.ar/ en donde se ofrecen productos como fondos comunes de inversión. Los usuarios "Adhemarcap" y "edgaradhemar" de Instagram ofrecen asesoramiento y efectúan una invitación a participar de la inversión realizando una transferencia mínima de $500.000 (Pesos Quinientos Mil) y prometiendo ganancias de más del 13% mensual.

Finalmente, el Banco Central de la República Argentina aplicaría las siguientes funciones a nuestro caso:

- Estabilidad Financiera: regular y supervisar el funcionamiento del sistema financiero, incluyendo la aplicación de normas para entidades financieras, bancarias y medios de pago.
- Protección al Usuario: proteger los derechos de los usuarios de servicios financieros, gestionando reclamos y supervisando la transparencia.
- Asesoramiento y Control: contribuir al desarrollo económico, promoviendo la inclusión financiera y la estabilidad del mercado de capitales.

Para el caso de marras, en enero de 2022 el Banco Central de la República Argentina (BCRA) solicitó a la Procuraduría de Criminalidad Económica y Lavado de Activos (PROCELAC) que investigara a Adhemar Capital ante la posibilidad de que estuviera desarrollando

una estafa piramidal bajo la fachada de supuestas inversiones en criptomonedas.

El BCRA actuó tras una denuncia de los gobernadores de Catamarca, Raúl Jalil, y de La Rioja, Ricardo Quintela, quienes alertaron en septiembre del 2021 por las actividades de una serie de empresas dedicadas a captar fondos para criptomonedas. El destape de esta presunta estafa coincidió con el escándalo de Generación Zoe, encabezada por LeonardoOsitorto, quien fue condenado en Goya, Corrientes.

También podemos requerir información a los municipios donde la empresa Adhemar Capital SRL tiene sus oficinas ya que ellos tienen el deber de ejercer el poder de policía para controlar, regular y sancionar actividades no autorizadas protegiendo el orden público y la seguridad.

Estos organismos cuando detectan irregularidades y verifican que las empresas o personas humanas no se encuentran inscriptas por la actividad de captación de fondos deberían actuar en forma casi inmediata y clausurar los establecimientos en cuestión. Y en casos como estos donde se verifica el delito en ningún momento se cuestionó el actuar de los organismos que deberían velar por el bienestar económico de la población.

Por último, tanto los allegados y empleados de Bacchiani pueden tener algún tipo de responsabilidad por encubrimiento o participación en el delito, como también debería indagarse a los profesionales que participaban de las operaciones —escribanos, asesores— ya que dan fe de sus actos, y también las asociaciones y/o fundaciones a las que la empresa hacía donaciones o participación de alguna forma, ya que las mismas podrían estar encubriendo activos de Bacchiani detrás de los fines de cada institución.

6. Conclusión

El fallo comentado indica que el autor de los delitos era una persona con las características de un delincuente de cuello blanco (Sutherland, 1999), que se valía de su audacia para captar ahorristas haciéndoles creer que obtendrían ganancias extraordinarias, con inversiones en bienes sobre las cuales la sociedad aún no comprende su funcionamiento.

El trabajo desarrollado nos permitió conocer nuevos delitos desde un punto de vista económico y federal, despojado del punitivismo que se enfoca en el daño físico a las personas y sus bienes. Nos permitió elaborar nuestra propia teoría del caso, proponiendo técnicas novedosas de investigación en sintonía con el sistema acusatorio adversarial vigente en el ámbito federal.

Por último, nos permitió ahondar en figuras penales poco usuales, generalmente tildadas de complejas —v. gr. intermediación financiera, lavado de activos, régimen cambiario, responsabilidad de las personas jurídicas, etc.— pero cuyo conocimiento resulta sumamente importante para el restablecimiento de la paz social y sobre todo para el cuidado del erario público, que en definitiva termina siendo el aporte económico de todos los ciudadanos para el desarrollo de las políticas públicas de los gobiernos.

Bibliografía

Ares, T. (2011). Autolavado de activos en el Código Penal Argentino. *Revista Pensamiento Penal,* febrero.

Argibay Molina, J. (2021). La administración como modalidad típica de lavado de activos, *Temas de Derecho Penal y Procesal Penal*, Agosto.

Carrara, A. (2017). Capítulo III. En *Poder Ciudadano : corrupción y transparencia : informe 2016-2017.* Secchi P., Kalpschtrej K. y Arcidiácono P. (comp). - CABA: Eudeba.

CIPCE. (2019). *Anteproyecto de Código Penal*. Centro de Investigación y Prevención de la Criminalidad Económica.

Fontán Tapia E. (2023). *Auditoría forense: técnica de investigación, prevención*. Guía práctica para la identificación, trazabilidad e incautación de criptoactivos. Ministerio Público Fiscal de la Nación

Platt, S. (2015). *Criminal capital: how the finance industry facilitates crime*. New York – Basingstoke: Palgrave Macmillan.

Saccani, R. R. (2012). *Tratado de auditoría forense* (Tomo I). KPMG.

Spessot, D. (2022). Delito de intermediación financiera no autorizada. *Revista Pensamiento Penal*, octubre, No. 444.

Sutherland, E. H. (1999). *El delito de cuello blanco*. Madrid. La Piqueta.

Normativa

Código Penal de la Nación Argentina.
Código Procesal Penal Federal.
Ley N.º 19.359 y modificatorias (Régimen Penal Cambiario, texto ordenado 1995).
Ley N.º 25.246/2000 (Encubrimiento y Lavado de Activos de origen delictivo).
Ley N.º 26.683/2011 (modificación art. 303 CP).
Ley N.º 27.401 (Responsabilidad Penal de las Personas Jurídicas Privadas).
Ley N.º 27.430 y modificatoria Ley N.º 27.799 (Régimen Penal Tributario).
Ley N.º 27.739/2024 (modificación Ley 25.246 – incorpora PSAV).
Resolución General CNV N.º 994/2024 y modificatoria N.º 1058/2025.
Resolución General ARCA N.º 4.614/2019 y modificatoria N.º 5.804/2025.
Resolución UIF N.º 70/2011.
Resolución UIF N.º 300/2014.

Jurisprudencia

Cámara en lo Criminal y Correccional de la 10° Nominación, Provincia de Córdoba. “Bacchiani, Edgar Adhemar p.s.a. Estafa Reiterada”. Fallo del 03 de abril de 2025.
“Córdoba, Segundo Pantaleón s/inf. art. 303 inc. 3 del CP”

El delito de estafa en el ecosistema de los activos virtuales: la modalidad rug pull y el caso $LIBRA en Argentina

Ignacio Chiarenza[1] y Manuela Belén Losada[2]

Resumen

El presente artículo analiza la problemática de los delitos económicos en el entorno de los activos virtuales, centrándose específicamente en la modalidad de estafa conocida como rug pull, término utilizado en este ámbito para referirse a una modalidad específica de estafa, cuya traducción al español es "tirón de alfombra". En este sentido, los autores examinan cómo el aprovechamiento de tecnologías descentralizadas y la falta de marcos regulatorios sólidos facilitan maniobras fraudulentas que comprometen la confianza en el orden económico. El núcleo del estudio es el caso LIBRA en Argentina, donde se investiga una presunta estructura criminal que vincula a altos funcionarios públicos con actores privados para la comisión de un delito de estafa mediante la utilización del mercado de los activos virtuales. Se detalla cómo la legitimación institucional y el uso de información privilegiada permitieron inflar artificialmente el valor de un token antes de retirar masivamente la liquidez, perjudicando a miles de

1- Contador Público egresado de la Universidad Nacional del Sur. Diplomado en Análisis Económico Forense. Se desempeña como perito contador en la Unidad de Análisis Contable, Económico y Financiero del Ministerio Público de Río Negro. Correo electrónico: chiarenzaignacio@gmail.com
2- Licenciada en Ciencia Política de la Universidad Nacional de Rosario. Diplomada en Análisis Económico Forense. Actualmente, presta funciones en la Unidad Fiscal Especializada en Microtráfico del Ministerio Público de la Acusación de la Provincia de Santa Fe. Correo: manuelalosada2002@gmail.com

inversores. Finalmente, se exponen los desafíos legales y técnicos que enfrentan las autoridades para prevenir y perseguir estos ilícitos.

1. Introducción

En el año 2008, bajo el seudónimo de Satoshi Nakamoto, se publicó el artículo que dio origen al Bitcoin, instaurando un nuevo paradigma socioeconómico fundamentado en técnicas criptográficas y la tecnología blockchain (cadena de bloques). Este sistema se configuró inicialmente como una red distribuida y descentralizada que permite transacciones sin los nodos intermediarios típicos de las monedas reguladas por los Estados (Nakamoto, 2008). A partir de este hito, se ha desarrollado un ecosistema global donde convergen diversos actores sociales y un "aluvión" de nuevas monedas con tecnologías similares.

En sus etapas de consolidación, el atractivo de los activos virtuales se vinculó a su naturaleza descentralizada y a la relativa anonimidad de las operaciones, aunque la evolución del sistema ha llevado a una mayor concentración en grandes plataformas de intercambio o exchanges. Con el tiempo, la oferta se ha complejizado con la aparición de nuevos productos financieros y activos digitales únicos, como los tokens no fungibles (NFT), lo que ha ampliado el abanico de las tecnologías financieras o fintech (Silva, Santos, Feser y Ferreiro, 2022).

En este contexto, las criptomonedas, en virtud de su carácter digital y descentralizado, se han consolidado como un nuevo escenario tanto para la innovación en el ámbito financiero como para el desarrollo de actividades criminales. De esta manera, la expansión de estas tecnologías financieras genera significativos retos para la prevención y persecución de la criminalidad económica, en un contexto marcado por marcos normativos y contables aún incipientes y por brechas tecnológicas. Asimismo, la proliferación de diversos delitos, tales como fraudes, estafas, lavado de activos y extorsiones, resulta cada vez más evidente, lo que incrementa la complejidad de las investigaciones vinculadas a estos tipos de ilícitos (Silva y Marsili, 2022).

El caso LIBRA en Argentina constituye un punto de inflexión en el uso de activos virtuales, tanto por los actores involucrados como por las tensiones que expone en las capacidades institucionales del

Estado[3]. En este sentido, este hecho presenta características compatibles con esquemas de estafa tipo rug pull, evidenciando la comisión de presuntos ilícitos en un entorno incipientemente regulado. Asimismo, pone en el ojo público las estafas con activos virtuales, al tiempo que da cuenta de su proliferación y de la creciente dificultad para su prevención y persecución, configurándose como un caso sin precedentes en el país.

1.1. Delito económico y elementos constitutivos del ecosistema cripto

En primer lugar, las estafas constituyen uno de los delitos económicos más frecuentes e históricamente extendidos en el orden económico. En este punto, resulta necesario precisar qué se entiende por delito económico. Siguiendo a Tiedemann (1983), se sostiene que las maniobras propias de la criminalidad económica implican ataques a la confianza en el orden económico, siendo su rasgo distintivo el abuso de la confianza social en el tráfico económico: "...el abuso de la confianza socialmente exigible en la vida económica constituye el delito económico" (p. 23).

Por su parte, Pegoraro (2011) conceptualiza los delitos económicos a partir de la noción de organización, en tanto entiende que el delito implica un lazo social que lo determina, en el cual se reproducen múltiples relaciones económicas, tanto legales como ilegales. De este modo, se refiere a la existencia de acciones que suponen una utilidad recíproca entre los actores involucrados, la cual no necesariamente debe ser equivalente ni obtenida de manera legal (Ibidem). A su vez, el autor destaca el carácter organizado del delito económico, el cual puede entenderse como una organización de tipo empresarial dedicada a negocios ilegales y legales de cierta complejidad político-jurídica, que requiere la participación de profesionales o expertos y, con frecuencia, de instituciones o funcionarios estatales, produce una recompensa económica significativa y cuyos participantes tienden a gozar de inmunidad o impunidad social y penal.

3- Infobae. (2026, 9 de abril). Sello institucional y encubrimiento: los motivos detrás de la acusación a funcionarios de Milei en el caso $LIBRA. https://www.infobae.com/judiciales/2026/04/09/sello-institucional-y-encubrimiento-los-motivos-detras-de-la-acusacion-a-funcionarios-de-milei-en-el-caso-libra/

En este marco, resulta pertinente recuperar el concepto de delito económico-político desarrollado por Naucke (2015) para el análisis del caso LIBRA. En particular, el autor atribuye el carácter político de estos delitos a la intervención, tolerancia, omisión o incluso al fortalecimiento estatal de conductas criminales. En este punto, siguiendo a Naucke (2015), el delito económico-político puede comprenderse como aquel que, lejos de ser ajeno al Estado, se configura en un entramado en el que éste resulta tolerante o incluso contribuye a su consolidación.

Por otro lado, al abordar el caso LIBRA en tanto presunto delito de estafa, se advierte que, aun cuando se despliegue en el ecosistema de los criptoactivos, mantiene la estructura típica de las modalidades previstas en este tipo penal: la existencia de un ardid o engaño idóneo que induce a error a la víctima y la conduce a realizar una disposición patrimonial perjudicial. En este sentido, el delito se compone de tres elementos fundamentales —el ardid o engaño, el error y la disposición patrimonial perjudicial— y requiere, además, la verificación de una doble relación causal: "...el ardid o engaño debe ser causa del error, y el error debe ser causa de la disposición patrimonial perjudicial" (Oficina Anticorrupción, 2012, p. 108).

Asimismo, para adentrarse en el entorno de los activos virtuales, se deben identificar los elementos y mecanismos que operan en el mismo. En primera instancia, Silva y Marsili (2024) sostienen que un activo virtual se define como "... una representación digital de valor que puede comercializarse o transferirse digitalmente y que puede utilizarse para pagos e inversiones" (p. 574). Por su parte, estos autores plantean que la tecnología blockchain materializa el funcionamiento del sistema al crear una base de datos virtual en la que cada usuario dispone de una copia actualizada y sincronizada, prescindiendo de una infraestructura centralizada y otorgando a cada participante control pleno sobre sus datos y activos.

En este contexto, dentro del ecosistema de los activos virtuales, las billeteras virtuales constituyen el espacio operativo fundamental para la gestión de activos y la recepción de dividendos, permitiendo que las transacciones queden registradas en la blockchain (Silva, Santos, Feser y Ferreiro, 2022). Estas se encuentran radicadas en software o hardware específicamente diseñados para almacenar y gestionar las claves públicas y privadas de las criptomonedas, las cuales operan de manera complementaria (Ibidem).

De esta manera, por un lado, la clave pública funciona como el identificador de la cuenta dentro de la blockchain y permite recibir fondos; por el otro, la clave privada otorga el control efectivo sobre dichos fondos, constituyendo la contraseña que habilita su disposición. Si bien estas herramientas operan bajo un anonimato relativo, la naturaleza pública de la red garantiza la trazabilidad de las transacciones, en tanto cada operación vincula de forma permanente las carteras intervinientes, lo que permite eventualmente identificar a sus titulares cuando se las asocia con datos de registro en plataformas verificadas (Silva, Santos, Feser y Ferreiro, 2022).

Finalmente, dentro de este esquema, la dinámica del sistema se apoya en los exchanges, plataformas que Silva, Santos, Feser y Ferreiro (2022) definen como agentes que facilitan el intercambio de criptoactivos por dinero fiduciario. Estas pueden ser de naturaleza centralizada, funcionando como nodos intermediarios, o descentralizadas (DEX), las cuales ejecutan los intercambios de forma automática mediante el uso de contratos inteligentes.

1.2. El rug pull como modalidad de estafa en el ecosistema de los activos virtuales

En el análisis penal de defraudaciones la enumeración de ardides es abierta: "en la norma se enumeran expresamente algunos casos... pero se trata de una enumeración no taxativa" (Oficina Anticorrupción, 2012, p. 108). Esto habilita a pensar las estafas con activos virtuales no como un fenómeno "nuevo" ajeno a las categorías clásicas, sino como una actualización de mecanismos de engaño tradicionales en soportes tecnológicos distintos.

En este marco, la prevención y persecución del fraude en el ecosistema de los activos virtuales presenta una serie de desafíos relevantes. Entre ellos, se destacan las dificultades derivadas del pseudoanonimato y de la naturaleza descentralizada de los criptoactivos, que obstaculizan la vinculación directa entre las direcciones de las billeteras digitales y las identidades físicas de sus titulares (Silva, Feser, Santos y Ferreiro, 2022).

En esta misma línea, otra característica relevante es la internacionalización de las transacciones, especialmente cuando estos delitos comprometen a una diversidad de actores que pueden articularse en redes criminales. En este sentido, dichas redes operan

como estructuras transnacionales que movilizan activos a través de circuitos distribuidos a escala global, trascendiendo las fronteras y los controles de los Estados nacionales (Silva y Marsili, 2022). De este modo, las organizaciones delictivas aprovechan las "zonas grises" de las regulaciones locales y la dispersión geográfica para dificultar la determinación de la competencia territorial y ocultar el flujo de capitales mediante el uso de entramados empresariales transnacionales (Ibidem).

No obstante, la propia evolución del sistema hacia el uso de exchanges, junto con la naturaleza pública de la blockchain, introduce elementos que permiten la trazabilidad de los activos, siempre que los investigadores cuenten con la capacitación técnica y la coordinación internacional necesarias para llevar adelante auditorías forenses (Silva, Feser, Santos y Ferreiro, 2022; Silva y Marsili, 2024).

Esta caracterización resulta pertinente al analizar estafas con activos virtuales, dado que el engaño puede presentarse bajo formatos propios del entorno digital —como estrategias de marketing, promesas de rentabilidad o la apariencia de solvencia o "legitimidad" del proyecto—, pero mantiene su función típica: inducir a error para obtener una transferencia de valor. En el caso de los rug pulls —como se verá en la modalidad utilizada en LIBRA—, el ardid suele vincularse con la creación y promoción de un token, la generación de confianza en torno a su liquidez y la posterior extracción de los fondos aportados por inversores, configurando un desplazamiento patrimonial en perjuicio de terceros.

En este sentido, el rug pull constituye una de las modalidades de fraude más prevalentes en el ecosistema de las Finanzas Descentralizadas (DeFi) y se configura como una estafa de salida (exit scam): los creadores de un proyecto atraen a inversores para que compren un nuevo token, inflan artificialmente su precio mediante el "hype" y el marketing, y luego retiran repentinamente los fondos de liquidez asociados.

A diferencia de los mercados tradicionales, donde las transacciones requieren la existencia de una contraparte, en estos sistemas los usuarios interactúan directamente con el fondo de liquidez. Los precios de los activos se determinan y ajustan en tiempo real mediante algoritmos conocidos como creadores de mercado automatizados (AMM), que regulan la relación entre los tokens disponibles en el pool.

En este marco, la fórmula del producto constante ($x \cdot y = k$) permite que, a medida que se intercambian activos, se modifique su proporción: si aumenta la cantidad de un token y disminuye la de otro, su valor relativo se ajusta automáticamente hasta restablecer el equilibrio definido por dicha constante.

A partir de ello, la estafa se configura en el engaño y el proceso de Rug Pull mayormente plantea los siguientes pasos:

- Creación: Se lanza un nuevo token, a menudo en un Intercambio Descentralizado (DEX), y se "empareja" con una criptomoneda estable (como USDT) o una principal (como ETH) en un pool de liquidez.
- Marketing: El equipo (a menudo anónimo o con identidades falsas) implementa una campaña de marketing agresivo en redes sociales, foros y con influencers para generar un "FOMO" (Fear Of Missing Out) masivo y atraer inversión.
- Inflación: La inversión de los usuarios inyecta capital al pool de liquidez, haciendo que el precio del nuevo token suba de forma espectacular.
- El tirón o "pull": Una vez que la liquidez alcanza un nivel crítico, los desarrolladores utilizan un contrato inteligente preestablecido (o simplemente sus claves privadas) para retirar todos los activos valiosos del pool de liquidez (ETH, USDT), rompiendo el par de intercambio.
- Colapso: Al vaciar la liquidez, el precio del token cae a prácticamente cero, dejando a los inversores con activos sin valor y sin la posibilidad de retirarlos.

Aunque el resultado es el mismo, el método de ejecución puede variar, y existen diferentes tipos de rug pulls:

- Retiro de liquidez (el clásico): Los desarrolladores retiran el ETH/USDT del pool de liquidez. Es el más frecuente.
- Venta masiva (pump and dump enmascarado): Los desarrolladores venden su gran reserva de tokens en un solo movimiento, inundando el mercado y haciendo que el precio se desplome catastróficamente.
- Limitación de venta (honeypot): Los desarrolladores codifican el contrato inteligente del token para que solo ellos puedan vender o para limitar estrictamente la capacidad de venta de los inversores minoristas.

En este contexto, se ejecuta la maniobra conocida como "rug pull" al retirar la liquidez de los mercados descentralizados, lo que provoca que los inversores queden con activos que pierden su valor de forma inmediata y resulten imposibles de vender o intercambiar. Un exchange descentralizado (DEX) es una plataforma que facilita el intercambio directo de activos entre usuarios mediante el uso de contratos inteligentes, prescindiendo de intermediarios centralizados.

De esta manera, el denominado pool de liquidez resulta un elemento central: un fondo colectivo de criptomonedas o tokens digitales bloqueados en un contrato inteligente, cuyo propósito es proveer liquidez a los protocolos de finanzas descentralizadas (DeFi) y facilitar el intercambio de criptoactivos. En términos operativos, estos pools se integran por dos o más tokens aportados por usuarios que actúan como proveedores de liquidez, quienes reciben, como contraprestación, una porción de las comisiones generadas por las transacciones realizadas en su interior.

Como se verá en el próximo apartado, esta infraestructura fue fundamental en el caso de LIBRA, un token lanzado en la red Solana que utilizó plataformas como Raydium y Júpiter para atraer liquidez de forma automatizada y sin las verificaciones rigurosas de los entornos tradicionales (Obiaño, 2025; Zeballos, 2025). Raydium funcionó como el exchange descentralizado (DEX) principal donde se listó y comercializó inicialmente el token $LIBRA y, en tanto creador de mercado automatizado (AMM), permitió la conformación de pools de liquidez sin verificaciones estrictas. Por su parte, Júpiter actuó como agregador de liquidez, concentrando gran parte de las operaciones de compra e intercambio al ofrecer a los usuarios las mejores condiciones de precio disponibles. En cuanto a los proveedores de servicios de activos virtuales (PSAV), Ripio fue la única plataforma argentina que listó públicamente el token y lo promocionó a través de sus canales habituales de comunicación.

1.3. El caso $LIBRA Argentina

En este marco, el caso LIBRA en la Argentina se inscribe dentro de las estafas de tipo rug pull, en tanto reproduce los pasos típicos que caracterizan esta modalidad delictiva. En términos de Pegoraro (2011), el caso pone de relieve la organización de tipo empresarial de múltiples relaciones económicas, tanto legales como ilegales, confi-

gurando un entramado económico-político en el que resulta central la participación de actores estatales. Entre estos actores se destacan el presidente Javier Milei, la Secretaria General de la Presidencia Karina Milei y otros funcionarios del gobierno argentino, junto con actores del ámbito privado como Mauricio Novelli, Terrones Godoy y Hayden Davis[4].

El esquema de la maniobra se habría estructurado mediante una colaboración coordinada en la que el respaldo de Javier y Karina Milei funcionó como el factor de legitimación institucional para atraer a miles de inversores hacia el proyecto (Acosta, 2026; Zeballos, 2025). Mientras el entorno presidencial proveía el aval público necesario, la ejecución de la arquitectura operativa habría estado a cargo de actores del sector privado: Mauricio Novelli actuó como el intermediario estratégico y nodo central en la gestión de documentos confidenciales entre las partes, mientras que Manuel Terrones Godoy articuló los contratos de lobby y el acceso a reuniones privadas con el Ejecutivo para influir en el mercado (Volosin, 2026). Por su parte, Hayden Davis, como fundador del token, facilitó el soporte financiero e internacional necesario para el despliegue de la criptomoneda (Volosin, 2026; Zeballos, 2025). Esta estructura organizada permitió la implementación de una estafa técnica de tipo rug pull, orientada a la extracción de rentas privadas mediante el ejercicio de la función pública (Volosin, 2026; Zeballos, 2025).

En primera instancia, LIBRA se desencadenó a partir de una publicación realizada por el Presidente Javier Milei en la red social "X" el día 14/02/2025, en la que promocionaba un proyecto privado orientado a "incentivar el crecimiento de la economía argentina"[5]. En dicha publicación, el Presidente compartió el enlace a la página web del proyecto (vivalalibertadproject.com), el código del contrato inteligente de la criptomoneda (Bo9jh3wsmcC2AjakLWzNmKJ3SgtZmXEcSaW7L2FAvUsU) y el tag "$LIBRA", haciendo pública información que hasta ese momento no se encontraba difundida, potenciando así su alcance y circulación.

4- Infobae. (2026, 8 de abril). Quién es quién en la causa $LIBRA: todos los involucrados y los roles que habrían tenido en la maniobra. https://www.infobae.com/judiciales/2026/04/08/quien-es-quien-en-la-causa-libra-todos-los-involucrados-y-los-roles-que-habrian-tenido-en-la-maniobra/

5- BBC Mundo. (2024). El escándalo de Javier Milei con $LIBRA: qué es el "rug pulling" y qué recomiendan los expertos para evitar este tipo de estafas con criptomonedas. https://www.bbc.com/mundo/articles/cj3n5gjd2dxo

El Informe Final de la Comisión Especial Investigadora sobre la Criptomoneda $LIBRA (2025) expone que el token denominado $LIBRA fue creado y emitido sobre la blockchain de Solana y que presentó un suministro total de 1.000 millones de unidades, de las cuales entre el 70% y el 85% quedaron en manos de un grupo reducido de promotores y creadores del activo, significando esta concentración un riesgo estructural para los eventuales compradores minoristas.

La investigación permitió determinar que la página web fue creada el mismo día de la publicación del Presidente, unas horas antes (14:05 hs.), y que, en forma posterior a la creación de la página y previo a la publicación del Presidente (19:01:22 hs.), se emitió el token (18:38 hs.) y se conformó el pool de liquidez (18:51 hs.). Diez minutos después de la creación del pool de liquidez (19:01 hs.) se registraron las primeras transacciones: 87 transacciones desde 74 billeteras distintas por un total de 13,5 millones de dólares, lo cual revela el conocimiento privilegiado acerca del lanzamiento por parte de algunas personas, ya que hasta la publicación del Presidente la información no era de público conocimiento (Comisión Investigadora sobre la Criptomoneda $LIBRA, 2025).

A las 19:01:22 hs (22 segundos después), el Presidente realizó la publicación en X. Luego de ello, el precio de la criptomoneda $LIBRA registró un incremento súbito, alcanzando un valor máximo cercano a los 1,20 USD por unidad. Alrededor de las 19:40 hs el valor de $LIBRA comenzó a caer en forma abrupta y sostenida, característica típica de una maniobra fraudulenta tipo rug pull, en las cuales los creadores y tenedores iniciales liquidan de manera masiva sus posiciones, retirando la liquidez del mercado y provocando pérdidas significativas para los inversores minoritarios (Comisión Investigadora sobre la Criptomoneda $LIBRA, 2025).

La magnitud del perjuicio económico derivado de esta maniobra alcanzó una escala masiva. Según el informe técnico pericial incorporado al expediente de la Comisión, un total de 143.142 billeteras operaron con el token $LIBRA, de las cuales el 79,93% (114.410 wallets) registraron pérdidas patrimoniales. En el ámbito local, solo el exchange Ripio contabilizó 1.329 usuarios argentinos afectados (Comisión Investigadora sobre la Criptomoneda $LIBRA, 2025). De este modo, puede sostenerse que la maniobra no sólo implicó un perjuicio patrimonial para un amplio número de inversores, sino que

también constituyó, siguiendo a Tiedemann (1983), un ataque a la confianza en el orden económico.

Desde el punto de vista técnico, la investigación confirmó la existencia de información privilegiada: se detectó que 74 billeteras realizaron compras por 13,5 millones de dólares apenas 22 segundos antes de la publicación presidencial. En este sentido, se señaló que es imposible identificar un contrato de 43 caracteres en la blockchain de Solana en medio de miles de operaciones simultáneas sin que alguien facilitara el código directamente al Presidente. Esto sugiere que la publicación no fue un acto espontáneo, sino el núcleo de una maniobra coordinada (Comisión Investigadora sobre la Criptomoneda $LIBRA, 2025).

En esta tónica, los apartados 6 y 7 de dicho informe evidencian los mecanismos utilizados, las características y los flujos de transacciones que acontecieron en la operación. En el apartado 6 se concluye que el lanzamiento, la promoción y el posterior vaciamiento del token $LIBRA presentan rasgos característicos de maniobras fraudulentas, evidenciados en la concentración del pool de liquidez en pocas billeteras, la compra anticipada de tokens por insiders y la difusión de una narrativa engañosa sobre su supuesta utilidad. Asimismo, se destaca que la promoción presidencial resultó determinante para dotar al activo de una visibilidad y un volumen de operaciones que no habría alcanzado por sí mismo. En el apartado 7, a partir de la información recabada de distintos exchanges, se logró identificar billeteras vinculadas a las personas investigadas, reconstruir flujos de transacciones potencialmente asociados a pagos indirectos a funcionarios públicos y detectar circuitos de liquidación de criptoactivos en efectivo (Comisión Investigadora sobre la Criptomoneda $LIBRA, 2025).

Meses más tarde de la publicación del informe final de la comisión investigadora de $LIBRA (2025), el informe de la Dirección de Apoyo Tecnológico a la Investigación Penal (DATIP), dependiente del Ministerio Público Fiscal de la Nación, presentado en el marco de la causa penal, expuso el análisis de los dispositivos electrónicos de uno de los principales implicados, Mauricio Novelli (Ministerio Público Fiscal de la Nación, 2026). A partir de las pericias informáticas, se evidenció que el vínculo entre el entorno presidencial y los organizadores del proyecto no resultaba casual ni reciente (Volosin, 2026). En este sentido, se recuperaron registros de reuniones realizadas por Zoom que datan de abril de 2021, en las que participaron Javier Milei, Karina

Milei y el propio Novelli, es decir, con anterioridad a la llegada al poder (Hauser, 2026).

Entre los hallazgos más relevantes del peritaje, se identificó una Carta de Intención (LOI) titulada "LOI_KELSIER.docx", enviada al celular de Novelli el 29 de enero de 2025, en la cual Hayden Davis figura como asesor del gobierno en materia de blockchain e inteligencia artificial, lo que permite inferir la existencia de un vínculo previo con el entorno presidencial (Alconada Mon, 2026).

Asimismo, el peritaje detectó comunicaciones directas entre el presidente Javier Milei, su hermana Karina Milei y Mauricio Novelli, ocurridas minutos antes y después del lanzamiento del token $LIBRA. También se identificaron chats que datan de enero de 2024, en los que se detallan gestiones vinculadas a eventos oficiales, manejo de efectivo y acceso directo a funcionarios de la Secretaría General de la Presidencia.

Por otra parte, se halló una factura de 250.000 dólares en USDC emitida por la empresa de Novelli (Tech Forum Argentina) a nombre de Kelsier Holding Limited, firma vinculada a Hayden Davis, por servicios de consultoría, lo que daría cuenta de un nexo comercial previamente negado[6]. El informe vincula estas comunicaciones con movimientos financieros posteriores al lanzamiento del activo, incluyendo el vaciamiento de una caja de seguridad en el Banco Galicia por parte de familiares de Novelli poco después de la operatoria (González del Solar, 2025).

En este marco, el peritaje elaborado por la DATIP constituye una pieza clave en la causa penal en trámite. Los hallazgos expuestos en el informe técnico incluyen registros de comunicaciones previas, precisiones de carácter contractual y evidencias sobre la participación de los distintos actores involucrados en la operatoria. Tales elementos refuerzan la hipótesis de la existencia de una estructura organizada orientada a facilitar la maniobra fraudulenta (Zeballos, 2025).

A su vez, esta evidencia implicaría la participación del presidente de la Nación, Javier Milei, y de la Secretaria General de la Presidencia, Karina Milei, en tanto su promoción pública del token habría constituido un factor determinante en el ascenso acelerado y posterior colapso del activo. En términos de Naucke (2015), este hecho

6- elDiarioAR. (2026, 2 de marzo). El Gobierno niega la firma de un acuerdo entre Milei y el mentor de la presunta estafa $LIBRA. https://www.eldiarioar.com/politica/gobierno-niega-firma-acuerdo-milei-mentor-presunta-estafa-libra_1_12964235.html

no solo permite advertir una forma de intervención estatal, sino que evidencia un involucramiento directo que contribuye a legitimar y amplificar la maniobra delictiva, es decir, la constitución de un delito económico-político.

En esta tónica, la Comisión Investigadora (2025) determinó que el caso LIBRA no fue un hecho aislado, sino la repetición de un patrón de conducta, detectado en diciembre de 2024 con la criptomoneda KIP. En ese antecedente, el Presidente también otorgó su aval político, permitiendo que los mismos operadores —Novelli y Terrones Godoy— liquidaran posiciones y obtuvieran ganancias antes del desplome del activo. Asimismo, el análisis de trazabilidad financiera detectó flujos de fondos que coinciden con un presunto acuerdo para "monetizar la imagen" del Jefe de Estado.

Producto del hecho descripto, se iniciaron múltiples denuncias penales en la República Argentina. Más de un centenar de presentaciones fueron radicadas en el fuero federal, concentrándose la causa principal ante el Juzgado Federal N.º 1. La investigación se orienta a determinar la posible comisión de delitos tales como estafa, cohecho, tráfico de influencias, abuso de autoridad y negociaciones incompatibles con la función pública, en un contexto atravesado por el presunto aprovechamiento de información privilegiada y la utilización de la investidura presidencial para inducir al público a invertir en un token que posteriormente habría sido liquidado de manera coordinada.

En paralelo, se activaron acciones judiciales en Estados Unidos (Infobae, 2025) y en España (Ruiz, 2025). En el primer caso, se promovió una demanda colectiva por fraude y manipulación de mercado contra los responsables del proyecto; en el segundo, se registró la acumulación de denuncias judiciales y la preparación de acciones colectivas internacionales a partir de la afectación de inversores españoles.

Estos acontecimientos no sólo dan cuenta de la magnitud y la proyección transnacional de la estafa, sino que también ponen en evidencia una de las principales dificultades en la prevención y persecución de delitos en el ecosistema de los activos virtuales: la multiplicidad de jurisdicciones involucradas. En efecto, la realización de transacciones a escala global no sólo complejiza su trazabilidad, sino que exige la articulación de mecanismos de cooperación internacional eficaces y ágiles.

2. Reflexiones finales

El presente artículo permite sostener que las estafas en entornos de activos virtuales —y en particular los rug pulls— obligan a repensar categorías centrales de los delitos económicos y de la práctica investigativa tradicional. En este sentido, la principal novedad no reside en la estructura delictiva, que reproduce esquemas clásicos de estafa y defraudación, sino en el espacio económico en el que estas maniobras se desarrollan.

El ecosistema cripto no elimina la racionalidad económica del delito, pero sí altera los tiempos y herramientas sobre los que históricamente se apoyó la intervención estatal, tensionando la eficacia de los mecanismos de control. Esto exige que los marcos regulatorios y las capacidades investigativas se amplíen y redefinan, no solo para perseguir penalmente estas conductas, sino también para interrumpir las lógicas de acumulación ilícita que las sostienen.

Siguiendo la concepción de Pegoraro (2011), esta acumulación debe entenderse como una "acumulación originaria" continua, que utiliza medios ilegales para producir y reproducir un orden social basado en la desigualdad y el privilegio. Bajo esta perspectiva, el desafío de control no es meramente técnico, sino político, ya que estas maniobras consolidan un lazo social delictivo que suele garantizar la impunidad o inmunidad de los sectores con mayor poder económico. De este modo, el delito económico organizado no se presenta como una anomalía, sino como un elemento constitutivo y funcional para la reproducción de la estructura social actual.

El caso LIBRA resulta ilustrativo de estas dinámicas. A nivel técnico, el uso de herramientas como el agregador Júpiter y el DEX Raydium en la red Solana habría permitido atraer una liquidez millonaria que luego fue retirada de forma abrupta, provocando el colapso del activo y dejando a los inversores con saldos imposibles de liquidar. A partir de este escenario, el hecho se consolida como un ejemplo paradigmático de rug pull en el ecosistema DeFi. A través de la creación de un token en la red Solana y el uso de exchanges descentralizados, se desplegó una maniobra que representa lo que Tiedemann (1983) denomina el abuso de las posibilidades formales y estructurales de los instrumentos económicos.

Pese a su sofisticación tecnológica, la operación mantuvo la lógica clásica del fraude: un ardid idóneo que indujo a error a los inversores y generó una disposición patrimonial perjudicial masiva. Al dejar a más de 114.000 billeteras con activos sin valor, el caso trascendió la estafa convencional para afectar un bien jurídico supraindividual: la integridad de la vida económica y la confianza en el orden que la rige. De este modo, la maniobra no solo lesionó patrimonios individuales, sino que, en términos de Tiedemann (1983), generó una afectación a la confianza social que es esencial para el funcionamiento de cualquier sector de la economía.

En este contexto, la dimensión más crítica de la maniobra de rug pull implementada en LIBRA radica en la intervención directa de miembros del Poder Ejecutivo, lo cual configura lo que Naucke (2015) denomina un delito económico-político: aquel que es fortalecido o auspiciado por el aparato del Estado. En este sentido, la participación oficial operó como un factor de legitimación institucional que transformó la maniobra en una forma de criminalidad estatal, donde el Estado, en lugar de controlar, potenció el éxito de la operación económica.

Por su parte, la evidencia técnica, que registró compras millonarias realizadas segundos antes del anuncio oficial, refuerza la hipótesis de coordinación y el uso de información privilegiada, manifestando un uso del poder público para favorecer un poder económico avasallador que, según Naucke (2015), destruye los fundamentos de la libertad individual y las instituciones jurídicas que deberían protegerla. Asimismo, los vínculos previos entre el entorno presidencial y actores privados involucrados esgrimen la posibilidad de la conformación de una estructura organizada orientada a la extracción de rentas mediante el ejercicio de la función pública.

No obstante, cabe destacar que la tecnología blockchain garantiza la trazabilidad de las operaciones, lo que permite a los investigadores reconstruir los flujos de fondos y avanzar en la eventual determinación de responsabilidades. En este sentido, la investigación de este tipo de maniobras requiere la articulación de herramientas específicas: en una primera etapa, la identificación de las billeteras vinculadas a los fundadores —especialmente cuando concentran grandes porcentajes de los tokens emitidos—; en segundo lugar, la desanonimización de la blockchain, que implica vincular direcciones digitales con identidades físicas mediante información externa; y, por último, la aplicación de

técnicas de análisis de redes y clustering, que permiten detectar comportamientos coordinados, identificar concentraciones de ganancias y reconstruir relaciones entre actores, incluso cuando las billeteras aparentan operar de manera independiente.

Asimismo, la investigación no debe limitarse al análisis digital: la detección de elementos físicos —como dispositivos, claves o documentación— en eventuales allanamientos puede resultar determinante para robustecer la reconstrucción de la maniobra. En paralelo, la rapidez en la intervención sobre los fondos en exchanges resulta clave para evitar su dispersión o conversión.

En síntesis, el caso LIBRA plantea un desafío institucional sin precedentes para las sociedades democráticas. La descentralización tecnológica exige una mayor capacidad técnica, coordinación internacional y transparencia para evitar que la investidura pública sea utilizada como herramienta de defraudación masiva, al tiempo que abre interrogantes sobre cómo las nuevas tecnologías reconfiguran los órdenes sociales y económicos contemporáneos en contextos de alta digitalización y desintermediación financiera. A su vez, en el contexto argentino, resulta necesario indagar de qué manera estas transformaciones impactan en la confianza institucional, en los mecanismos de control estatal y en la capacidad efectiva de regulación.

Bibliografía

Acosta, M. (2026). El escándalo $LIBRA y la opinión pública argentina. *Más Poder Local*, (63), 108-120. https://doi.org/10.56151/maspoderlocal.315

Nakamoto, S. (2008). *Bitcoin: Un sistema de efectivo electrónico usuario-a-usuario*. https://bitcoin.org/files/bitcoin-paper/bitcoin_es_latam.pdf

Naucke, W. (2015). *El concepto de delito económico-político: Una aproximación* (E. Sarrabayrouse, Trad.). Marcial Pons.

Obiaño, P. O. (2025). El caso $LIBRA: una mirada desde el derecho penal. *Revista Pensamiento Penal*, 1(4), 105-109. https://doi.org/10.64178/c5j2xz82

Oficina Anticorrupción. (2012). *Perspectiva del derecho penal sobre los actos de corrupción: El rol de la Oficina Anticorrupción*. Ministerio de Justicia y Derechos Humanos de la Nación; PNUD Argentina.

Pegoraro, J. S. (2011). *Los lazos sociales del delito económico y el orden social*. Eudeba.

Silva, G., Feser, M. E., Santos, M., y Ferreiro, J. (2022). Criptomonedas y delitos complejos: hacia una nueva perspectiva de su impacto en la investigación criminal. *Minerva. Saber, arte y técnica*, 6(2), 6–19.

Silva, G., y Marsili, M. (2022). ¿Cómo desarrollar una investigación en criminalidad económica a partir de metodologías de investigación consolidadas en las ciencias sociales? En *Delitos económicos: Caja de herramientas para quienes investigan, litigan y juzgan* (Tomo I). Instituto de Estudios Comparados en Ciencias Penales y Sociales (INECIP).

Silva, G., y Marsili, M. (2024). Criptoactivos y los desafíos pendientes: Modelos de datos alternativos aplicados a la criminalidad económica con uso de criptoactivos. En *El Estado y la administración pública en debate: Encrucijadas y desafíos para el desarrollo* (Vol. 2, pp. 563–575). Asociación Argentina de Estudios de Administración Pública.

Tiedemann, K. (1983). El concepto de derecho económico, de derecho penal económico y de delito económico. *Revista Chilena de Derecho*, 10, 59–70.

Volosin, N. (2026, 6 de marzo). EXCLUSIVO $LIBRA: el acuerdo que habría firmado Milei con Hayden Davis. *La Justa*. https://www.nataliavolosin.com/newsletter/65

Zeballos, A. (2025). $LIBRA: Anatomía de un cryptogate argentino. *Revista Pensamiento Penal*, 1(1), 96–99. https://doi.org/10.64178/5r4dc340

Informes y documentos institucionales

Honorable Cámara de Diputados de la Nación. (2025). Informe final de la Comisión Investigadora sobre la Criptomoneda $LIBRA (Expte. 6622-D-2025). https://www4.hcdn.gob.ar/dependencias/dsecretaria/Periodo2025/PDF2025/TP2025/6622-D-2025.pdf

Ministerio Público Fiscal de la Nación. (2026, 20 de marzo). Comunicado de la Fiscalía Nacional en lo Criminal y Correccional Federal N.º 8 sobre la causa $LIBRA. https://www.fiscales.gob.ar/fiscalias/comunicado-de-la-fiscalia-nacional-en-lo-criminal-y-correccional-federal-n8-sobre-la-causa-libra/

Fuentes periodísticas

Alconada Mon, H. (2026, 18 de marzo). Caso $LIBRA | Los pagos que exponen cómo Mauricio Novelli forjó su relación con los Milei en el camino al poder. *La Nación*.

BBC Mundo. (2024). El escándalo de Javier Milei con $LIBRA: qué es el "rug pulling" y qué recomiendan los expertos para evitar este tipo de estafas con criptomonedas.

elDiarioAR. (2026, 2 de marzo). El Gobierno niega la firma de un acuerdo entre Milei y el mentor de la presunta estafa $LIBRA.

González del Solar, F. (2025, 9 de julio). Uno de los protagonistas del caso $LIBRA manejó cajas de seguridad en un banco en paralelo al asesoramiento financiero que brindaba. *La Nación*.

Hauser, I. (2026, 27 de febrero). Las conversaciones entre Javier Milei y Mauricio Novelli por LIBRA. *Página/12*.

Infobae. (2025, 17 de febrero). Las consecuencias legales que enfrentan los involucrados en la estafa de $LIBRA según la ley de EE.UU.

Infobae. (2026, 8 de abril). Quién es quién en la causa $LIBRA: todos los involucrados y los roles que habrían tenido en la maniobra.

Infobae. (2026, 9 de abril). Sello institucional y encubrimiento: los motivos detrás de la acusación a funcionarios de Milei en el caso $LIBRA.

Ruiz, I. (2025, 26 de febrero). El escándalo de la criptomoneda $LIBRA sumó una denuncia judicial en España. *La Nación*.

Desafíos de la persecución penal estratégica en materia de criptoactivos. Un Análisis FODA (fortalezas, oportunidades, debilidades y amenazas)

Elia Bollecich Masters[1]

Resumen

El presente artículo analiza los desafíos que plantea la persecución penal estratégica de los delitos cometidos mediante la utilización de criptoactivos, a partir de un análisis de las fortalezas, oportunidades, debilidades y amenazas que inciden en la capacidad de respuesta estatal. Para ello, se emplea la matriz FODA como herramienta metodológica orientada a construir un diagnóstico integral del fenómeno y a identificar posibles líneas de acción.

1. Introducción

El crecimiento exponencial de las tecnologías emergentes ha transformado el panorama financiero global, y los criptoactivos han jugado un papel central en esta evolución. Sin embargo, su naturaleza anónima, descentralizada y cambiante, combinada con marcos normativos débiles y brechas tecnológicas, ha transformado las formas de circulación de valor, introduciendo un nuevo paradigma tecnológico-financiero

1- Elia Bollecich Masters. Abogada (UNR). Especializanda en Derecho Penal (UNR). Diplomada en Análisis Económico Forense (CEI – UNR). Auxiliar del Proyecto de Investigación "Criptoactivos. Herramientas contables y jurídicas para la prevención e investigación de delitos cometidos a través de operaciones con activos digitales". Correo: elibmasters@gmail.com

que, si bien presenta desafíos importantes para los mecanismos tradicionales de investigación, también abre oportunidades para desarrollar nuevas capacidades investigativas y regulatorias.

Este análisis parte de la hipótesis de que los criptoactivos instauran un nuevo paradigma tecnológico-financiero que modifica profundamente las condiciones en las que ciertos delitos pueden materializarse, exigiendo enfoques innovadores en materia de prevención y persecución penal.

Ante este escenario, se plantea como objetivo general identificar las fortalezas y debilidades de los Estados relativos a la prevención y persecución de los delitos cometidos mediante su utilización, con el fin de diseñar mecanismos de control e investigación más eficaces. Y partiendo de ello, se plantean las estrategias y acciones para avanzar en la prevención e investigación del delito cuando es cometido por este medio.

2. Análisis FODA

Los criptoactivos no solo transforman las dinámicas económicas, sino también las condiciones en las que se desarrollan las investigaciones penales. Al respecto, se ha señalado que su utilización puede constituir simultáneamente una fortaleza y una debilidad para la investigación criminal, en tanto el anonimato de las transacciones puede facilitar la detección de actividades ilícitas, pero al mismo tiempo la complejidad tecnológica y la escasa regulación dificultan la identificación de los sujetos intervinientes y el rastreo de las operaciones relevantes.

El análisis FODA constituye una herramienta metodológica orientada a evaluar los factores internos y externos que inciden en una organización o fenómeno determinado de manera integral. Este análisis permite identificar las fortalezas y debilidades que configuran su situación interna, así como las oportunidades y amenazas que surgen del entorno. Se trata de un instrumento de carácter sintético que facilita la construcción de una visión estratégica global, en tanto posibilita articular las capacidades propias con las condiciones externas (Ponce Talancón, 2006, p. 2). A fin de abordar de manera sistemática la complejidad que presenta la persecución penal en materia

de criptoactivos, se recurre al análisis FODA como herramienta metodológica. La determinación de fortalezas, oportunidades, debilidades y amenazas posibilita construir un diagnóstico integral de la situación analizada y, a partir de ello, formular estrategias orientadas a optimizar la respuesta institucional frente a este tipo de criminalidad.

2.1. Fortalezas a destacar

1. Trazabilidad de la blockchain

Una de las principales fortalezas en la investigación de delitos vinculados a criptoactivos radica en la trazabilidad inherente a la tecnología blockchain. Esta característica se explica a partir del propio diseño del sistema que se basa en un registro distribuido en el que cada transacción queda asentada de forma permanente, pública e inmutable. En la blockchain, la información se organiza en bloques interconectados, cuya integridad se garantiza mediante el uso de funciones hash, esto es, algoritmos matemáticos que actúan como una "huella digital" de los datos. De este modo, cualquier alteración en la información registrada modifica el hash correspondiente y rompe la cadena, lo que permite detectar inmediatamente cualquier intento de manipulación (Aginsky, 2023).

Asimismo, la estructura encadenada de los bloques posibilita reconstruir el historial completo de las transacciones, ya que cada bloque contiene información del anterior, generando una secuencia continua y verificable. Esta combinación de transparencia, inmutabilidad y registro descentralizado no solo impide la alteración de los datos, sino que además permite seguir el recorrido de los activos digitales a lo largo del tiempo.

En consecuencia, la trazabilidad se configura como una herramienta de gran valor para la investigación penal, en tanto habilita la reconstrucción de circuitos financieros digitales, la detección de patrones de comportamiento y el rastreo de operaciones sospechosas.

2. Regulación de los Proveedores de Servicios de Activos Virtuales en Argentina

Otra de las fortalezas relevantes en materia de persecución penal vinculada a criptoactivos en Argentina radica en el avance progresivo de su regulación, particularmente a partir de la incorporación de los

Proveedores de Servicios de Activos Virtuales (PSAV) como sujetos obligados dentro del sistema de prevención de lavado de activos y financiamiento del terrorismo. La Ley 27.739[2], al incorporar el artículo 4 bis y modificar el régimen de la Ley 25.246[3], reconoce y delimita normativamente a estos actores, comprendiendo a aquellas personas humanas o jurídicas que intervienen en el intercambio, transferencia, custodia o administración de activos virtuales.

La relevancia de esta regulación radica en que permite incorporar a los principales intermediarios del ecosistema cripto, como las plataformas de intercambio o exchanges, dentro del circuito formal de control estatal. En ese marco, se impone la obligación de registración de los PSAV ante la Comisión Nacional de Valores (CNV), así como el deber de informar operaciones y reportar operaciones sospechosas ante la Unidad de Información Financiera.

Por otra parte, el marco regulatorio vigente impone a los PSAV la adopción de sistemas de prevención, incluyendo la implementación de manuales de procedimiento, designación de oficiales de cumplimiento y, de manera especialmente relevante, la utilización de herramientas tecnológicas de análisis y rastreo de transacciones en blockchain. Estas exigencias no solo fortalecen los estándares de control, sino que además generan condiciones institucionales que facilitan el acceso a información clave para la reconstrucción de maniobras ilícitas.

En razón de ello, la regulación de los PSAV se configura como una fortaleza en tanto reduce los niveles de opacidad del sistema, facilita la individualización de los sujetos intervinientes y habilita la articulación entre organismos de control y operadores judiciales.

3. Experiencia de los Ministerios Públicos Fiscales en la investigación de criminalidad compleja

Otra fortaleza relevante radica en la experiencia acumulada por los Ministerios Públicos Fiscales en la investigación de fenómenos de criminalidad compleja. Si bien la criminalidad vinculada a criptoactivos presenta particularidades técnicas propias, comparte rasgos estructurales con otras formas de criminalidad económica organizada, tales como la transnacionalidad, la sofisticación de las maniobras, la

2- Ley 27.739, modificatoria de la Ley 25.246, Boletín Oficial de la República Argentina, 15/03/2024.
3- Ley 25.246, Boletín Oficial de la República Argentina, 10/05/2000.

utilización de testaferros y la necesidad de articular conocimientos interdisciplinarios, ya sean legales, contables, forenses, entre otros.

Desde este enfoque, las capacidades previamente desarrolladas en la investigación de delitos como el lavado de activos, estafas o la criminalidad organizada, resultan transferibles al análisis de operaciones con criptoactivos. Ello se traduce en la aptitud para reconstruir circuitos financieros complejos, coordinar investigaciones con múltiples organismos y articular el trabajo con equipos técnicos especializados.

Cabe destacar que en la ciudad de Rosario, el Ministerio Público de la Acusación tiene una unidad fiscal especializada en la investigación de delitos económicos. Del mismo modo, a nivel federal, en el Ministerio Público Fiscal funciona la Procuraduría de Criminalidad Económica y Lavado de Activos (PROCELAC).

2.2. Principales debilidades identificadas

1. Falta de especialización y formación de los investigadores en la temática

La persecución penal de la criminalidad asociada a los criptoactivos presenta una debilidad marcada que radica en la insuficiente capacitación y especialización técnica de los operadores del sistema de justicia. La complejidad inherente a estas tecnologías no solo exige la incorporación de nuevos conocimientos, sino también la reformulación de prácticas, metodologías y herramientas de investigación tradicionales. Al respecto, se ha señalado que la actualización de los procedimientos investigativos implica el tránsito por nuevas curvas de aprendizaje, que resultan costosas tanto para los individuos como para las instituciones encargadas de la persecución penal (Silva, Feser, Santos y Ferreiro, 2023, p. 5).

Esta situación se ve agravada por la rápida evolución del ecosistema cripto, que genera una brecha constante entre la innovación tecnológica y la capacidad de respuesta estatal. En virtud de ello, los organismos encargados de la investigación, y en particular los Ministerios Públicos Fiscales, enfrentan la necesidad de fortalecer sus capacidades técnicas para abordar fenómenos delictivos cada vez más complejos, caracterizados por el uso de herramientas digitales avanzadas y estructuras descentralizadas (Ministerio Público Fiscal de la Nación, 2023, p. 10).

La falta de formación especializada impacta directamente en la eficacia de las investigaciones, en tanto dificulta la correcta interpretación de la evidencia digital, la identificación de maniobras ilícitas y el diseño de estrategias investigativas adecuadas. De este modo, la capacitación continua y la incorporación de conocimientos técnicos específicos se presentan no solo como una necesidad operativa, sino como una condición indispensable para reducir la brecha existente entre la sofisticación del delito y la respuesta del sistema penal.

2. Anonimato / pseudoanonimato de los operadores de cripto

Una segunda debilidad relevante en la persecución penal de ilícitos vinculados al ecosistema cripto se vincula con el carácter pseudónimo de las transacciones y las limitaciones estructurales para la individualización de los sujetos intervinientes. Cabe destacar que la tecnología blockchain no incorpora datos personales en sus registros, limitándose a consignar direcciones alfanuméricas sin referencia directa a identidades reales, lo que impide, por sí sola, determinar quién se encuentra detrás de cada operación (*Ibíd*., pp. 37–38).

En este contexto, la individualización de los usuarios requiere necesariamente el acceso a información complementaria proveniente de fuentes externas, tales como plataformas de intercambio, registros administrativos u otros datos asociados a la actividad digital de los individuos. Sin embargo, cuando las operaciones se realizan por fuera de estos circuitos o mediante herramientas diseñadas para incrementar la opacidad, la posibilidad de vincular las transacciones con personas determinadas se ve significativamente reducida (*Ibíd*., p. 38).

Esta problemática ha sido advertida también a nivel internacional por el Grupo de Acción Financiera Internacional (GAFI). En particular, se ha señalado que las características propias de los criptoactivos, como la posibilidad de realizar operaciones transfronterizas de manera rápida y fuera de los sistemas financieros tradicionales, permiten a los actores criminales ocultar el origen y destino de los fondos, dificultando la detección oportuna de actividades sospechosas y generando obstáculos concretos para su detección e investigación (Grupo de Acción Financiera Internacional, 2020).

3. Limitaciones en el acceso a herramientas tecnológicas especializadas y capacidades técnicas

La investigación de delitos vinculados a criptoactivos presenta una elevada complejidad técnica que excede los marcos tradicionales del análisis jurídico-penal. Como se ha indicado en el punto anterior, si bien la tecnología blockchain permite acceder a un registro público de transacciones, la información disponible se limita a datos técnicos, como direcciones, montos, fechas y hashes, sin revelar por sí misma la identidad de las personas intervinientes (Oppel, 2022). Esta característica obliga a los investigadores a recurrir a herramientas adicionales para reconstruir operaciones y vincular direcciones con sujetos determinados.

En ese marco, existen softwares especializados que permiten analizar transacciones, agrupar direcciones e identificar patrones de comportamiento (*Ibíd*). Sin embargo, estas herramientas son mayormente desarrolladas por empresas privadas, lo que restringe su acceso y utilización por parte de los organismos públicos.

La práctica investigativa confirma esta limitación. En un caso, analizado en el primer número de los *Cuadernos sobre criminalidad económica* (Gimenez Monti y Loyola, 2025, pp. 67-89), el avance en la determinación de los responsables por parte del Ministerio Público de la Acusación fue posible a partir del uso de software específico y la colaboración de empresas privadas como TRM Labs, que aportaron herramientas de análisis del flujo de fondos y vinculación de direcciones, evidenciando la dependencia de estos recursos para el desarrollo eficaz de la investigación.

En definitiva, la limitada disponibilidad de herramientas tecnológicas, sumada a la necesidad de conocimientos técnicos especializados para su utilización, configura una debilidad estructural que incide directamente en la eficacia de la persecución penal de este tipo de criminalidad.

En este marco, resulta particularmente relevante la existencia de antecedentes en la investigación de delitos vinculados a criptoactivos, en los que se han abordado problemáticas como las dificultades probatorias, la recuperación de activos digitales y la cooperación internacional. Estas experiencias evidencian que, lejos

de partir desde cero, los Ministerios Públicos Fiscales cuentan con una base operativa, técnica y metodológica que, adecuadamente adaptada, permite enfrentar con mayor eficacia los desafíos que plantea el ecosistema cripto.

2.3. Amenazas

1. Uso de herramientas que aumentan la opacidad (mixers, peeling chain, cross-chain swaps)

En esta investigación, se advirtió que una de las principales amenazas para las investigaciones de delitos cometidos con criptoactivos es el uso de distintas herramientas que están diseñadas para ocultar o dificultar el rastreo de las transacciones. Entre ellas, se destacan los mixers o servicios de mezcla, el peeling chain y los cross-chain swaps, que permiten fragmentar, redistribuir o trasladar activos entre distintas redes con el objetivo de desdibujar su recorrido.

Si bien la tecnología blockchain permite reconstruir el flujo de fondos a partir de la información pública de las transacciones, tal como fue desarrollado en el punto 2.1.1., identificando direcciones intervinientes, montos, fechas y horarios, dicha trazabilidad no implica la identificación directa de los sujetos involucrados, sino únicamente de las direcciones utilizadas (Oppel, 2022, pp. 90-93). En este marco, las herramientas indicadas operan precisamente sobre esta limitación estructural, introduciendo mecanismos que rompen la vinculación lineal entre origen y destino de los activos.

En esta línea, el GAFI ha advertido que los activos virtuales pueden ser utilizados para ocultar el origen de los fondos ilícitos y facilitar su movimiento a través de múltiples transacciones y jurisdicciones, dificultando su detección e investigación (Grupo de Acción Financiera Internacional, 2020, p. 2). El organismo indica como señales de alerta, entre otras, la realización de múltiples transacciones consecutivas entre distintas direcciones o el uso de servicios de mezcla inmediatamente después de recibir fondos.

El GAFI también ha señalado que la evolución constante de estas tecnologías incrementa la sofisticación de los mecanismos de ocultamiento, generando desafíos adicionales para las autoridades encargadas de la persecución penal (Grupo de Acción Financiera Internacional, 2021).

Desde una perspectiva práctica, el uso de estas herramientas impacta directamente en la eficacia de las investigaciones, en tanto obligan a recurrir a capacidades técnicas avanzadas para reconstruir el flujo de fondos. Incluso en aquellos casos en que se logra avanzar en el análisis, la intervención de múltiples direcciones y redes puede generar rupturas en la cadena de trazabilidad, dificultando la obtención de prueba robusta en sede judicial.

2. Evolución constante del mundo cripto y el avance en su utilización en el marco de delitos complejos

Otra de las principales amenazas para la persecución penal estratégica en materia de criptoactivos radica en la dinámica evolutiva del ecosistema, caracterizado por la aparición constante de nuevas tecnologías, herramientas y modalidades de uso que son rápidamente adoptadas tanto por usuarios legítimos, que utilizan los activos virtuales como medio de ahorro y/o inversión, como por actores delictivos.

El desarrollo del mundo cripto no es estático sino que se encuentra en permanente transformación, incorporando innovaciones como nuevas blockchains, servicios descentralizados (DeFi), tokens, mecanismos de anonimización y plataformas de intercambio con funcionalidades cada vez más complejas. Esta evolución tecnológica impacta directamente en el ámbito de la criminalidad económica, en tanto amplía el abanico de herramientas disponibles para la comisión de delitos y dificulta la adaptación de los sistemas de control e investigación.

En esa línea, el GAFI ha advertido que el rápido crecimiento y la constante innovación en el sector de activos virtuales generan nuevos riesgos y vulnerabilidades, en tanto los actores ilícitos explotan estas innovaciones antes de que los marcos regulatorios y las capacidades institucionales logren adaptarse. A su vez, destaca que la aparición de nuevos productos y servicios, particularmente aquellos que operan de manera descentralizada, puede reducir la efectividad de los mecanismos tradicionales de prevención y detección de operaciones sospechosas (Grupo de Acción Financiera Internacional, 2021).

Desde una perspectiva empírica, esta situación se refleja en la proliferación de nuevas formas de criminalidad vinculadas a criptoactivos. Tal como se ha señalado en el ámbito de las investigaciones forenses, el desarrollo de estas tecnologías genera constantemente

nuevos escenarios propicios para las estafas y el lavado de activos, entre otros delitos.

Ahora bien, esta evolución se verifica claramente en la práctica. Tal como se explicó en puntos anteriores, el análisis de operaciones en blockchain permite reconstruir flujos de fondos, pero exige interpretar cada transacción según el tipo de servicio involucrado (exchange, billetera, procesador de pagos, etcétera). A medida que surgen nuevas plataformas y funcionalidades, también se multiplican las posibles lecturas de una misma operación, incrementando la complejidad investigativa (Oppel, 2022, pp. 94-95).

De este modo, la constante innovación del mundo cripto no sólo incrementa la sofisticación de las maniobras delictivas, sino que también genera un desfase estructural entre la evolución tecnológica y la capacidad de respuesta de los sistemas de investigación, consolidándose así como una amenaza estratégica para los Ministerios Públicos Fiscales.

3. Transnacionalidad

Una de las características propias de los activos virtuales es su capacidad para ser transferidos de manera inmediata y sin intermediarios tradicionales a cualquier parte del mundo, sin necesidad de pasar por sistemas financieros sujetos a controles territoriales. Tal como ha sido señalado por el GAFI, el ecosistema de activos virtuales presenta una naturaleza inherentemente "sin fronteras", lo que facilita la realización de operaciones transfronterizas rápidas y de bajo costo, permitiendo a los actores ilícitos trasladar fondos entre distintas jurisdicciones con el objetivo de evadir controles regulatorios y dificultar su rastreo (Grupo de Acción Financiera Internacional, 2021).

La transnacionalidad no sólo se limita al movimiento de los fondos, sino que también se proyecta sobre los distintos elementos del delito. En una misma maniobra pueden intervenir usuarios ubicados en diferentes países, plataformas de intercambio radicadas en otras jurisdicciones, servidores alojados en territorios diversos y proveedores de servicios sujetos a regulaciones disímiles o, incluso, inexistentes. Esta dispersión geográfica genera una fragmentación de la información relevante para la investigación, dificultando la reconstrucción integral de los hechos.

A ello, se suma la existencia de asimetrías regulatorias entre los distintos Estados. Tal como advierte el GAFI, el grado de implementación de estándares internacionales en materia de activos virtuales es desigual entre jurisdicciones, lo que habilita que los actores delictivos operen estratégicamente desde territorios con menores niveles de supervisión o control, profundizando las dificultades para su detección y persecución (Grupo de Acción Financiera Internacional, 2021, pp. 2-3).

Desde una perspectiva práctica, esta característica impacta directamente en la eficacia de la persecución penal, en tanto obliga a los organismos intervinientes a recurrir a mecanismos de cooperación internacional que, en muchos casos, resultan insuficientes frente a la velocidad de las operaciones en el ecosistema cripto. La necesidad de canalizar pedidos de asistencia jurídica internacional, identificar autoridades competentes en cada jurisdicción y adaptarse a marcos normativos heterogéneos introduce demoras que pueden resultar críticas para el éxito de la investigación.

En suma, la transnacionalidad del delito en el ámbito de los criptoactivos no sólo complejiza la reconstrucción de las maniobras ilícitas, sino que también tensiona los mecanismos tradicionales de cooperación penal, consolidándose como una amenaza estructural que exige respuestas coordinadas a nivel internacional.

2.4. Oportunidades

1. Uso de inteligencia artificial en el análisis de datos y detección de patrones

El avance y adopción de tecnologías basadas en inteligencia artificial (IA) constituye una de las principales oportunidades para fortalecer la persecución penal en materia de criptoactivos, particularmente en lo que respecta al análisis de grandes volúmenes de datos y la detección de patrones complejos asociados a maniobras delictivas.

La integración de sistemas de IA en el ámbito de la seguridad y la justicia penal permite procesar de manera eficiente cantidades masivas de información provenientes de diversas fuentes, tales como registros financieros, transacciones digitales, redes sociales y evidencia electrónica, facilitando la identificación de comportamientos sospechosos, vínculos entre actores y estructuras delictivas (EL PACCTO 2.0., 2024, p. 6).

En tal sentido, herramientas como el aprendizaje automático (machine learning) y el procesamiento de lenguaje natural permiten detectar regularidades, anomalías y patrones ocultos que difícilmente podrían ser advertidos mediante métodos tradicionales de investigación, optimizando la capacidad de los organismos encargados de la persecución penal para reconstruir maniobras complejas, como aquellas vinculadas al lavado de activos mediante criptoactivos.

También, la IA posibilita el desarrollo de modelos predictivos que contribuyen a anticipar conductas delictivas, identificar zonas de riesgo y priorizar recursos investigativos, lo que resulta particularmente relevante en contextos de criminalidad económica y organizada, caracterizados por su dinamismo y sofisticación tecnológica (El PACCTO 2.0, 2024, pp. 10–11).

Desde una perspectiva operativa, la utilización de estas tecnologías no sólo permite mejorar la eficacia de las investigaciones, sino también reducir los tiempos de respuesta y optimizar la asignación de recursos humanos y materiales dentro de los Ministerios Públicos Fiscales, contribuyendo a una persecución penal más estratégica e inteligente.

Por ende, el uso de inteligencia artificial en el análisis de datos y detección de patrones se presenta como una oportunidad clave para fortalecer las capacidades investigativas en materia de criptoactivos, permitiendo abordar con mayor eficacia fenómenos delictivos caracterizados por su complejidad, volumen de información y carácter transnacional.

2. Cooperación interinstitucional e internacional

La cooperación interinstitucional e internacional se configura como una oportunidad estratégica fundamental para fortalecer la persecución penal en materia de criptoactivos, especialmente frente a la naturaleza transnacional y altamente compleja de este tipo de delitos.

Tal como ha sido señalado por el GAFI, la eficacia de los sistemas de prevención y persecución del lavado de activos vinculados a activos virtuales depende en gran medida de la capacidad de los Estados para articular mecanismos de cooperación internacional, intercambio de información y asistencia jurídica mutua (Grupo de Acción Financiera Internacional, 2023, p. 11). En un contexto caracterizado por la circulación transfronteriza de fondos y la dispersión de los elementos

del delito en múltiples jurisdicciones, la actuación aislada de los organismos nacionales resulta insuficiente para abordar de manera eficaz estas problemáticas.

Además, la cooperación no sólo debe proyectarse a nivel internacional, sino también al interior de cada Estado, mediante la articulación entre los distintos organismos que intervienen en la investigación penal, tales como Ministerios Públicos Fiscales, unidades de información financiera, fuerzas de seguridad y organismos reguladores. La coordinación interinstitucional permite integrar distintas fuentes de información, optimizar recursos y evitar la fragmentación de las investigaciones, contribuyendo a una respuesta más eficiente y coherente frente a la criminalidad económica.

Ahora bien, en el ámbito específico de los criptoactivos, la cooperación adquiere una dimensión adicional vinculada a la necesidad de establecer canales de comunicación ágiles y efectivos con actores del sector privado, particularmente con plataformas de intercambio y proveedores de servicios vinculados al ecosistema digital. Así, se ha señalado que la posibilidad de avanzar en la identificación de los usuarios detrás de determinadas operaciones exige no sólo el conocimiento técnico del funcionamiento de estas plataformas, sino también la existencia de mecanismos de requerimiento de información que resulten rápidos y eficaces en términos operativos (Oppel, 2022, p. 77).

De la misma manera, el desarrollo de redes de cooperación internacional resulta clave para agilizar el acceso a información relevante, especialmente en un entorno donde la velocidad de las operaciones con criptoactivos puede tornar ineficaces los canales tradicionales de asistencia jurídica internacional. En este marco, el fortalecimiento de mecanismos de intercambio directo de información, la participación en redes internacionales y la celebración de acuerdos de cooperación específicos aparecen como herramientas indispensables para reducir los tiempos de respuesta y mejorar la trazabilidad de los activos.

Por otra parte, diversos organismos internacionales han impulsado iniciativas orientadas a fomentar la cooperación en materia tecnológica y digital. En el ámbito de la inteligencia artificial, por ejemplo, se han promovido espacios de articulación entre países y regiones con el objetivo de desarrollar infraestructuras digitales seguras,

compartir buenas prácticas y fortalecer las capacidades institucionales para enfrentar el crimen organizado en entornos digitales (El PACCTO 2.0, 2024, pp. 11–12).

Desde una perspectiva estratégica, la cooperación interinstitucional e internacional no sólo permite superar las limitaciones derivadas de la fragmentación jurisdiccional, sino que también potencia el desarrollo de capacidades técnicas, el acceso a herramientas especializadas y la generación de estándares comunes de actuación.

3. Creación y fortalecimiento de fiscalías especializadas

La creación y fortalecimiento de fiscalías especializadas en delitos vinculados a criptoactivos se presenta como una oportunidad estratégica clave para mejorar la eficacia de la persecución penal en este ámbito, en tanto permite consolidar capacidades técnicas, optimizar recursos y desarrollar abordajes investigativos acordes a la complejidad de estos fenómenos.

Tal como se ha abordado a lo largo del texto, estas investigaciones tienen una especificidad técnica sobre contenidos relativos a los activos virtuales, como el funcionamiento de la tecnología blockchain, el análisis de transacciones digitales y la interacción con plataformas tecnológicas. Todo ello exige la intervención de operadores con formación especializada y experiencia acumulada en la materia. Por esto, la institucionalización de unidades fiscales especializadas favorece la concentración de conocimiento, la estandarización de prácticas investigativas y el desarrollo de criterios de actuación más eficientes.

En este punto, la oportunidad no se limita exclusivamente a la creación de nuevas estructuras, sino que también comprende el fortalecimiento de aquellas ya existentes, en línea con las capacidades institucionales previamente identificadas en el análisis de fortalezas. La experiencia acumulada por determinadas unidades especializadas dentro de los Ministerios Públicos Fiscales constituye una base sólida sobre la cual profundizar procesos de capacitación, incorporación de herramientas tecnológicas y desarrollo de protocolos de actuación específicos.

Así, la creación y fortalecimiento de fiscalías especializadas no sólo contribuye a mejorar la eficacia de la persecución penal en materia de criptoactivos, sino que también se erige como un elemento central para

el desarrollo de una política criminal estratégica, orientada a enfrentar fenómenos delictivos cada vez más complejos, dinámicos y tecnológicamente sofisticados.

3. Hacia la formulación de estrategias

Tal como se planteó en la introducción, la creciente complejidad de la criminalidad vinculada a criptoactivos impone a los Ministerios Públicos Fiscales el desafío de repensar sus formas de intervención, avanzando hacia modelos de persecución penal estratégica que permitan dar respuestas eficaces en contextos caracterizados por la innovación tecnológica, la transnacionalidad y la sofisticación de las maniobras delictivas.

A partir del análisis FODA desarrollado, es posible avanzar hacia la formulación de estrategias de persecución penal estratégica orientadas a optimizar la respuesta institucional frente a la criminalidad vinculada a criptoactivos. De allí que la determinación de fortalezas, debilidades, oportunidades y amenazas no constituye un fin en sí mismo, sino que se presenta como un insumo metodológico para el diseño de líneas de acción que permitan articular las capacidades existentes con las condiciones del entorno.

El análisis realizado permite proyectar, de manera preliminar, distintas líneas estratégicas que comprenden, entre otras, el fortalecimiento de las capacidades técnicas y tecnológicas de los organismos de persecución penal, la incorporación de herramientas especializadas para el análisis de criptoactivos, el desarrollo de instancias de capacitación continua para operadores judiciales, así como la consolidación de estructuras organizacionales especializadas que permitan abordar este tipo de fenómenos con mayor eficacia.

Asimismo, se advierte la necesidad de profundizar mecanismos de articulación interinstitucional e internacional, promoviendo el intercambio de información, la cooperación operativa y la generación de redes de trabajo que permitan superar las limitaciones derivadas de la fragmentación jurisdiccional. En este marco, también pueden proyectarse líneas de acción orientadas al establecimiento de canales de comunicación más ágiles con actores del sector privado, particularmente con proveedores de servicios vinculados al ecosistema cripto,

así como al diseño de protocolos de actuación específicos para la investigación de este tipo de delitos.

Del mismo modo, el análisis habilita la formulación de estrategias tendientes a anticipar y enfrentar la evolución constante del fenómeno delictivo, mediante la adopción de enfoques dinámicos, el uso de tecnologías avanzadas, incluyendo inteligencia artificial, y el desarrollo de capacidades institucionales que permitan adaptarse a escenarios cambiantes y de alta complejidad. A su vez, permite identificar la importancia de diseñar respuestas orientadas a mitigar las debilidades estructurales en contextos adversos, especialmente frente a desafíos como el anonimato, la sofisticación de las maniobras y la transnacionalidad del delito.

Estas líneas estratégicas que pueden estructurarse en función de las distintas combinaciones entre fortalezas, debilidades, oportunidades y amenazas, constituyen un punto de partida para el diseño de políticas criminales específicas en la materia, integrando dimensiones tecnológicas, organizacionales y de cooperación institucional.

No obstante, la definición precisa de dichas estrategias, así como su traducción en acciones concretas, indicadores de evaluación y mecanismos de implementación, requiere un desarrollo ulterior que excede el alcance del presente trabajo, quedando abierta como una línea de investigación futura orientada a profundizar el diseño de herramientas de persecución penal estratégica en el ámbito de los criptoactivos.

Bibliografía

Aginsky, A. (2023, 19 de octubre). *Blockchain por y para abogadas y abogados*. SAIJ, Id SAIJ: DACF230111. https://www.saij.gob.ar

EL PACCTO 2.0. (2024). *Inteligencia artificial y crimen organizado*. Unión Europea. Madrid, Unión Europea.

Ernst & Young. (2021). Blockchain Forensic Investigations: Managing Financial Crime Risks in the Cryptocurrency Era.

Gimenez Monti, M. L. y Loyola, G. N. (2025). Análisis de un caso real de estafa vinculada a criptomonedas. Pautas para afrontar las investigaciones judiciales del fenómeno delictivo. En S. R. Narvaja et al. (comps.), *Cuadernos sobre criminalidad económica*, vol. 1. CEI Ediciones.

Grupo de Acción Financiera Internacional. (2020). *Activos virtuales: señales de alerta de lavado de dinero y financiamiento del terrorismo*.
Grupo de Acción Financiera Internacional. (2021). *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*.
Grupo de Acción Financiera Internacional. (2023). *Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers*. FATF.
Ministerio Público Fiscal de la Nación. (2023). *Informe sobre criptoactivos*.
Oppel, S. (2022). "Bitcoin: herramientas de análisis para abordar investigaciones penales que incluyan operaciones con esta cripto-moneda", *Revista de Derecho Penal y Criminología La Ley*, Año 12, Nº 6, julio, Buenos Aires, 2022. http://www.laley.com.ar/
Ponce Talancón, H. (2006). "La matriz FODA: una alternativa para realizar diagnósticos y determinar estrategias de intervención en las organizaciones productivas y sociales", *Contribuciones a la Economía*. https://eco.mdp.edu.ar/cendocu/repositorio/00290.pdf
Silva, G., Feser, M. E., Santos, M. y Ferreiro, J. (2023). "Criptomonedas y delitos complejos: hacia una nueva perspectiva de su impacto en la investigación criminal", *Minerva*, *2* (6). https://ojs.editorialiupfa.com/index.php/minerva/article/view/118

Normativa

Ley 25.246. (2000, 10 de mayo). Boletín Oficial de la República Argentina.
Ley 27.739. (2024, 15 de marzo). Modificatoria de la Ley 25.246. Boletín Oficial de la República Argentina.

Regulación de los PSAV en Argentina: avances formales y desafíos

María Alejandra Freire[1]

Resumen

El presente trabajo analiza el régimen jurídico aplicable a los Proveedores de Servicios de Activos Virtuales (PSAV) en Argentina a partir de la sanción de la Ley 27.739 y su reglamentación por la Comisión Nacional de Valores y la Unidad de Información Financiera, en el período 2024-2026. El trabajo examina el alcance de la normativa, las principales obligaciones impuestas y los desafíos que presenta su implementación en materia de prevención del lavado de activos, financiamiento del terrorismo y proliferación de armas de destrucción masiva. Se sostiene que, si bien la regulación actual constituye un avance en términos de adecuación a estándares internacionales, su eficacia se ve limitada por deficiencias estructurales, entre las que se destacan la falta de coordinación interinstitucional, las dificultades para regular a los actores que operan desde el exterior y los problemas operativos vinculados a la aplicación de herramientas tecnológicas en un entorno dinámico y transnacional. Por lo cual, se propone una

1- Magister en Finanzas egresada de la UCEMA, abogada de formación de grado, egresada de la Universidad de Buenos Aires. Forma parte del equipo de Honisch & Asociados. Cuenta con 20 años de experiencia en compliance, anticorrupción, lavado de activos y regulación bancaria. Ha ocupado diversos cargos en áreas de gestión del sector público nacional. Ha participado de diversas publicaciones. Es docente en el IUPFA y de la Maestría en Finanzas en la UNSAM. Forma parte del equipo de investigación del Proyecto CRIPTO ACRE (UNR 2024-2027) e integra el equipo de tutores en la Especialización en delitos económicos y lavado de activos en esa casa de estudios. Es tallerista en el Proyecto Escuelas y Bitcoin y socia activa de la ONG Bitcoin Argentina. Es parte del Centro de Investigación y Prevención de la Criminalidad Económica (CIPCE). Coordinadora Argentina de Amassuru y miembro de Women in Compliance. Correo: freirealejandra09@gmail.com

lectura crítica que pone en foco de análisis la adecuación normativa con la efectividad real del sistema, señalando los principales desafíos regulatorios pendientes.

1. Introducción

En los últimos años, el crecimiento del ecosistema de criptoactivos[2] ha planteado grandes desafíos para los sistemas regulatorios a nivel global[3], especialmente en materia de prevención y persecución de lavado de activos, financiamiento del terrorismo y financiamiento de armas de proliferación masiva.

Zocaro (2020) sostiene en ese sentido que se observan problemas normativos en la mayoría de los países en relación a la regulación de los criptoactivos y que es un problema compartido a nivel mundial el potencial uso que tienen para realizar maniobras de evasión de impuestos, lavado de activos o financiamiento de actividades ilícitas.

Las características propias de estas representaciones de valor como la descentralización y cierto grado de pseudoanonimato, han generado nuevas oportunidades para que organizaciones criminales

2- El Grupo de Acción Financiera Internacional (GAFI) define a los criptoactivos como toda representación digital de valor que se puede intercambiar, o transferir o ser utilizada como medio de pago en forma digital. Asimismo, aclara que no es un criptoactivo la representación digital de las monedas fiduciarias. Véase https://www.fatf-gafi.org/en/topics/virtual-assets.html

3- Según el informe 2025 de la Fundación Blockchain Argentina, nuestro país desde el año 2024 se encuentra en el primer puesto de los países latinoamericanos que han adoptado el uso de criptomonedas y se encuentra en el puesto 20 a nivel mundial. Si bien el informe no analiza los riesgos de las plataformas de ser usadas para lavar activos o ser vehículos utilizados por organizaciones criminales para realizar operaciones vinculadas a flujos ilícitos financieros, sí hace referencia al conocido caso Libra y el aumento de las consultas de usuarios a diferentes plataformas en temas relacionados a la seguridad, custodia y requisitos regulatorios. Ver https://fundacionblockchain.com/argentina-lidera-la-adopcion-cripto-en-latinoamerica-y-consolida-su-crecimiento-informe-2025/ Por otro lado, el informe 2025 de TRM menciona que entre los años 2024 y 2025 las sanciones a plataformas de criptomonedas produjo un cambio en la utilización ilícita de las mismas, observándose el aumento de la utilización de activos digitales que no son stablecoins, esto es criptomonedas que mantienen su valor anclado al valor de otro activo, ya sea virtual, fiduciario o producto, etc., y se redujeron un 60% las sanciones vinculadas al uso ilícito de stablecoins. Así los desafíos regulatorios se dan en torno al aumento del uso de criptomonedas en la economía lo que permite un escenario más amplio para ocultar maniobras ilícitas, la expansión de las finanzas descentralizas y el rápido y constante avance de la tecnología que impone la necesidad de contar con regulaciones dinámicas que puedan adaptarse a los cambios repentinos del ecosistema.

canalicen flujos financieros ilícitos, desafiando los marcos normativos existentes en diferentes jurisdicciones que fueron diseñados para el sistema financiero tradicional y por lo tanto generando la necesidad de regulación propia del campo de los criptoactivos.

En este contexto, el Grupo de Acción Financiera Internacional (GAFI) ha identificado riesgos relacionados a las operaciones con activos virtuales e impulsado la incorporación de estándares orientados a la regulación de los denominados Proveedores de Servicios de Activos Virtuales (PSAV), promoviendo su registro, supervisión y el cumplimiento de obligaciones de debida diligencia y reporte de operaciones sospechosas, entre otras.[4]

Por otro lado, desde el año 2021 el GAFI publica informes sobre la implementación de la Recomendación 15, la última actualización corresponde a mediados del año 2025 en la que se afirma que los activos virtuales son transfronterizos por definición y por lo tanto al existir deficiencias regulatorias en una jurisdicción es posible que esas fallas tengan consecuencias globales, de ahí la necesidad de generar instancias de coordinación y cooperación entre los distintos países[5].

En ese último informe se destacan como principales riesgos identificados en la utilización de operaciones criminales: a) el uso de las stablecoins, sobre todo el aumento de su utilización, (con las salvedades mencionadas en la nota 1 por el aumento de las sanciones relacionadas a uso en el ámbito criminal); b) la utilización de activos virtuales en fraudes y estafas; y c) la implementación desigual de los miembros del GAFI, en especial las Recomendaciones 15 y 16.

Por su parte, la evaluación de riesgos sectorial realizada por GAFILAT en 2025, señala como principales riesgos: a) riesgo alto de la utilización para el lavado de activos de hechos que involucran fraude, estafas, los ataques cibernéticos, el tráfico de drogas, trata de personas, evasión y corrupción, y b) riesgo medio de la utilización de activos virtuales para la financiación del terrorismo[6].

En lo que respecta a nuestro país, las últimas evaluaciones de riesgos de lavado de activos y financiamiento del terrorismo no incorporaron el análisis sobre la utilización de activos virtuales[7]. Tampoco se han

4- GAFI, Updated Guidance for a Risk-Based Approach to Virtual Assets and VASPs, 2021.
5- El informe completo se puede consultar en https://www.fatf-gafi.org/en/topics/virtual-assets.html
6- El informe completo se puede consultar en https://biblioteca.gafilat.org/?cat=9
7- Las evaluaciones se pueden consultar en http://www.bibliotecadigital.gob.ar/items/show/2771

identificado informes específicos realizados por organismos estatales. Sin embargo, en los últimos años se ha observado un aumento de la utilización de instrumentos del ecosistema cripto en diferentes maniobras delictivas[8], situación que puso en alerta a distintos organismos estatales[9].

En ese sentido, Argentina en el marco de la cuarta ronda de evaluación mutua del GAFI, encontró un impulso importante para avanzar en la regulación mediante la incorporación de los lineamientos del GAFI a través de la sanción de la Ley 27.739 en marzo del año 2024[10], así como también en su rápida reglamentación por parte de la Comisión Nacional de Valores (CNV) y de la Unidad de Información Financiera (UIF).

Así, el presente trabajo tiene por objeto analizar el marco jurídico aplicable a los PSAV en Argentina entre los años 2024 y 2026, con el fin de evaluar su alcance, principales obligaciones y los desafíos que presenta su implementación en la dimensión operativa y regulatoria, especialmente en materia de prevención del lavado de activos, financiamiento del terrorismo y proliferación de armas de destrucción masiva.

Como hipótesis de trabajo, se sostiene que, si bien el régimen de los PSAV representa un avance significativo en términos de adecuación normativa a los estándares del GAFI, su diseño e implementación presentan deficiencias estructurales en materia de coordinación entre los organismos reguladores, la supervisión de sujetos internacionales y la operatividad de las herramientas de control. Ello compromete su eficacia como mecanismo de mitigación de riesgos y pone en cuestión su capacidad real de prevención en contextos de alta complejidad y transnacionalidad como los que representa el ecosistema de criptoactivos.

El presente trabajo se estructura en cuatro apartados. En primer lugar, se realiza una breve reconstrucción del desarrollo normativo de los criptoactivos en Argentina. En segundo término, se analiza la

8- No vamos a ahondar en la casuística ya que ese análisis excede el objeto de investigación. Para analizar diferentes casos relacionados al ecosistema cripto se puede consultar el sitio www.fiscales.gob.ar.

9- Desde la conformación de mesas de trabajo entre actores nacionales, internacionales, capacitaciones, regulaciones internas de los organismos competentes, colaboraciones de actores privados, uso de tecnología, etc.

10- Véase https://servicios.infoleg.gob.ar/infolegInternet/anexos/395000-399999/397355/norma.htm

incorporación de los PSAV al sistema de prevención de lavado de activos. Seguidamente, se examina la implementación del régimen a partir de la actuación de los organismos reguladores. En cuarto lugar, se identifican las principales tensiones y deficiencias del sistema. Finalmente, se realiza una reflexión en torno a los desafíos regulatorios pendientes.

2. Marco normativo de los activos virtuales en Argentina

2.1. Antecedentes de la sanción de la Ley 27.739

El desarrollo normativo de los criptoactivos en Argentina previo a la sanción de la Ley 27.739 se caracterizó por un enfoque parcial y reactivo, en el que distintos organismos del estado intervinieron de forma aislada en la emisión de normas destinadas a recolectar información, mitigar riesgos, establecer algunas pautas de actuación, pero sin la existencia de un marco regulatorio integral.

En ese sentido, la Unidad de Información Financiera (UIF) incorporó tempranamente a las monedas virtuales dentro del esquema de prevención mediante la Resolución 300/2014[11], en la que estableció obligaciones de reporte sistemático de operaciones para determinados sujetos obligados. Esta medida, si bien constituyó un antecedente relevante en términos de reconocimiento del fenómeno desde la perspectiva antilavado, tuvo un alcance limitado, ya que no implicó la regulación de los actores que operan en el ecosistema de criptoactivos ni pautas específicas de debida diligencia. Sin embargo, cabe destacar que en el año 2014 recién se estaba planteando por parte del GAFI en forma pública el riesgo que podrían implicar las operaciones con esos instrumentos y no había regulación en otros países en ese sentido, por lo cual la rápida respuesta de la UIF ante el planteamiento de la necesidad de observar ese incipiente y desconocido fenómeno fue muy significativa ya que permitió contar en forma temprana con herramientas iniciales de recolección de información para el monitoreo del sistema.

11- La resolución se puede consultar en https://servicios.infoleg.gob.ar/infolegInternet/anexos/230000-234999/231930/norma.htm

En relación con las acciones impuestas por otros organismos reguladores, el Banco Central de la República Argentina (BCRA) se limitó a emitir comunicados en los que advertía sobre los riesgos asociados a su utilización, tales como su volatilidad, la ausencia de respaldo estatal y la falta de garantías para los usuarios. Posteriormente, avanzó en la imposición de restricciones indirectas, como la prohibición a las entidades financieras de ofrecer o facilitar operaciones con activos virtuales que no se encuentren autorizados por una autoridad competente[12]. Asimismo, de acuerdo a lo manifestado por el propio BCRA en su página web está realizando tareas de monitoreo a los efectos de avanzar en entender cuáles son los riesgos e implicancias que configuran las operaciones en las que se utilizan criptoactivos en nuestro país[13].

Por su parte, en esa primera etapa y con anterioridad a la sanción de la Ley 27.739, la Comisión Nacional de Valores (CNV) siguió las acciones del BCRA, en ese sentido emitió comunicaciones públicas incluso conjuntamente con el BCRA, en las que se realizaron advertencias al público inversor respecto de los riesgos asociados a determinados instrumentos vinculados a criptoactivos, como por ejemplo las ofertas iniciales de monedas (ICO), sin avanzar en una regulación sistemática del sector[14].

Por último, cabe mencionar que la Agencia de Recaudación y Control Aduanero (ARCA) avanzó en la incorporación de los criptoactivos dentro de los regímenes de información y en su tratamiento impositivo, particularmente en el impuesto a las ganancias y en el impuesto sobre los bienes personales, pero sin integrarse en una estrategia regulatoria más amplia en materia financiera o de prevención de lavado de activos[15].

12- Todas las acciones del BCRA en ese sentido se encuentran disponibles en https://www.bcra.gob.ar/criptoactivos/

13- No se observan publicaciones actualizadas dentro del sitio web. Ver https://www.bcra.gob.ar/criptoactivos/

14- Las comunicaciones se pueden consultar en https://www.argentina.gob.ar/noticias/alerta-del-bcra-y-la-cnv-sobre-los-riesgos-e-implicancias-de-los-criptoactivos

15- Específicamente se han regulado a través de la Ley de impuesto a las ganancias, bienes personales (ARCA en el Dictamen N° 2/2022 DI ALIR expresó que los criptoactivos se encuentran gravados en el Impuesto sobre los Bienes Personales de acuerdo a lo previsto en el inciso j) del artículo 19 de la Ley N° 23.966) y Régimen de información RG 4614/2019 y modificatorias RG 5804/2025. Los textos y novedades en materia tributaria se pueden ver en https://www.afip.gob.ar/economia-digital/

De este modo, se observa que la intervención de los distintos organismos se desarrolló de manera parcial y desarticulada, generando un escenario caracterizado por la superposición de competencias ya que cada organismo avanzó en la regulación sin criterios uniformes ni un objetivo claro y preciso.

En este contexto, la regulación de los criptoactivos en Argentina previo a la sanción de la Ley 27.739 puede ser entendida como un conjunto de respuestas dispersas frente a un fenómeno en expansión no solo en Argentina sino a nivel global, en el que predominó la lógica de mitigación de riesgos específicos por sobre el diseño e implementación de un régimen integral.

Esa situación marcó la necesidad de avanzar hacia una regulación que permitiera no solo ordenar las competencias de cada uno de los organismos de control, sino también incorporar estándares internacionales en materia de prevención del lavado de activos y financiamiento del terrorismo a los efectos de cumplir con los estándares del GAFI, y asimismo aprobar la evaluación mutua en curso en la que se encontraba Argentina.

2.2. Incorporación de los PSAV al sistema de prevención del lavado de activos

La sanción de la Ley 27.739 en marzo del año 2024 marcó un punto de inflexión en la regulación de los criptoactivos en Argentina, al introducir por primera vez un marco normativo específico orientado a su tratamiento dentro del sistema de prevención del lavado de activos, financiamiento del terrorismo y de la proliferación de armas de destrucción masiva[16]. Fue así que en línea con los estándares internacionales impulsados por el GAFI[17] incorporó definiciones, sujetos y obligaciones que permiten estructurar un régimen más sistemático e integral.

16- El delito de financiamiento de la proliferación de armas de destrucción masiva fue incorporado por la Ley 27.739 en el artículo 306 del Código Penal.

17- En la versión taquigráfica de la segunda reunión de la primera sesión pública especial del período 142 de la Honorable Cámara de Senadores en la que se trató el proyecto se hace mención a que esta ley viene a dar cumplimiento a los estándares del GAFI mientras Argentina se encontraba en la etapa de evaluación mutua. Véase https://www.senado.gob.ar/parlamentario/sesiones/busquedaTac

En este sentido, uno de los avances centrales de la ley radica en la incorporación de una definición legal de activos virtuales[18], entendidos como representaciones digitales de valor que pueden ser comercializadas o transferidas digitalmente y utilizadas como medio de pago o inversión, excluyendo expresamente a la moneda de curso legal.

Asimismo, la norma introduce la categoría de Proveedores de Servicios de Activos Virtuales, la cual siguiendo al GAFI fue definida como aquellas personas humanas o jurídicas que, de manera habitual y profesional, realizan actividades u operaciones con activos virtuales por cuenta propia o de terceros, tales como el intercambio entre activos virtuales y monedas fiduciarias, la transferencia, custodia o administración de dichos activos, o la provisión de servicios financieros vinculados a su emisión.

En ese sentido, la incorporación de esta figura, en cumplimiento de lo dispuesto en la Recomendación 15 del GAFI[19], permite, en principio, identificar a los actores que operan en el ecosistema y someterlos a un régimen específico de obligaciones.

Es así que al ser incorporados como sujetos obligados los PSAV deben cumplir entre otras obligaciones, las de inscripción en organismos reguladores, reporte de operaciones, cumplimiento de deberes de debida diligencia, y de políticas de prevención acordes a los riesgos asociados a su actividad.

Por otro lado, se produce un desplazamiento desde un enfoque en una primera etapa, basado en la recolección de información y conocimiento del sistema que se encontraba centrado en la UIF, hacia un enfoque basado en riesgos. En esta nueva etapa los PSAV adquieren un rol activo en la detección y mitigación de operaciones sospechosas y empiezan a tener una mirada desde diferentes organismos reguladores.

Por otra parte, la ley asigna a la CNV la obligación de creación y administración de un registro específico de PSAV, así como el ejercicio de facultades de supervisión, fiscalización y sanción sobre estos sujetos.

18- Si bien se había tomado la definición de activos virtuales del GAFI en la Resolución 300/2014 de la UIF, no se encontraba hasta ese momento en un texto aprobado por el H. Congreso de la Nación. Esta definición, alineada con los criterios desarrollados por el GAFI, permite delimitar el objeto de regulación y establecer un punto de partida común para la actuación de los distintos organismos competentes.

19- Ver https://biblioteca.gafilat.org/?p=7500

Esta decisión implica un reconocimiento de la necesidad de contar con una autoridad especializada que concentre la información y supervise el funcionamiento del sector, siguiendo los lineamientos del GAFI.

En términos generales, la incorporación de los PSAV al sistema de prevención del lavado de activos representa un avance significativo en la estructuración de un marco normativo más integral y alineado con los estándares internacionales. Sin embargo, como se analizará en los apartados siguientes, la efectividad de este régimen no depende únicamente de su diseño formal, sino también de las condiciones de su implementación y de la articulación entre los distintos organismos a los que se han asignado funciones y competencias específicas.

3. Implementación de la normativa sobre PSAV

La implementación del régimen aplicable a los PSAV en Argentina, como se mencionó, se dio en el marco de la evaluación del GAFI en la cuarta ronda, en la que los organismos competentes como la CNV y la UIF debieron dictar rápidamente las reglamentaciones a las que se encontraban obligadas de acuerdo a sus funciones a los efectos de hacer operativos los cambios introducidos por la Ley 27.739.

3.1. Registro de PSAV y supervisión por la Comisión Nacional de Valores

Los estándares del GAFI en su Recomendación 15 establecen que los PSAV deben integrarse en un sistema de licencia o registro y ser monitoreados en sus actividades. El sistema de otorgamiento de licencias es por definición más amplio que el registro, ya que implica como mínimo otorgar un permiso en base al análisis de información sobre el sujeto a analizar, y en el registro se valida la existencia del sujeto en base al cumplimiento de la integración de cierta información solicitada, por lo que podría pensarse como en un paso previo a la licencia.

En ese entendimiento es que la Ley 27.739[20] estableció el sistema de registro[21]. Cabe destacar que la ley fue sancionada el 15 de marzo de 2024 y que la Resolución General CNV 944/2024[22] por la cual se crea el Registro de Proveedores de Servicios de Activos Virtuales es de fecha 20 de marzo.

El fundamento de la celeridad en emitir la reglamentación la encontramos en los propios considerandos de esa resolución en la que se menciona que el GAFI se encontraba realizando la evaluación de Argentina en el marco del cual se iban a analizar técnicamente la existencia de leyes en materia de prevención de lavado de activos, así como las facultades y procedimientos de las autoridades competentes o reguladores correspondientes. Al ser analizada técnicamente no se requería su implementación efectiva, al menos en esa instancia de la evaluación, y por lo tanto se cumpliría con el GAFI con contar con la reglamentación aprobada. Esa situación explica las deficiencias que se identificaron en su implementación sobre todo en relación a la coordinación de los registros con la UIF.

La CNV estableció como requisitos que los PSAV deberían inscribirse en el registro las personas humanas y jurídicas que fueran residentes o fueran constituidas en Argentina y que lleven adelante alguna de las actividades de PSAV antes de realizar esas operaciones. La excepción estaba dada por aquellos sujetos que no superen las 35.000 UVAS por operaciones mensuales[23]. Por otro lado, respecto de los PSAV que ya estaban operando, debían solicitar la inscripción dentro de los 45 días de entrada en vigencia de la Resolución de CNV.

20- Véase el artículo 37 de la Ley 27.739 en el que se establece que la CNV es la autoridad de aplicación de los PSAV y que en ese marco debe reunir información adecuada, precisa y actualizada y ejercer las facultades de supervisión, regulación, inspección, fiscalización y sanción que se encuentran establecidas en el artículo 19 de la Ley de Mercado de Capitales N° 26.831.

21- Decidida la modalidad de aplicación entre licencia y registro, también existió el debate sobre cuál sería la autoridad competente, si la CNV o el BCRA. Ese debate quedó plasmado en la versión taquigráfica de la segunda reunión de la primera sesión pública especial del período 142 de la Honorable Cámara de Senadores. Ver https://www.senado.gob.ar/parlamentario/sesiones/busquedaTac

22- La norma completa se puede consultar en https://servicios.infoleg.gob.ar/infolegInternet/anexos/395000-399999/397598/norma.htm

23- La norma establece que sobre las personas residentes o constituidas fuera de Argentina, se va a entender que operan en el país cuando el dominio que utilicen sea .ar, cuando tengan acuerdos comerciales por los cuales se reciban fondos de residentes argentinos para realizar operaciones, cuando sus principales usuarios sean residentes en Argentina, cuando la publicidad esté destinada a residentes, y/o cuando el 20% de sus operaciones sean en nuestro país.

Ahora bien, entre la información solicitada para la inscripción se permite contar con la clave de identificación (CDI) otorgada por ARCA, lo cual en principio no sería un problema a los efectos de la registración en la CNV. Sin embargo, tuvo implicancias prácticas ya que se contrapuso con la obligación de inscripción que estos sujetos debían cumplir ante la UIF, ya que el sistema de ese organismo no permitía en un primer momento la inscripción con CDI, razón por la cual el registro de los PSAV extranjeros que no contaban con CUIT se demoró en la UIF y con él la integración de la información y el cumplimiento de su obligación de reportes.

El 12 de marzo de 2025, un año después, se realizó una modificación a la reglamentación por Resolución General CNV 1058/2025[24]. Esa modificación implicó que la excepción de registro fuera únicamente para las personas humanas, y se incorporaron reglas para integrar los órganos de control y fiscalización, requisitos sobre patrimonio neto mínimo de acuerdo a las distintas categorías definidas en esa normativa que pueden tener los PSAV, requisitos sobre normativa interna, compliance, gestión de riesgos, sistemas de información, entre otros, todos los cuales robustecen la aplicabilidad de los estándares internacionales.

El registro completo se puede consultar en la página web de la CNV[25] en el que se puede acceder a los datos de identificación de los sujetos inscriptos.

El sistema de registro establece como novedad un mecanismo de control con anterioridad al inicio de las operaciones en Argentina y realizar tareas de supervisión con posterioridad y por lo tanto su eficacia va a depender en gran parte de la capacidad del organismo para detectar PSAV no registrados y de la coordinación con otras jurisdicciones en casos de prestación de servicios desde el exterior.

La Comisión Nacional de Valores (2025) en su informe de gestión muestra la participación del organismo en gran cantidad de eventos y congresos nacionales e internacionales en el que se ha explicado el sistema implementado en Argentina y su evolución en el marco de sus competencias sin realizar una evaluación sobre su implementación[26].

24- El texto de la norma se puede consultar en https://servicios.infoleg.gob.ar/infolegInternet/anexos/410000-414999/410635/norma.htm

25- Para consultar el registro ingresar a https://www.cnv.gov.ar/SitioWeb/ProveedoresServiciosActivosVirtuales/RegistrosPSAV. Al 9 de abril de 2026 se encuentran inscriptos 163 PSAV que son personas jurídicas, de los cuales 14 tienen identificación extranjera.

26- Los PSAV registrados se pueden consultar online en la página web de la CNV.

3.2. Obligaciones de prevención y supervisión por la Unidad de Información Financiera

La reglamentación por parte de la UIF también se diseñó y aprobó a pocos días de la sanción de la Ley 27.739, así el 22 de marzo de 2024 se sancionó la Resolución 49/2024[27] por la cual se establecieron los requisitos normativos y operativos que deben cumplir los PSAV en nuestro país en materia de prevención de lavado de activos, financiamiento del terrorismo y de armas de destrucción masiva.

El elemento más significativo sin dudas que se incorporó fue la denominada regla de viaje en el artículo 37 de la Resolución 49[28]. Esto significa que los sujetos obligados deben cumplir con la identificación de quien realiza la operación y del beneficiario de las transacciones realizadas.

En ese sentido, el mayor desafío tanto por parte de los sujetos obligados como por la UIF se encuentra en torno al desarrollo y la puesta en marcha de todo el sistema antilavado conjuntamente con los requisitos tecnológicos, los costos asociados al cumplimiento y la adaptación a un entorno caracterizado por su rápida evolución.

Bensousan (2024) respecto de la regla de viaje menciona que si bien no se ha establecido la forma en que se enviará y validará la información, la exigencia de los reportes mensuales que deberán cumplir los PSAV requieren identificar a los participantes de las operatorias y país de origen y destino de las transacciones. Ello, ya que las transferencias de activos virtuales se encuentran expuestas a riesgos de lavado de activos y financiamiento del terrorismo y proliferación de armas de destrucción masiva al igual que las transferencias en el sistema financiero tradicional por lo que en definitiva lo que se pretende es posibilitar el seguimiento y bloqueo de transacciones sospechosas de activos virtuales.

27- La norma se puede consultar en https://servicios.infoleg.gob.ar/infolegInternet/anexos/395000-399999/397597/norma.htm

28- Las demás exigencias se encuentran alineadas a las especificaciones solicitadas para todos los sujetos obligados: la Unidad de Información Financiera (UIF) reglamentó las obligaciones específicas en materia de prevención del lavado de activos y financiamiento del terrorismo aplicables a los PSAV, incorporándolos como sujetos obligados dentro de su ámbito de control. En este marco, se establecen deberes de debida diligencia, identificación y conocimiento del cliente, monitoreo de operaciones, conservación de documentación y reporte de operaciones sospechosas.

Asimismo, hace referencia a posibles implicancias que se deben tener en cuenta en el marco del funcionamiento del ecosistema, como por ejemplo que la falta de instrumentación de la regla de viaje puede traer aparejado que los PSAV que operen en mercados globales y con mayor capacidad operativa y económica, sean requeridos del cumplimiento de contar con sistemas de trazabilidad y en el caso de no tener instrumentados los mismos puedan provocar el bloqueo de pagos o restricción de operaciones con empresas argentinas (Bensousan, 2024).

Por otro lado, la UIF no hace mención de la incorporación como sujetos obligados ante ese organismo de los proveedores de servicios de activos virtuales en su informe de gestión, ni en informes sectoriales, por lo cual no se ha podido analizar la progresiva implementación y la evaluación de las obligaciones establecidas en la Resolución 49 por parte de ese organismo regulador.

En cuanto a las supervisiones a cargo de la CNV y la UIF sobre los PSAV, no es posible profundizar en el presente análisis ya que no se cuenta con información disponible por parte de esos organismos de control competentes[29].

Si bien en materia normativa la evolución regulatoria ha sido mayor en el ámbito de la CNV, no se observa en ninguno de los organismos la existencia de una evaluación de eficacia respecto de la prevención de la utilización de PSAV en maniobras de lavado de activos, financiamiento del terrorismo y de las armas de destrucción masiva.

3.3. Herramientas operativas y desafíos de implementación

De lo expuesto en los apartados anteriores, surge que entre los principales instrumentos previstos para la implementación del régimen se destacan aquellos orientados a la trazabilidad de las operaciones con activos virtuales, en particular la denominada regla de viaje.

Sin embargo, la aplicación efectiva de estos mecanismos presenta dificultades significativas. Por un lado, requiere el desarrollo e implementación de soluciones tecnológicas y el intercambio de información entre distintos proveedores y ello necesita del desarrollo de protocolos

29- De un relevamiento sobre supervisiones realizadas solo se encontró la mención sobre un procedimiento realizado en la ciudad de Rosario a fines del año 2024 en forma conjunta entre la UIF y la CNV, sin indicar mayores precisiones. Ver https://www.argentina.gob.ar/noticias/rosario-procedimiento-de-supervision-proveedores-de-servicios-de-activos-virtuales

comunes y sistemas compatibles, lo que implica costos elevados y desafíos de interoperabilidad entre los sujetos obligados.

En el ámbito de los criptoactivos, estas tareas presentan un grado de complejidad superior al del sistema financiero tradicional, debido a la utilización de direcciones alfanuméricas, la posibilidad de operar sin intermediarios, la existencia de mecanismos que incrementan el anonimato o dificultan el rastreo de fondos entre otros.

Esta situación puede generar que PSAV con menor capacidad operativa y financiera queden por fuera de la supervisión de los organismos de control porque al no prever en un futuro cercano el cumplimiento de las obligaciones exigidas por la reglamentación evalúen la no registración. Por otro lado, se podría dar la situación de que se consolide una estructura de mercado en la que los PSAV con mayor capacidad económica puedan cumplir adecuadamente con las exigencias regulatorias, más allá de las posibles consecuencias económicas que se mencionaron con anterioridad.

Por otra parte, la naturaleza descentralizada y transnacional de los criptoactivos limita la capacidad de control de los organismos de control competentes en el ámbito nacional, especialmente cuando las operaciones involucran actores que se encuentran radicados en jurisdicciones con estándares regulatorios diferentes y que requiere de medidas de coordinación y cooperación establecidas y fluidas.

En este contexto, si bien el régimen implementado introduce herramientas relevantes desde el punto de vista formal, su eficacia práctica se encuentra condicionada por factores técnicos, operativos e institucionales que inciden directamente en su capacidad para prevenir y detectar operaciones vinculadas a actividades ilícitas.

Por otra parte, la rápida evolución tecnológica del sector genera una dinámica en la que las herramientas regulatorias pueden quedar rápidamente desactualizadas. Por otro lado, el surgimiento o el diseño de nuevos modelos de negocios, plantea interrogantes constantes sobre la aplicabilidad de los esquemas tradicionales de supervisión y control que no pueden ser los mismos que los utilizados para el sistema financiero tradicional, ni adaptarse los marcos normativos existentes, sino que requieren como mínimo de capacidad técnica, desarrollo de sistemas y colaboración con otros organismos.

En ese sentido, las dificultades operativas mencionadas no solo afectan a los sujetos obligados, sino también a los propios organismos

regulatorios, ya que se requiere que los recursos con los que cuentan para supervisar a los PSAV puedan adaptarse rápidamente a los cambios que se producen constantemente en ese sector altamente dinámico y especializado.

Es así que la brecha entre el diseño normativo y las condiciones reales de su implementación, teniendo en cuenta que los recursos estatales para llevar adelante esas tareas son siempre escasos, se configura como un factor determinante en la evaluación de la eficacia de su implementación, ya sea por parte de los propios organismos en miras de identificar oportunidades de mejora continua en el sistema antilavado o por parte del GAFI en el marco de la próxima evaluación de Argentina.

4. Tensiones y deficiencias del sistema

4.1. Falta de coordinación interinstitucional: tensiones entre la CNV y la UIF

Uno de los principales desafíos que presenta la implementación del régimen aplicable a los PSAV en Argentina radica en la articulación entre la CNV y la UIF. Si bien la distribución de funciones entre ambas entidades responde, en términos formales, a la lógica de sus respectivas competencias, en la práctica se advierten posibles superposiciones, vacíos y tensiones que afectan la coherencia del sistema.

En ese sentido, la CNV asume un rol central en la registración y supervisión de los PSAV, estableciendo requisitos de inscripción, condiciones operativas y facultades de fiscalización. Por su parte, la UIF regula las obligaciones en materia de prevención del lavado de activos, imponiendo deberes de debida diligencia, monitoreo y reporte de operaciones sospechosas. Sin embargo, si bien esta división podría resultar complementaria, la ausencia de mecanismos claros de coordinación y cooperación genera incertidumbre respecto del alcance de las obligaciones y de los criterios de supervisión aplicables.

Esta situación se manifiesta, en primer lugar y haciendo la salvedad de que no se da solamente en el marco de la regulación de los PSAV y requiere un debate mucho más amplio, en la coexistencia de requerimientos regulatorios que derivan en cargas de presentaciones

superpuestas y en la necesidad de interpretar requerimientos que no siempre presentan un grado adecuado de coherencia interna, como ser la presentación de documentación estatutaria, o las exigencias de políticas y procedimientos internos.

En segundo lugar, la ausencia de una estrategia coordinada de supervisión limita la eficacia del control estatal. La información recabada por la CNV en el marco del registro y fiscalización de los PSAV no necesariamente se integra de manera sistemática con los mecanismos de análisis y detección de operaciones sospechosas de la UIF. Esta fragmentación puede generar zonas de opacidad en las que se debilita la capacidad de identificar riesgos y detectar posibles maniobras de lavado de activos, especialmente en un entorno caracterizado por la velocidad y complejidad de las transacciones digitales.

Asimismo, la falta de coordinación plantea interrogantes en materia sancionatoria, en tanto no siempre resulta claro cómo se articulan las facultades de ambos organismos frente a un mismo incumplimiento.

Así, si bien el diseño institucional del régimen de PSAV en Argentina refleja un intento de adaptar las estructuras existentes a las nuevas exigencias del ecosistema digital y al cumplimiento de los estándares internacionales, analizar la eficacia del sistema requiere no solo atender a su adecuación normativa, sino también examinar las condiciones reales de su implementación, la articulación entre los organismos competentes y la capacidad operativa de supervisión.

4.2. Problemas en la regulación de PSAV extranjeros

Uno de los aspectos más problemáticos se vincula con la regulación de aquellos actores que operan desde el exterior.

En términos formales, la normativa vigente establece la obligación de inscripción en el registro de PSAV para aquellos sujetos que desarrollen actividades en el país. Sin embargo, la aplicación de este criterio presenta dificultades cuando se trata de plataformas radicadas en el extranjero que, sin contar con presencia física en Argentina, prestan servicios a residentes locales. En estos casos, la determinación de la jurisdicción aplicable y la exigibilidad de obligaciones regulatorias puede dar lugar a la utilización de maniobras para eludir esas obligaciones.

En ese sentido, a diferencia de los PSAV radicados en Argentina, los proveedores extranjeros operan, en muchos casos, fuera del alcance efectivo de las autoridades competentes, en este caso de Argentina,

lo que limita la capacidad de identificar posibles incumplimientos al registro y por lo tanto su control y supervisión.

En este contexto, se configura una asimetría regulatoria en su aplicación práctica entre los proveedores argentinos y los extranjeros que no son residentes. Por lo expuesto, la regulación de los PSAV extranjeros constituye uno de los puntos críticos del régimen antilavado que necesariamente requiere avanzar hacia esquemas de cooperación y coordinación internacional consolidados.

El GAFI (2026) recientemente publicó un informe sobre los PSAV offshore, o sea aquellos creados bajo las leyes de una jurisdicción, con o sin presencia física, que prestan servicios a clientes residentes en otra jurisdicción. El informe analiza cómo se estructuran las actividades de estos PSAV para evitar o eludir las obligaciones regulatorias y cómo esas vulnerabilidades son aprovechadas a su vez por quienes llevan adelante maniobras ilícitas.

De acuerdo al relevamiento realizado por el GAFI, el 46% de sus miembros han implementado normas de cumplimiento de los PSAV independientemente de donde residan o se constituyan, como es el caso de Argentina y por lo tanto quedan bajo esa normativa los PSAV offshore.

Asimismo, el informe menciona por ejemplo que se han utilizado PSAV para lavar activos utilizando a sujetos offshore que no tienen registro ni licencia en la jurisdicción que opera pero que actúa como si fuera un cliente particular de otro PSAV que cuenta con la licencia o registro requerido.

En ese sentido, recomienda a las jurisdicciones avanzar en medidas de mitigación entre las que se encuentran, por ejemplo, fomentar la cooperación y mejorar la coordinación entre grupos de trabajo interinstitucionales y realizar asociaciones público-privadas, mejorar los canales de comunicación entre organismos supervisores y la cooperación entre las UIFs de diferentes jurisdicciones a fin de agilizar el acceso a la información y coordinar las acciones de mitigación que se consideren necesarias.

4.3. Influencia de los estándares internacionales y el rol del GAFI

El proceso de incorporación del régimen aplicable a los PSAV en Argentina no puede comprenderse de manera aislada, sino en el marco de la influencia de la mirada de los organismos internacionales especialmente el GAFI, tal como ha sido mencionado en los apartados anteriores.

En este sentido, la adopción de regulaciones específicas para los activos virtuales responde, en gran medida, a que en nuestro país se avanzó por la necesidad de adecuación a los lineamientos establecidos a nivel global, en un contexto de un proceso de evaluación mutua y exigencias de cumplimiento ligadas al resultado de la evaluación.

La sanción de la Ley 27.739 y las normas emitidas por la CNV y la UIF fueron parte de ese proceso de adecuación, en el que la adopción de estándares internacionales opera como un factor determinante en el diseño del marco normativo local. Sin embargo, esta incorporación no siempre se traduce en una implementación efectiva, en tanto las particularidades del contexto institucional, económico y tecnológico pueden dificultar la aplicación de modelos regulatorios diseñados para jurisdicciones diferentes.

En este sentido, la influencia del GAFI plantea una tensión entre la necesidad de cumplir con estándares internacionales y la capacidad real de adaptación del ordenamiento jurídico interno y no necesariamente logran identificar los riesgos propios de la jurisdicción ni impactar de manera significativa en su mitigación.

Así, si bien la incorporación de los estándares del GAFI constituye un elemento central en la evolución del régimen de PSAV en Argentina, su análisis permite advertir que la eficacia del sistema no depende exclusivamente de su alineación con los estándares internacionales, sino también de su capacidad de adaptación a las particularidades del contexto local y de la articulación efectiva entre sus distintos organismos competentes.

5. Conclusiones

El análisis de la normativa aplicable a los PSAV en Argentina permite afirmar que la incorporación de este tipo de actores al sistema de prevención del lavado de activos constituye un avance significativo en lo formal, en términos de adecuación a los estándares internacionales. La sanción de la Ley 27.739 y su posterior reglamentación han contribuido a dotar de mayores herramientas y estructura a un ámbito que, hasta ese momento, se caracterizaba por su fragmentación normativa y la ausencia de un enfoque integral.

Sin embargo, este avance normativo, que si bien es reciente, no se traduce necesariamente en una mayor eficacia del sistema. Tal como hemos mencionado, la implementación de la normativa relativa a los PSAV presenta una serie de deficiencias que limitan su capacidad real de prevención. Entre ellas, se destacan la falta de coordinación y cooperación efectiva entre los organismos competentes, las dificultades para regular y supervisar a los actores que operan desde el exterior, y los desafíos operativos derivados de las particularidades tecnológicas del ecosistema de activos virtuales, especialmente la regla de viaje.

Asimismo, la influencia de la evaluación del GAFI en cuanto al cumplimiento de las 40 Recomendaciones, ha sido un impulso importante para la sanción de la Ley 27.739 y la reglamentación por parte de la CNV y la UIF en un tiempo récord. Sin embargo, hemos planteado algunas cuestiones en relación con la falta de análisis de la capacidad de adaptación a nuestro régimen jurídico interno, contexto económico y cultural, evidenciando que la adecuación formal a dichos estándares no garantiza por sí misma la efectividad de las políticas de prevención.

En ese sentido, la regulación de los PSAV pone en discusión un problema más amplio que su diseño e implementación en Argentina, pone de manifiesto las limitaciones de los enfoques regulatorios tradicionales frente a fenómenos que son de naturaleza global, descentralizada, tecnológicamente compleja y que evolucionan a un ritmo acelerado y constante. La regulación de los criptoactivos exige no solo la incorporación de nuevas normas, sino también el desarrollo de capacidades institucionales, mecanismos de coordinación y cooperación interinstitucional e internacional y herramientas tecnológicas que permitan identificar los riesgos asociados y diseñar acciones de mitigación.

Del análisis realizado en el presente trabajo se desprende que más allá de las dificultades mencionadas, el marco normativo aplicable a los PSAV en Argentina aún se encuentra en una primera etapa de implementación, por lo cual se requiere realizar un monitoreo del grado de maduración del sistema que permita observar cómo se van integrando en la práctica las capacidades institucionales y tecnológicas, los mecanismos de supervisión y los flujos de información entre organismos. Ello en razón de que solo a partir de una evaluación integral basada en evidencia, va a ser posible determinar si la adecuación formal a los estándares internacionales se traduce en el

fortalecimiento efectivo del sistema de prevención, como así también identificar oportunidades de mejora a los efectos de abordar un fenómeno tan complejo como cambiante como es el ecosistema de activos virtuales.

Bibliografía

Bensousan, J. (2024). Travel Rule MICA.

Comisión Nacional de Valores. (2024). Resolución General 944/2024.

Comisión Nacional de Valores. (2025). *Informe de gestión*. https://www.argentina.gob.ar/cnv/informes-de-gestion

Comisión Nacional de Valores. (2025). Resolución General 1058/2025.

Grupo de Acción Financiera Internacional. (2021). Updated guidance for a risk-based approach to virtual assets and VASPs.

Grupo de Acción Financiera Internacional. (2024). *Informe de evaluación mutua de la República Argentina*. https://biblioteca.gafilat.org/?p=7460

Grupo de Acción Financiera Internacional. (2024). Targeted update on virtual assets and VASPs.

Grupo de Acción Financiera Internacional. (2026). *Understanding and mitigating the risks of offshore virtual asset service providers*. https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Virtualassets/Understanding-Mitigating-Risks-Offshore-VASPs.html

Ley 27.739. (2024). Modificaciones del Código Penal

TRM. (2025). Informe 2025 sobre adopción de criptomonedas y uso de stablecoin.

Unidad de Información Financiera. (2024). Informe de gestión. https://www.argentina.gob.ar/uif/informes-de-gestion

Unidad de Información Financiera. (2024). Resolución UIF 49/2024.

Zocaro, M. (2020). *El marco regulatorio de las criptomonedas en Argentina: Comparativa con otros países*. Centro de Estudios en Administración Tributaria (CEAT), Facultad de Ciencias Económicas, Universidad de Buenos Aires.

Fiscalidad internacional de criptoactivos: panorama actual, desafíos normativos y perspectivas

Antonella Gervagi[1] y Ana Laura Jaruf[2]

Resumen

El artículo analiza cómo el crecimiento del mercado de criptoactivos —caracterizado por su opacidad y el anonimato relativo de sus transacciones— plantea desafíos para las administraciones tributarias en términos de recaudación, equidad fiscal y prevención de ilícitos como el lavado de dinero y el financiamiento del terrorismo. Tras repasar las definiciones y categorías de criptoactivos (criptomonedas, NFT, stablecoins, security tokens), se centra en el Marco de Reporte de Criptoactivos (CARF) impulsado por la OCDE junto con las modificaciones al Estándar Común de Reporte (CRS), que buscan establecer un intercambio automático de información entre jurisdicciones, aunque reconoce limitaciones frente a las transacciones peer-to-peer,

1- Economista y magíster en Economía (UBA) y doctoranda en Economía Política (UNSAM). Trabajó en la División Intercambio Automático de Información y en la División Economía Digital de ARCA, y antes en la Comisión Federal de Impuestos. Coordina la línea de Economía Digital del Departamento de Economía Política del Centro Cultural de la Cooperación Floreal Gorini y preside el Comité de Jóvenes Investigadoras de IAFFE. Investiga el intercambio de información sobre criptoactivos con fines fiscales, la tributación de la economía digital y los vínculos entre fiscalidad, ambiente y género en América Latina. Correo: antogervagi@gmail.com

2- Economista y magíster en Economía (UBA) y doctoranda en Ciencias Económicas, subárea Finanzas (UBA). Es analista senior de Riesgo Crediticio y Finanzas Sostenibles en FIX SCR (afiliada de Fitch Ratings) y coordina proyectos de transparencia y acceso a la información socioambiental en CEPPAS. Integra el área de Economía y Ambiente del Centro Cultural de la Cooperación Floreal Gorini. Investiga la fiscalidad internacional de la economía digital, la gobernanza de datos y las finanzas sostenibles. Correo: analaurajaruf@gmail.com

las finanzas descentralizadas (DeFi) y los wallets auto-custodiados. Luego, compara experiencias regulatorias en países desarrollados (Estados Unidos, Unión Europea, Japón), economías emergentes (India, Singapur) y América Latina (Brasil, México y especialmente Argentina, con la Ley 27739 y el Dictamen 2/2022 de AFIP, incluyendo el episodio de la criptomoneda LIBRA). Concluye que la efectividad de estos marcos depende de la adopción internacional, el fortalecimiento de capacidades técnicas de las administraciones fiscales y la coordinación interinstitucional, y plantea que para Argentina es clave adherir temprano al CARF, implementar las obligaciones de reporte y balancear la fiscalización con la promoción de la innovación financiera, sin perder de vista la dimensión de equidad fiscal y de género que atraviesa la opacidad de estos instrumentos.

1. Introducción

Desde la aparición del Bitcoin en 2009, los activos criptográficos han adquirido una importancia creciente en el sistema financiero internacional. Caracterizados como dinero en efectivo de Internet, estos instrumentos se basan en una tecnología innovadora que posibilita la creación y transferencia de activos sin la participación de intermediarios financieros tradicionales y sin que exista una autoridad central con visibilidad plena sobre las transacciones, sus titulares o la localización de los recursos. Esta característica alertó a los gobiernos sobre la ausencia de control, particularmente respecto de operaciones que involucran volúmenes significativos de capital.

En este contexto, para otorgar mayor claridad al sistema financiero, el G20, bajo liderazgo italiano en 2021, encomendó a la Organización para la Cooperación y Desarrollo Económicos (OCDE) el diseño de un marco de transparencia fiscal específico para criptoactivos, que permitiera la recopilación estandarizada de información sobre este tipo de operaciones desde una perspectiva de fiscalidad internacional.

Esta iniciativa respondió a la constatación de que tales instrumentos pueden constituir vehículos para la evasión tributaria, dada su limitada supervisión regulatoria y el anonimato relativo que ofrecen, lo cual representa un riesgo para los avances logrados en materia de transparencia fiscal a nivel global.

La opacidad de las transacciones con criptoactivos para las administraciones fiscales trasciende la mera pérdida recaudatoria, dado que pueden emplearse en actividades ilícitas y financiamiento del terrorismo. Por estos motivos, la OCDE promovió un nuevo esquema de intercambio de información denominado Marco de Reporte de Criptoactivos (Crypto Asset Reporting Framework, CARF), junto con modificaciones al Estándar Común de Reporte (CRS). Estos instrumentos requerirán que los proveedores de servicios relacionados con criptoactivos suministren información de usuarios a las autoridades nacionales, para su posterior intercambio entre países participantes.

Para Argentina, esto implicaría que la administración tributaria nacional reciba información sobre tenencias de criptoactivos de residentes argentinos, tanto en el país como en otras jurisdicciones participantes del intercambio, siempre que se encuentren en instituciones sujetas a la obligación de reporte.

Este sistema de intercambio aún no ha sido implementado y, aunque se proyecta su adopción para 2027, presenta debilidades, como la dificultad para acceder a información sobre criptoactivos que no operen mediante intermediarios regulados.

Para abordar integralmente el debate sobre fiscalidad en el mercado cripto, el presente trabajo se estructura de la siguiente manera: un primer apartado analiza la composición del mercado para dimensionar los volúmenes operados y su relevancia fiscal. El segundo apartado revisa definiciones y aspectos generales. En el tercero se examina la importancia de la fiscalización, no solo desde el punto de vista recaudatorio sino también en términos de transparencia, equidad fiscal y reducción de ilegalidad. El cuarto apartado detalla la aplicación del intercambio de información en la fiscalidad internacional de criptoactivos. Finalmente, las dos secciones conclusivas revisan los avances regulatorios a nivel global y regional.

2. Situación actual del mercado de criptoactivos

Como se mencionó, la primera criptomoneda (Bitcoin) surgió en 2009. Actualmente se estima que existen más de 9.000 criptomonedas en circulación. Según CoinMarketCap, la capitalización del mercado global de criptomonedas supera los 2,09 billones de dólares. Del

total, el volumen en finanzas descentralizadas (DeFi) representa aproximadamente 3,57 mil millones de dólares, equivalente al 6,8% del volumen total. Un estudio de Triple-A (2024) estima que el 6,8% de la población mundial posee y utiliza monedas digitales. En Argentina, este porcentaje alcanza el 5,6%, representando a 2,5 millones de personas.

Según el análisis de Triple-A, la creciente adopción en Argentina puede vincularse, parcialmente, con la alta inflación y las restricciones cambiarias. En este sentido, numerosos trabajadores perciben remuneraciones en criptomonedas por servicios prestados de forma remota en el exterior, encontrando en estos instrumentos mecanismos para eludir controles estatales.

La aceptación y uso global presenta heterogeneidad significativa. La consultora Chainalysis desarrolló un índice de adopción que, en 2023, posiciona a Brasil como líder en uso de estos activos en América Latina, mientras Argentina ocupa el puesto 15 a nivel mundial.

El uso creciente debe interpretarse conjuntamente con el proceso de digitalización acelerado por la pandemia de COVID-19, que impulsó el uso de esta tecnología y su valorización: entre el inicio de la pandemia en 2020 y su conclusión en 2022, el valor del Bitcoin se multiplicó por diez y su capitalización creció más del 300%.

A pesar de su expansión, el mercado cripto ha experimentado volatilidades y cuestionamientos. Un ejemplo paradigmático es el caso de FTX, plataforma de intercambio con sede en Bahamas fundada en 2019 que, en su apogeo, contaba con más de 1 millón de usuarios, constituyéndose en uno de los mercados más grandes del mundo. Sin embargo, el 14 de noviembre de 2022 se declaró en bancarrota tras surgir dudas sobre su solvencia, generando una crisis de confianza en el mercado de criptoactivos hacia finales de ese año.

Esta crisis permitió conocer mejor la adopción estructural de estos activos, evidenciándose que el impacto fue heterogéneo entre países: aquellos con menor capacidad adquisitiva no se desprendieron masivamente de sus criptoactivos. Esto sugiere que estos instrumentos funcionan más como vehículos de ahorro que como medios transaccionales. Resulta pertinente, entonces, considerar a los criptoactivos como activos financieros y no como moneda per se, dado que las monedas deben cumplir tres funciones: medio de intercambio,

unidad de cuenta y reserva de valor. Dado que las criptomonedas no son universalmente aceptadas como medio de pago, se las entiende principalmente como instrumentos de reserva de valor, aspecto relevante al momento de diseñar esquemas de fiscalización.

3. Definiciones y características de los criptoactivos

Cuando nos referimos a criptoactivos, incluimos tanto criptomonedas como otros activos digitales que utilizan criptografía para asegurar transacciones y controlar la creación de nuevas unidades (NFT, stablecoins, tokens de seguridad, entre otros).

Constituye un hito relevante en la regulación de activos virtuales la reciente Ley 27.739, que modifica la Ley 25.246 sobre prevención del lavado de activos, el financiamiento del terrorismo y la proliferación de armas de destrucción masiva. Esta norma incorpora una definición legal del término activos virtuales y asigna a la Comisión Nacional de Valores (CNV) la regulación de los proveedores de servicios de activos virtuales (PSAV). El artículo 4 de la Ley 27.739 especifica:

> "Activos virtuales: representación digital de valor que se puede comercializar y/o transferir digitalmente y utilizar para pagos o inversiones. En ningún caso se entenderá como activo virtual la moneda de curso legal en territorio nacional y las monedas emitidas por otros países o jurisdicciones (moneda fiduciaria)."

Las criptomonedas constituyen una forma de dinero digital con diversas aplicaciones que utiliza un sistema descentralizado basado en criptografía. A diferencia del dinero tradicional, no requieren intermediarios para su transferencia y permiten transacciones directas entre usuarios. La tecnología subyacente, denominada blockchain, registra todas las transacciones en una red distribuida, proporcionando transparencia y seguridad al sistema.

El funcionamiento de las criptomonedas se basa en la criptografía asimétrica, donde cada usuario posee un par de claves: una pública (equivalente a un número de cuenta) y una privada (equivalente a una contraseña). Las transacciones se firman con la clave privada y se verifican mediante la clave pública, garantizando autenticidad sin revelar la identidad del usuario.

Existen diferentes categorías de criptoactivos. Los NFT (non-fungible tokens) representan la propiedad de objetos únicos o contenidos específicos en la blockchain. A diferencia de las criptomonedas como Bitcoin, que son fungibles (cada unidad es intercambiable por otra del mismo valor), los NFT son únicos y no intercambiables por algo equivalente.

Las stablecoins o monedas estables constituyen un tipo de criptomoneda diseñada para mantener un valor estable en relación con una moneda o activo de referencia, como el dólar estadounidense o el euro. Este diseño busca reducir la volatilidad característica de otras criptomonedas.

Los tokens de seguridad, también conocidos como security tokens, conforman una categoría de tokens digitales que representan una inversión en un activo real y se encuentran regulados por las leyes de valores. A diferencia de las criptomonedas y los tokens de utilidad, que se emplean para acceder a servicios o productos dentro de una plataforma, los tokens de seguridad están diseñados para reflejar activos financieros tradicionales, como acciones, bonos, participaciones en bienes raíces o contratos futuros.

4. Importancia de la fiscalización de criptoactivos

La fiscalización de criptoactivos trasciende el objetivo meramente recaudatorio y se vincula con múltiples dimensiones de política pública. La ausencia de mecanismos adecuados de control genera consecuencias que afectan la equidad del sistema tributario, la capacidad recaudatoria del Estado y la prevención de actividades ilícitas.

La naturaleza descentralizada de los criptoactivos y la posibilidad de evitar la interacción con el sistema financiero tradicional ha abierto nuevas oportunidades para que los contribuyentes, tanto individuos como entidades, oculten sus ingresos y riquezas a la vista de las autoridades fiscales.

4.1. ¿Cuál es el impacto de mejorar la fiscalidad internacional de los criptoactivos en términos de justicia fiscal?

Al igual que el sector financiero tradicional, que históricamente ha estado bajo estricta supervisión regulatoria y requisitos de presentación de informes (incluyendo aspectos fiscales), los criptoactivos y los

intermediarios que facilitan su uso han sido objeto de recomendaciones también por parte del Grupo de Acción Financiera Internacional (GAFI). En este sentido, en 2015, redactó un documento específico en materia de monedas virtuales llamado "Directrices para un enfoque basado en riesgo para el caso de las monedas virtuales" (GAFI, 2015).

A pesar de estos avances, estos instrumentos aún no se encuentran sujetos a los mismos requisitos que el sector financiero tradicional y, sumado que constituyen una industria que se halla en constante evolución y desarrollo, carecen de la experiencia acumulada durante años de declaraciones fiscales. En cuestiones de fiscalidad internacional, este punto resulta relevante porque son los PSAV los que conformarán la fuente del intercambio de información CARF (desarrollado en el siguiente apartado). Para poner en contexto, antes de la implementación del intercambio de CRS, las autoridades fiscales enfrentaban dificultades para conocer si sus contribuyentes poseían cuentas financieras en el extranjero, quiénes eran los beneficiarios finales y cuáles eran sus montos de transacciones. Situación similar a lo que ocurre hoy en día con el mundo cripto. Esto complicaba la tarea de obtener una visión completa de los ingresos y la riqueza de los contribuyentes, y, por ende, de aplicar adecuadamente las normativas tributarias nacionales.

En el caso de los criptoactivos, la naturaleza flexible del sector y la facilidad con la que pueden efectuarse transacciones, incluso transfronterizas, incrementan los riesgos asociados, particularmente en términos de evasión fiscal. Esta situación puede derivar en una reducción de los recursos disponibles de los Estados, lo que indirectamente agrava situaciones de desigualdad, las cuales se manifiestan no solo en términos de ingresos y condiciones socioeconómicas, sino también en dimensiones de género, dado que las mujeres se encuentran sobrerrepresentadas en los deciles de menores ingresos.

En este contexto, el fortalecimiento de la capacidad recaudatoria de los Estados podría contribuir a la disminución de las brechas de ingresos y de género.

Adicionalmente, una dimensión que puede analizarse en términos de desigualdad es la existente entre mujeres y varones. A nivel global, la adopción de criptoactivos presenta una marcada disparidad de género: el 61% de los usuarios son varones frente al 39% correspondiente a mujeres (Triple-A, 2024), con una diferencia más acentuada

en el grupo etario de 25 a 44 años. Si se considera que estos activos pueden ser utilizados como instrumentos para la evasión fiscal, dicha asimetría en la adopción podría profundizar aún más las desigualdades de género, por el mayor involucramiento de los varones en este tipo de operaciones.

Con relación a lo anterior, algunos autores han demostrado que gran parte de la desigualdad económica actual se halla vinculada a la evasión fiscal. Mencionan Noelia Méndez Santolaria y Antonella Gervagi:

> La omisión de pago de impuestos en Argentina socava la eficacia de la recaudación y contribuye a que se caiga en una especie de círculo vicioso: para alcanzar adecuados niveles de recaudación que permitan sostener una política de intervención activa, se apela a una presión mayor sobre la economía registrada y los tributos indirectos, lo que a su vez desincentiva la registración e incentiva la búsqueda por la minimización de la carga (Méndez Santolaria y Gervagi, 2022, p. 8).

Por su parte, Grondona et al. (2016) apuntan que la disminución en la capacidad de recaudar impuestos por parte del Estado no resulta neutral en términos de género. La pérdida de ingresos suele compensarse al gravar a contribuyentes cumplidores, como pequeñas y medianas empresas (PYMES) o personas de ingresos medios, y expandir la tributación indirecta. Ello tiene una especial incidencia en las mujeres sobrerrepresentadas en los estratos de ingresos más bajos y en las PYMES que se benefician menos de las oportunidades de eludir impuestos.

Siguiendo la lógica señalada por las autoras, la evasión fiscal que habilitan estos instrumentos, que permiten ocultar ingresos y riquezas, deriva en una merma de impuestos progresivos y se continúa con la dependencia del sistema tributario en impuestos indirectos y regresivos, como el impuesto al valor agregado (IVA). Cuando individuos o entidades utilizan mecanismos para ocultar sus ingresos y riqueza, el impacto negativo en la equidad y la justicia social se profundiza. A esto se le suma que los agentes económicos con más recursos son los que acceden a mecanismos más sofisticados de evasión, lo que les permite eludir sus responsabilidades tributarias y acrecentar sus riquezas a costa de una reducción significativa de los ingresos para los gobiernos.

Como riesgo colateral, también el uso de activos y/o intermediarios que no se encuentran cubiertos por los marcos existentes del intercambio de información de cuentas financieras amenaza con deshacer los beneficios de transparencia logrados con la implementación generalizada del CRS.

4.2. Estado actual de la fiscalidad internacional en materia de criptoactivos

Los riesgos asociados al uso de criptoactivos adquieren particular relevancia cuando estas tecnologías se utilizan sin intermediarios. La naturaleza descentralizada de muchos criptoactivos permite realizar transacciones sin requerir identificación del cliente, lo que dificulta vincular las operaciones con sujetos concretos fuera del entorno virtual. En este contexto, la ausencia de mecanismos institucionales de control —como organismos reguladores o sistemas efectivos de prevención del lavado de activos— genera serias limitaciones para el monitoreo de estas actividades.

Pero incluso cuando los contribuyentes interactúan con intermediarios, las administraciones tributarias enfrentan desafíos si estos últimos se encuentran radicados en el extranjero. Aquí la fiscalidad internacional cobra especial importancia, ya que las autoridades competentes locales poseen dificultades para acceder a información precisa que permita auditar adecuadamente esas operaciones. Además, resulta más sencillo requerir información a entidades residentes que a no residentes, lo que pone en evidencia la necesidad de marcos de cooperación internacional robustos, adaptados a las nuevas dinámicas del ecosistema cripto.

En esta línea, Grondona y Gervagi (2024) y Rua (2024) mencionan el rol de los criptoactivos como un nuevo vehículo para los flujos financieros ilícitos. Su arquitectura tecnológica, basada en la descentralización y el anonimato, convierte a los criptoactivos en verdaderos "agujeros" dentro del entramado tributario internacional, que actúan como nuevas formas de guaridas fiscales. Esto deviene en un problema sistémico que impacta especialmente en los países en desarrollo, que muchas veces poseen menores capacidades de control y fiscalización.

Adicionalmente, Grondona et al. (2016) aclaran que los flujos financieros ilícitos pueden incluir, entre otras cuestiones, los productos

de la evasión por parte de personas físicas y jurídicas, actividades delictivas como el cohecho, el narcotráfico o la trata de personas, así como la elusión impositiva practicada por empresas multinacionales. En contextos de controles cambiarios, estos flujos también funcionan como vehículos para sortear regulaciones.

Un ejemplo ilustrativo de evasión fiscal derivada de la falta de regulación se expone en Rua (2024), quien analiza una práctica recurrente por parte de determinadas empresas mediante el uso de ofertas iniciales de monedas (initial coin offerings) o tokens. A través de esta modalidad, las compañías emiten nuevos criptoactivos con el objetivo de recaudar fondos, eludiendo muchas veces los marcos regulatorios tradicionales aplicables a la emisión de valores negociables. En estos casos, la empresa lanza al mercado un nuevo tipo de activo digital —en lugar de acciones u otros instrumentos financieros convencionales— que se vende a cambio de criptomonedas, como Bitcoin, o dinero.

Estos tokens suelen ser presentados como oportunidades de inversión ligadas al desarrollo de proyectos futuros. Sin embargo, dada la escasa o nula supervisión estatal y la ausencia de garantías jurídicas, pueden terminar siendo vehículos para fraudes de gran escala. Un caso paradigmático en esta línea radica en el proyecto Libra, promovido en Argentina por el presidente de la Nación. En este caso, se ofreció una criptomoneda con la promesa de financiar empresas nacionales, pero terminó configurando un esquema fraudulento que perjudicó a aproximadamente 40 mil personas por un estimado en torno a los 90 millones de dólares (Smink, 2025).

Ante el incremento sostenido de estas transacciones financieras a nivel global, la creciente posibilidad de arbitraje normativo entre jurisdicciones y la emergencia de nuevos escenarios económicos impulsados por la digitalización, se vuelve imperativo avanzar hacia mecanismos efectivos de cooperación internacional. En particular, resulta crucial el desarrollo de acuerdos que permitan el intercambio automático de información tributaria relativa a criptoactivos, con el objetivo de reducir la opacidad y prevenir tanto la evasión fiscal como los flujos financieros ilícitos.

Si bien es cierto que las transacciones sin intermediarios representan grandes dificultades para la fiscalidad internacional, aún

suponen una porción minoritaria del mercado: 6,9% del volumen total. Es decir que la gran mayoría de las operaciones se canalizan a través de exchanges, lo cual implica una oportunidad concreta para implementar sistemas de información que, aunque todavía limitados frente al uso de tecnologías totalmente descentralizadas, permitirían fortalecer la capacidad fiscalizadora de los Estados.

Es en este contexto, y reconociendo los riesgos asociados, que la OCDE ha impulsado el desarrollo del CARF, así como una adenda al CRS, con el propósito de ampliar el alcance del intercambio automático de información financiera a este tipo de activos digitales.

Pero este esfuerzo no se lleva a cabo de manera aislada, sino que sigue los pasos de otros organismos internacionales, como el GAFI, y se alinea con la Directiva de Cooperación Administrativa 8 de la Unión Europea, entre otros.

El GAFI ha desempeñado un papel fundamental en la gestión de los riesgos vinculados con los criptoactivos, al establecer estándares y directrices globales para regular este sector. Estas directrices incluyen la implementación de requisitos de cumplimiento, como el conocimiento del cliente, y la debida diligencia, que obligan a los PSAV a identificar a sus usuarios y vigilar transacciones sospechosas. Además, el GAFI ha instado a los países miembro a regular adecuadamente las plataformas de intercambio y los PSAV para reducir riesgos.

En Argentina, se cumplió con la Recomendación 15 del GAFI en marzo de 2024, al aprobar la citada Ley 27.739, en la cual se establece un registro para los PSAV —en el ámbito de la CNV—, de manera que quienes no estén registrados no puedan operar en el país. El registro abarca a todos aquellos que utilicen páginas web, redes sociales u otros medios para dirigir su oferta y/o publicidad a residentes en Argentina, que tengan un volumen significativo de operaciones en el país o que utilicen cualquier tecnología para recibir fondos de residentes argentinos.

Sin embargo, resulta importante destacar que, a la fecha de elaboración del presente capítulo, Argentina no forma parte de los cincuenta países que ya han suscripto el Acuerdo Multilateral entre Autoridades Competentes sobre el intercambio automático de información conforme al CARF (OCDE, 2022).

5. El intercambio de información con fines fiscales[3]

Entre las herramientas que posee la fiscalidad internacional —para prevenir la evasión fiscal y combatir los flujos financieros ilícitos—, el intercambio de información se ha consolidado como una herramienta clave, que puede llevarse a cabo bajo tres modalidades: espontánea, a requerimiento o automática; esta última es la que contemplan tanto el CARF como la adenda al CRS.

En este contexto, Argentina es miembro del Foro Global sobre Transparencia e Intercambio de Información con Fines Fiscales desde 2009 y desde 2013 participa activamente en la Convención sobre Asistencia Administrativa Mutua en Materia Fiscal, la cual establece un marco legal multilateral que habilita el intercambio automático de información entre jurisdicciones. Como antecedente relevante, en 2017 el país implementó por primera vez este mecanismo en el marco del CRS, aplicado a cuentas financieras.

El CARF y la adenda al CRS se complementan y se centran en distintos conceptos específicos, y se diferencian en cuanto a los sujetos obligados, el alcance de los activos cubiertos y los tipos de transacciones e información que deben reportarse.

El CARF entiende como "criptoactivo" a cualquier representación digital de valor respaldada por tecnologías de registro distribuido o similares, cuya propiedad puede transferirse digitalmente. Es decir que abarca tanto tokens fungibles como no fungibles (NFT), incluyendo a aquellos utilizados como medio de pago o inversión. En consecuencia, los NFT comercializados en plataformas digitales también pueden considerarse criptoactivos, y, por ende, ser reportados.

Por su parte, la adenda al CRS amplía su alcance para incorporar monedas digitales emitidas por bancos centrales, productos de dinero electrónico, derivados referenciados en criptoactivos e inversiones indirectas a través de vehículos financieros. Esta expansión busca mantener la coherencia del estándar frente a las innovaciones tecnológicas y garantizar que se apliquen los mismos procedimientos de debida diligencia y reporte a todos los tipos de activos, entre ellos, los digitales.

3- Esta sección ha sido tomada sustancialmente de Grondona y Gervagi (2024).

Con relación a los sujetos obligados a reportar, la adenda al CRS indica que son las instituciones financieras tradicionales, lo que abarca bancos, instituciones de custodia y depósito, entidades de inversión y compañías de seguros. Mientras que el CARF está dirigido a una gama distinta de entidades, como exchanges de criptoactivos, billeteras digitales, cajeros automáticos, corredores y distribuidores, que actúan como intermediarios en el ecosistema de criptoactivos.

El CARF abarca transacciones como intercambios entre criptoactivos y dinero, operaciones entre distintos criptoactivos relevantes, transferencias hacia o desde billeteras externas no custodiadas (por ejemplo, billeteras frías) y pagos minoristas. La información a reportar incluye el nombre del criptoactivo, monto bruto pagado o recibido, cantidad de unidades, número de transacciones, valor de mercado y detalles de transferencias hacia billeteras externas no gestionadas por entidades reportantes.

En contraste, el CRS ya contemplaba derivados sobre activos financieros tradicionales; la inclusión de derivados basados en criptoactivos y de entidades de inversión que mantienen posiciones en ellos busca garantizar consistencia normativa y coherencia con el marco internacional existente.

Se destaca el avance de la cooperación entre los países para establecer normativas y estándares internacionales claros en términos de fiscalidad de los criptoactivos, que aborda desafíos como la evasión fiscal y asegura que los ingresos generados por los criptoactivos sean adecuadamente gravados de acuerdo con las leyes fiscales nacionales e internacionales.

6. Marco regulatorio vigente de las criptomonedas en América Latina

América Latina se encuentra en una etapa de adaptación y fortalecimiento de sus marcos regulatorios, en respuesta a las iniciativas internacionales descriptas en el apartado anterior. Aunque el grado de avance varía entre los países de la región, muchos gobiernos latinoamericanos han comenzado a alinear sus políticas con estos estándares globales, al reconocer la importancia de contar con un entorno

regulatorio más transparente y seguro ante el crecimiento acelerado del uso de criptoactivos.

México ha sido pionero en la región en establecer un marco regulatorio para los criptoactivos. En 2017 se publicó un comunicado conjunto de los tres organismos reguladores financieros (la Comisión Nacional Bancaria y de Valores, la Secretaría de Hacienda y Crédito Público y el Banco de México), en el que se advertía sobre los riesgos vinculados al uso de activos virtuales y a los esquemas de inversión asociados a las ofertas iniciales de monedas (CNBV et al., 2017). Al año siguiente, a través de la ley para regular las instituciones de tecnología financiera (Ley Fintech), obligó a las plataformas de criptomonedas a registrarse y cumplir con medidas contra el lavado de dinero y financiamiento del terrorismo. Además, ha avanzado en la implementación de la "regla de viaje" del GAFI, que requiere que los PSAV compartan información sobre las transacciones (Proskalovich et al., 2023).

Adicionalmente, en la Ley Fintech (Art. 30) se definió por primera vez qué se entiende por activo virtual:

> Un activo virtual es la representación de valor registrada electrónicamente y utilizada por el público como medio de pago para todo tipo de actos jurídicos, cuya transferencia solo puede realizarse a través de medios electrónicos. En ningún caso los activos virtuales se entenderán como moneda de curso legal en el territorio nacional, moneda extranjera o cualquier otro activo denominado en moneda nacional o extranjera (Ley para regular las instituciones de tecnología financiera, 2018).

Por su parte, en Brasil, la primera normativa que introdujo una definición de criptoactivos y de plataforma de intercambio fue la Instrucción Normativa 1888/19 de la Receita Federal do Brasil, que, de este modo, definió al criptoactivo:

> Una representación digital de valor, denominada en su propia unidad de cuenta, cuyo precio puede expresarse en moneda soberana local o extranjera, transaccionada electrónicamente mediante el uso de criptografía y tecnologías de registro distribuido, que puede utilizarse como forma de inversión, instrumento de transferencia de valor o acceso a servicios, y que no constituye moneda de curso legal (Receita Federal do Brasil, 2019).

Luego, en 2022, el país aprobó la Ley 14478 de activos virtuales, que establece directrices para la prestación de servicios con activos virtuales y la regulación de los proveedores de estos servicios (Proskalovich et al., 2023).

Por su parte, Colombia implementó un sandbox regulatorio que permite a las entidades financieras probar productos y servicios relacionados con blockchain y criptomonedas en un entorno controlado. Además, en abril de 2022, entró en vigor una norma que exige que las transacciones en criptomonedas superiores a 150 dólares sean notificadas a la Unidad de Información y Análisis Financiero, con el objetivo de prevenir operaciones ilícitas.

El Salvador fue el primer país del mundo en adoptar el bitcoin como moneda de curso legal, aunque en enero de 2025 se aprobaron reformas que revirtieron esa decisión. A pesar de esto, su uso continúa siendo voluntario.

En el caso de Bolivia, en junio de 2024, el Banco Central derogó la resolución que prohibía el uso, comercio e integración de las criptomonedas en su sistema financiero. Con la nueva legislación, se determina que la entidad será la encargada de regular y fiscalizar a las empresas del sector de las criptomonedas.

En Uruguay, durante 2018, la Cámara Uruguaya de FinTech creó una Comisión de Criptomonedas con el objetivo de desarrollar un marco regulatorio específico para el sector y, en 2021, el Banco Central de Uruguay publicó un comunicado en el cual indicaba que se encontraba trabajando en la preparación de una posible regulación, enfocada en las actividades comerciales generadas alrededor de los activos virtuales. En 2024, aprobó la Ley 20.345, que regula los activos virtuales y amplía la supervisión del Banco Central sobre los PSAV. Adicionalmente, se estableció que la Superintendencia de Servicios Financieros abordará el cumplimiento dentro de las leyes de valores, la prevención del lavado de dinero y la protección al consumidor.

Impuesto a las ganancias

Al analizar la carga tributaria de este tipo de activos a nivel regional, se observa una notable heterogeneidad. Para el caso del impuesto a las ganancias, en el extremo inferior derecho del Gráfico 1, se encuentran países como Panamá y El Salvador, en los cuales no se aplican impuestos sobre este tipo de activos. De manera opuesta, Chile cuenta con una normativa fiscal que contempla una imposición que puede alcanzar hasta el 40% según ingresos. En Perú, por ejemplo, la alícuota se determina en función del volumen de criptoactivos reportado, y oscila entre el 5 y el 30%. Por su parte, en países como Argentina, México, Costa Rica, Bolivia y Brasil, la carga tributaria para personas físicas suele ubicarse en un rango que va del 15 al 20%, mientras que en Colombia se aplica una tasa aproximada del 10% (HelloSafe, 2025).

También puede existir variación en la operación que se grava. En el caso de Brasil, las operaciones gravadas consisten en la venta de criptomonedas por dinero, el intercambio entre diferentes criptomonedas y el uso de estas para pagar bienes o servicios. Por el contrario, quedan exentas las operaciones de compra de criptomonedas con dinero y las transferencias entre billeteras propias.

En Argentina, lo que se grava en el impuesto a las ganancias son las operaciones de compraventa de criptomonedas, ya que se consideran como ganancias de capital. Por otro lado, se incluye también el impuesto a los créditos y débitos bancarios (impuesto al cheque), el cual se aplica a las transacciones que involucren criptomonedas y que impacta en las billeteras que ejecutan la operación. También debe mencionarse el IVA, que solo afecta a las comisiones de los exchanges.

En Bolivia, este gravamen se denomina impuesto a las grandes fortunas. En este caso, aunque la normativa no menciona explícitamente a los criptoactivos, se podría inferir su inclusión al considerar que la fortuna sujeta a este impuesto comprende tanto bienes como activos financieros y otros bienes con valor económico. Por lo tanto, si un contribuyente posee criptoactivos cuyo valor, sumado al de otros bienes, supera el umbral establecido, estará sujeto al pago del impuesto.

El caso de Venezuela no se encuentra incluido en el gráfico precedente, dado que en este país se cobra el impuesto a las grandes transacciones financieras, que es del 3% sobre las operaciones en divisas o criptomonedas distintas al bolívar y al petro, realizadas por ciertas personas naturales y jurídicas.

Bienes personales o al patrimonio

En Argentina, deben valuarse los activos al 31 de diciembre y al costo de adquisición, y tributan si superan el mínimo no imponible (Dictamen 2/2022 DI ALIR). Esto aplica tanto a los activos en el país como a los que se encuentran en el exterior.

En el caso de Uruguay, rige el principio de territorialidad, por lo que solo se grava la renta y el patrimonio generados o ubicados dentro del país. Es decir que las criptomonedas no se gravan si estas se encuentran en el exterior. Ahora bien, si una persona física o jurídica uruguaya tuviera criptos en una empresa domiciliada en Uruguay, podrían estar alcanzadas por el impuesto al patrimonio, aunque no resulta claro cómo se evalúan ni cómo deberían declararse, ya que no existe una norma que las regule y la autoridad uruguaya (Dirección General Impositiva) no se expidió al respecto.

En el caso de Colombia, sí pueden estar alcanzadas por el impuesto. La Dirección de Impuestos y Aduanas Nacionales considera a las criptomonedas como activos intangibles, y deben incluirse en la declaración patrimonial si superan el mínimo sujeto a impuesto (alrededor de 830 mil dólares). En este caso, se valúan al costo de adquisición, en pesos colombianos, y a la tasa oficial.

Impuesto al valor agregado

A nivel regional, la venta de criptomonedas no se encuentra gravada con el IVA, aunque sí se gravan los servicios de intermediación a aquellas plataformas que cobran una comisión por facilitar la compra o venta de criptomonedas.

Tabla 1: IVA aplicado a criptoactivos, por país

País	Impuesto aplicado	Alícuota general	¿Aplica a intermediación cripto?
Argentina	IVA	21%	Sí
Brasil	ISS (municipal)	2% – 5%	Sí
México	IVA	16%	Sí
Colombia	IVA	19%	Sí
Chile	IVA	19%	Sí
Perú	IGV	18%	Sí
Uruguay	IVA	22%	Sí
Paraguay	IVA	10%	Sí
Bolivia	IVA	13%	Sí
Ecuador	IVA	12%	Sí
El Salvador	IVA	13%	No (salvo servicios no financieros)

Fuente: Elaboración propia en base a fuentes nacionales (HelloSafe, 2025)

7. Conclusiones

En el presente capítulo abordamos la complejidad de la fiscalidad internacional en el mercado de los criptoactivos. ¿De qué manera los Estados pueden regular un activo que se creó con el fin del anonimato, de generar una especie de moneda anárquica y de promover intercambios entre privados?

En este contexto, un repaso de las principales características de este tipo de instrumentos nos ayudó a pensar en las dificultades de las autoridades nacionales para avanzar en su regulación. El anonimato a través de sus operaciones, el alto grado de accesibilidad y flexibilidad, la existencia de riesgos por la falta de regulación y su volatilidad, así como las posibilidades de fraude y asociación con actividades ilícitas fueron algunos de los puntos analizados.

Los Estados, por su parte, con sus entramados legales formales, estructuras burocráticas y procesos legislativos extensos, operan como sistemas pesados, estancos y con tiempos de reacción lentos. En contraste, el ecosistema de criptoactivos —junto con las fintech y otros actores digitales emergentes— se caracteriza por su dinamismo, adaptabilidad y capacidad de mutar constantemente frente a nuevas regulaciones o restricciones.

Mientras los Estados intentan alcanzar y regular las operaciones cripto, varios años después de que las criptomonedas hayan surgido, los actores del ecosistema digital despliegan nuevas formas de encriptación, descentralización y herramientas tecnológicas que les permiten mantenerse un paso adelante.

En este marco, ponderamos como positivo el avance en la fiscalidad internacional, aunque, si bien representa aumentos en la recaudación y mayor justicia fiscal, aún queda trabajo por hacer en las modalidades que no operan con intermediarios, como las DeFi, que quedarán por fuera del alcance del marco de regulación nacional e internacional, y, por tanto, fuera del futuro intercambio de información de estas operaciones.

Sin perjuicio de lo anterior, la fiscalidad internacional consiste en una oportunidad clara de incremento de recaudación y progresividad, lo que apuntala una reducción de la brecha socioeconómica y de género. La demora en trazar estrategias de control específicas amplía las posibilidades de maniobras de evasión, elusión y planificación fiscal nociva, y genera un tratamiento impositivo desigual e inequitativo. Asimismo, la sencilla movilidad transfronteriza, sumada a su atractivo para ser utilizada por el crimen organizado transnacional como herramienta para el lavado de activos, deviene en la vital importancia de potenciar acciones de control y fiscalización.

Sin embargo, la efectividad de este tipo de herramientas dependerá no solo de su implementación técnica, sino también de la voluntad política de los Estados para coordinar globalmente, actualizar sus legislaciones y asumir una fiscalización más ágil, y proporcional y digitalmente competente.

En definitiva, la fiscalidad internacional se enfrenta a un reto que resulta tanto normativo como estructural. Si quedan países por fuera del estándar, continuarán existiendo oportunidades para ocultar información. Por tanto, el desafío radica en construir un

marco de cooperación internacional que sea completo, justo, eficaz y tecnológicamente actualizado, capaz de garantizar la integridad de los sistemas tributarios sin desalentar la innovación digital. Para ello, será clave avanzar en la cooperación multilateral, promover la transparencia y fortalecer las capacidades de fiscalización, especialmente en los países en desarrollo, que enfrentan mayores barreras técnicas para abordar estos nuevos escenarios, ya que hoy en día, al no haberse implementado todavía el intercambio, predomina la opacidad en este universo.

Bibliografía

Chainalysis. (2023). The 2023 Global Crypto Adoption Index. https://www.chainalysis.com/blog/2023-global-crypto-adoption-index/

Comisión Nacional Bancaria y de Valores (CNBV), Secretaría de Hacienda y Crédito Público (SHCP) y Banco de México (Banxico). (2017). Comunicado de prensa: Las autoridades financieras advierten de los riesgos asociados al uso de activos virtuales y a la participación en los esquemas de inversión conocidos como Oferta Inicial de Monedas o 'Initial Coin Offerings'. www.banxico.org.mx/publicaciones-y-prensa/miscelaneos/%7B6D5AAB8C-3BFA-0A8B-5EDD-7EDC04E1931C%7D.pdf

Grupo de Acción Financiera Internacional. (2015). *Directrices para un enfoque basado en riesgo: monedas virtuales*. FATF/OECD.

Grondona, V., Bidegain Ponte, N. y Rodríguez Enríquez, C. (2016). *Flujos financieros ilícitos que socavan la justicia de género*. Friedrich Ebert Stiftung.

Grondona, V. y Gervagi, A. (2024). Intercambio de información sobre criptoactivos con fines fiscales. En M. Burgos y S. Scasserra (coords.), *Criptomonedas. Un desafío al Estado y a los bancos*. Peña Lillo/Ediciones Continente/Callao Cooperativa Cultural.

HelloSafe. (2025). *Mapa exclusivo de la fiscalidad de las criptomonedas en el mundo*. https://hellosafe.com.mx/inversiones/criptomonedas/mapa-fiscalidad-mundo

Ley para regular las instituciones de tecnología financiera. (2018, 9 de marzo). *Diario Oficial de la Federación*. México.

https://www.cnbv.gob.mx/Normatividad/Ley%20para%20Regular%20las%20Instituciones%20de%20Tecnolog%C3%ADa%20Financiera.pdf

Méndez Santolaria, N. y Gervagi, A. (2022). *El sistema tributario argentino y propuestas para la construcción de un Sistema de Cuidados Integrado y Federal*. CIEPP.

Organización para la Cooperación y el Desarrollo Económicos (OCDE). (2022). *Crypto-Asset Reporting Framework and Amendments to the Common Reporting Standard*. OECD Publishing.

Proskalovich, R., Jack, C., Zarifis, A., Montes Serralde, D., Vershinina, P., Naidoo, S., Njoki, D., Pernice, I., Herrera, D. y Sarmiento, J. (2023). Cryptoasset *Ecosystem in Latin America and the Caribbean. Cambridge Centre for Alternative Finance*. www.jbs.cam.ac.uk/faculty-research/centres/alternative-finance/publications/cryptoasset-ecosystem-in-latin-america-and-the-caribbean/

Receita Federal do Brasil. (2019). Instrução Normativa RFB N.º 1888 (3 de mayo de 2019).

Rua, M. (2024). Criptomonedas y opacidad. En M. Burgos y S. Scasserra (coords.), *Criptomonedas. Un desafío al Estado y a los bancos*. Peña Lillo/Ediciones Continente/Callao Cooperativa Cultural.

Smink, V. (2025, 17 de febrero). 3 claves para entender el escándalo $LIBRA de Javier Milei, la promoción de una criptomoneda por parte del presidente argentino que terminó con pérdidas millonarias. *BBC News*.

Triple-A. (2024). The State of Global Cryptocurrency Ownership in 2024. *Triple-A*. https://www.hkdca.com/wp-content/uploads/2024/09/state-of-global-crytocurrency-ownership-2024-triplea.pdf

Zocaro, M. (2024). *Criptoactivos: Regímenes de Información en Argentina y a nivel internacional*. CEAT.

Abordaje del aspecto contable e impositivo de los criptoactivos

Jésica Nicol Luisi[1] y Martín Regalini[2]

Resumen

El presente trabajo aborda el tratamiento contable e impositivo de los criptoactivos en Argentina, analizando su evolución normativa, su encuadre jurídico y las implicancias fiscales derivadas de su utilización. En los últimos años, las criptomonedas y demás activos digitales adquirieron una creciente relevancia económica y financiera, generando nuevos desafíos para los organismos de control, la profesión contable y el sistema tributario.

A diferencia de otros activos tradicionales, los criptoactivos presentan características particulares vinculadas a su descentralización, volatilidad y funcionamiento mediante tecnología blockchain, lo que ha motivado distintas interpretaciones por parte de organismos como la UIF, el BCRA, la CNV y ARCA. En este contexto, resulta necesario analizar de qué manera deben reconocerse contablemente, cómo deben valuarse y cuál es el tratamiento tributario aplicable en impuestos como Ganancias, IVA y Bienes Personales.

1- Contadora Publica (UNR). Diplomada en Prevención del Lavado de Activos (UNER) y en Análisis Económico Forense (UNR). Desempeñándose actualmente en la Procuraduría de Criminalidad Económica y Lavado de Activos del Ministerio Publico Fiscal. Correo: luisijesica@gmail.com

2- Contador Público (UBA). Magister en Finanzas Corporativas (Di Tella). Profesor y tutor de la Diplomatura Especialización en Investigación Criminal de Delitos Económicos y Lavado de Activos (UNR). Subsecretario de la Corte Suprema (7 años). Especialista en delitos complejos y crimen organizado. Basta experiencia en el mundo privado, Auditor, Analists Contable, Jefe de Finanzas, experiencia en Control Interno, Lavado de Activos y Compliance. Correo: martinregalini@gmail.com

Asimismo, el trabajo examina los mecanismos de control e intercambio de información implementados por ARCA a través de distintos regímenes informativos, así como también las limitaciones existentes frente a operaciones realizadas mediante exchanges del exterior, billeteras de autocustodia y transacciones peer-to-peer. Finalmente, se desarrollan algunas zonas grises vinculadas al uso de criptoactivos en operaciones internacionales y su posible impacto en el régimen cambiario vigente, como así también la capacidad de acción por parte de las autoridades para el respectivo control, congelamiento y recupero de criptoactivos en caso de que se requiera.

1. Introducción

En nuestro país, la primera aproximación conceptual y regulatoria de las criptomonedas no provino de una única ley, sino de interpretaciones de organismos fiscales. Así obtuvimos la primera definición de la Unidad de Información Financiera (UIF) a partir de la Resolución 300/2014 (B.O. 10/07/2014).

Siguiendo lo estipulado por el Grupo de Acción Financiera Internacional, la UIF las definió (art. 2 de la Res. 300) como:

> "...la representación digital de valor que puede ser objeto de comercio digital y cuyas funciones son la de constituir un medio de intercambio, y/o una unidad de cuenta, y/o una reserva de valor, pero que no tienen curso legal, ni se emiten, ni se encuentran garantizadas por ningún país o jurisdicción. En este sentido las monedas virtuales se diferencian del dinero electrónico, que es un mecanismo para transferir digitalmente monedas fiduciarias, es decir, mediante el cual se transfieren electrónicamente monedas que tienen curso legal en algún país o jurisdicción".

Por su parte, el Banco Central de la República Argentina (BCRA), en mayo de 2014 emitió un comunicado afirmando que las monedas virtuales "no son emitidas por este Banco Central ni por otras autoridades monetarias internacionales, por ende, no tienen curso legal ni poseen respaldo alguno". A su vez, alertó por la volatilidad de su precio y los riesgos de operar con estos activos. Este comunicado no fue acompañado de una nueva definición oficial del término moneda virtual.

Posteriormente, el BCRA ha dictado algunas normas que mencionan, tímidamente, las expresiones monedas virtuales y criptoactivos.

El 04/12/2017 la Comisión Nacional de Valores (CNV) emitió un comunicado alertando a los inversores sobre los potenciales peligros de las ofertas iniciales (ICO) de monedas virtuales o tokens. En el comunicado la CNV sostiene que se denomina ICOs "a la forma digital de recaudar fondos del público a través de la oferta inicial de monedas virtuales o tokens, implementada sobre una cadena de bloques o blockchain". Y agrega que son inversiones especulativas de alto riesgo debido a la:

> "(a) falta de regulación específica, (b) volatilidad de precios y falta de liquidez, (c) potencial fraude, (d) inadecuado acceso a información relevante, (e) proyectos en etapa inicial, (f) fallas tecnológicas y de infraestructura y (g) carácter transnacional de las negociaciones con ICOs".

Y concluye que "solo debería invertir en ICOs un inversor experto, que está capacitado para analizar el proyecto financiado por la ICO y está preparado para perder, eventualmente, toda su inversión". Esta alerta fue la única declaración de la CNV sobre el tema hasta la fecha. De este texto, que ni siquiera es una norma, no se pueden extraer muchas conclusiones más allá de lo peligroso que pueden llegar a ser las ICO.

2. Tratamiento contable en Argentina

Las normas contables profesionales argentinas no dan una definición textual de qué es un activo, sino más bien definen cuándo se tiene uno. Particularmente, la Resolución Técnica (RT) N.º 16, que es el Marco Conceptual (MC) de las normas contables profesionales locales, indica:

> "Un ente tiene un activo cuando, debido a un hecho ya ocurrido, controla los beneficios económicos que produce un bien (material o inmaterial con valor de cambio o de uso para el ente)".

Además, agrega que un bien tiene valor de cambio cuando existe la posibilidad de canjearlo por efectivo o por otro activo, utilizarlo para cancelar una obligación o distribuirlo entre los propietarios del

ente. Y un bien tendrá valor de uso cuando el ente pueda emplearlo en una actividad productora de ingresos. Por último, la RT añade que

> "...en cualquier caso, se considera que un bien tiene valor para un ente cuando representa efectivo o equivalentes de efectivo o tiene aptitud para generar (por sí o en combinación con otros bienes) un flujo positivo de efectivo. De no cumplirse este requisito, no existe un activo para el ente en cuestión."

Analizando esta definición de activo que da el Marco Conceptual, y la de criptomoneda detallada anteriormente, se desprende que estamos ante un activo, específicamente, un activo digital. Y, sin dudas, la persona o ente que posea criptomonedas como consecuencia de "un hecho ya ocurrido" controla los beneficios económicos que el bien le otorga, ya sea porque las adquirió en una compra, en una operación de intercambio, o porque se obtuvieron como consecuencia de validar y registrar las transacciones de cadenas de bloques. Las criptomonedas pueden adquirirse principalmente por tres motivos:

- Medio de pago: servir como elemento de intercambio en operaciones de compra y venta de productos y servicios, el cual sería el fin original por el cual fueron creadas.
- Negocio: un ente puede tener como actividad principal la compra-venta de criptomonedas.
- Inversión: se puede tratar a las criptomonedas como un elemento de inversión (alto riesgo) con el que obtener un rendimiento en el futuro.

Entonces, a la hora de valuar las criptomonedas se pueden dar diversas situaciones, en las cuales el tratamiento contable puede variar de acuerdo al destino que cada sujeto u ente le dé a su tenencia:

2.1. Criptoactivos como medio de pago: Caja y Bancos

Un ente que utiliza bitcoin en el marco de su actividad comercial como medio para realizar cobros y pagos debería exponer su tenencia de bitcoin en el activo, dentro del rubro Caja y Bancos. Esto resulta evidente en aquellos países donde bitcoin tiene el status de moneda de curso legal (como El Salvador o República Centroafricana), pero también en países donde, a pesar de no serlo, las criptomonedas sí se erigen como medio de pago legalmente aceptado (es el caso de Brasil desde la sanción de la ley 14.478/2022).

2.2. Criptoactivos como inversión: rubro Inversiones

Un ente que mantiene tenencias de bitcoin con el objetivo de obtener rendimientos futuros por el aumento de su cotización debería exponer su tenencia de bitcoin en el activo, dentro del rubro Inversiones. Dado que bitcoin posee un precio de mercado, puede ser utilizado como un activo para inversión, al igual que las divisas, acciones, bonos, commodities, bienes muebles e inmuebles, o cualquier otro tipo de activo real o financiero. Esto ocurre en Estados Unidos, donde la empresa cotizante Microstrategy posee bitcoin como inversión a largo plazo y expone su tenencia como un activo digital no corriente.

2.3. Criptoactivos como actividad principal: rubro Bienes de Cambio

Un ente cuya actividad consiste en el intercambio de criptomonedas debería exponer su tenencia de bitcoin dentro del rubro Bienes de Cambio. Si la actividad de un ente consiste en realizar intercambios entre criptomonedas percibiendo comisiones por dichas transacciones (los denominados exchanges), podría exponer su tenencia dentro del rubro Bienes de Cambio, dado que dicha tenencia representa los bienes cuya compraventa les permite realizar su actividad principal y generar sus ingresos.

2.4. Criptoactivos recibidos como préstamo o depósito: Pasivo

Un ente que recibiera sumas en calidad de préstamo o depósito debería exponer dichas tenencias como un Pasivo. La tenencia de bitcoin recibido de terceros podría originarse en un préstamo pactado en dicha especie, o bien haber sido recibidos en calidad de depósito, para su custodia o administración. En tales casos, se deberían exponer estas tenencias como parte del pasivo del ente.

3. Tratamiento impositivo en Argentina

3.1. Impuesto a las Ganancias

La Agencia de Recaudación y Control Aduanero ha dispuesto que los resultados obtenidos producto de la enajenación de criptoactivos/monedas digitales constituyen ganancias alcanzadas por el impuesto.

La forma de declarar dichas ganancias y la alícuota a aplicar dependen de si quien las obtiene es una persona humana o sucesión indivisa no constituida como empresa o explotación unipersonal, o una persona jurídica y demás sujetos del artículo 53 de la ley.

Personas humanas y sucesiones indivisas no constituidas como empresas o explotaciones unipersonales

En este caso se trata de una renta de segunda categoría, cuyo tratamiento impositivo variará según sea de fuente argentina o extranjera. Frente a una renta de fuente argentina, resultará de aplicación el impuesto cedular comprendido en los incisos a)[3] y b) del artículo 98 de la ley, con alícuotas del 5% o 15% respectivamente, según se trate de la enajenación de criptoactivos/monedas digitales en pesos y sin cláusula de ajuste —inciso a)— o, en su defecto, de una operación de venta en moneda extranjera —inciso b)—.

En ambos casos, se admite el cómputo de la deducción especial que prevé el artículo 100, además de los costos de adquisición y gastos directa o indirectamente relacionados con las ganancias obtenidas. Si se trata de una renta de fuente extranjera, los resultados obtenidos estarán alcanzados a una alícuota del 15% en todos los casos.

Personas jurídicas y demás sujetos del artículo 53 de la ley

En este caso, las ganancias se encuentran gravadas a la tasa progresiva que prevé el artículo 73 de la ley del tributo, la que dependerá de la ganancia neta imponible acumulada del período fiscal que se trate.

3.2. Impuesto al Valor Agregado (IVA)

La venta de criptoactivos no se encuentra gravada. El IVA alcanza a la venta de cosas muebles, y los criptoactivos al ser bienes digitales, su venta no se encuentra gravada por el tributo. No obstante, la prestación del servicio de intermediación en la compraventa de criptoactivos

3- Según lo dispuesto por el artículo 245 del Decreto Reglamentario de la Ley del Impuesto a las Ganancias (t.o. en 2019).

por el cual se cobre una contraprestación, ya sea en moneda fiduciaria, en especie o en criptoactivos, sí se encuentra gravada por el IVA.

3.3. Impuesto sobre los Bienes Personales

A través del Dictamen N.º 2/2022 DI ALIR, la Agencia de Recaudación y Control Aduanero expresó su opinión jurídica a través de la cual considera que los criptoactivos se encuentran gravados en el Impuesto sobre los Bienes Personales de acuerdo a lo previsto en el inciso j) del artículo 19 de la Ley N.º 23.966 (t.o. en 1997 y sus modificaciones). Es decir, los asemeja a los títulos, las acciones, cuotas o participaciones sociales y otros títulos valores representativos de capital social o equivalente, emitidos por entes públicos o privados.

Mediante el mismo, se estableció que los criptoactivos deben valuarse al 31/12 de cada año conforme lo expuesto en el inciso h) del artículo 22 de la ley del impuesto, esto es, a su costo de adquisición, incrementado en el importe de los intereses, actualizaciones y diferencias de cambio que se hubieran devengado hasta dicha fecha.

La declaración se realiza desde el servicio de clave fiscal "Bienes Personales web", seleccionando el tipo de bien "Monedas digitales, monedas virtuales, criptoactivos o similares".

4. Control de información ARCA

El análisis de criptoactivos no constituye un universo separado, sino una extensión del circuito económico-financiero tradicional, susceptible de reconstrucción, valuación y verificación en términos patrimoniales.

El régimen informativo establecido por la ex-AFIP mediante las Resoluciones Generales 4614/2019, 4647/2019, 5029/2021, 5348/2023 y 5512/2024 permite acceder a información detallada sobre operaciones con criptoactivos en plataformas locales, constituyendo una fuente relevante para la reconstrucción patrimonial, aunque con limitaciones respecto de operatorias desarrolladas en exchanges del exterior o en esquemas de autocustodia.

Estas resoluciones permiten justificar cruces fiscales, detectar omisiones en declaraciones juradas, cuantificar tenencias, reconstruir flujos locales, acceder a información de exchanges locales y detectar inconsistencias.

Algunas actualizaciones dentro de las resoluciones de ARCA se refieren a los saldos en criptoactivos que, a través de la RG 5804/2025, deben informarse convertidos a pesos al cierre del mes, obligando a los exchanges a valuar criptoactivos mensualmente e informar saldos por usuario, con el fin de tener una foto mensual del patrimonio cripto.

A través de las distintas resoluciones, aún no se cubre completamente operatorias y entrecruzamiento de datos en relación a: wallets autocustodiadas; información de exchanges foráneas; y operaciones P2P.

5. "Zonas grises" en el uso de criptoactivos

El uso de cripto como medio de pago en exportaciones puede funcionar como mecanismo de elusión del régimen cambiario, porque permite no ingresar divisas, mantener activos fuera del sistema y diferir liquidación.

En ausencia de una regulación específica del BCRA sobre la percepción de ingresos en criptoactivos en el marco de exportaciones de servicios, dichos cobros deben ser reconocidos y valuados en moneda local a efectos contables e impositivos. No obstante, desde una perspectiva sustancial, su utilización como medio de pago puede generar tensiones con el régimen cambiario vigente, en tanto podría implicar la no canalización de ingresos equivalentes a divisas a través del mercado de cambios.

La utilización de criptomonedas como medio de pago en operaciones internacionales no elimina la existencia de un ingreso económico, sino que modifica el canal de percepción, pudiendo generar tensiones con el régimen cambiario vigente, sin afectar la obligación de registración contable ni la potencial relevancia fiscal de la operación.

Debe reconocerse en dicha operatoria: la existencia de valor económico equivalente a divisas, su tratamiento como operación internacional, y la posibilidad de existencia de una obligación de liquidación en el mercado cambiario.

6. Recupero y congelamiento de criptoactivos

En relación a contar con una guía detallada para el debido proceso de obtención de datos referidos al recupero y congelamiento de criptoactivos, es necesario contar con la siguiente información pormenorizada:

6.1. Identificación de las personas requeridas

Es fundamental identificar inicialmente a las personas requeridas: nombre, apellido, documento de identidad, nacionalidad, CUIT o CUIL, en caso que corresponda.

6.2. Delimitación temporal

Delimitar un tiempo determinado de relevamiento y control donde se pueda circunscribir, ante la necesidad de cumplimiento, el detalle fehaciente de los movimientos y tenencias que se necesiten analizar.

6.3. Levantamiento de secretos fiscal, bancario y bursátil

En caso de requerir detalles de tenencias personales a través de organismos autárquicos o de control, deberá solicitarse el levantamiento del secreto fiscal, bancario y bursátil de aquellas personas identificadas anteriormente, para darle visibilidad a la información que se encuentra amparada a la protección de datos de las personas.

6.4. Documentación a solicitar a entidades vinculadas

Se debe solicitar documentación a las entidades vinculadas al control y tenencia de los criptoactivos:

- Exchanges y Wallets: a través de la Comisión Nacional de Valores (CNV), en el marco de la Ley N.º 27.739, quien es el organismo encargado de regular a los Proveedores de Servicios de Activos Virtuales (PSAVs). Enmarca en la actualidad a 82 entidades que disponen de información integral relacionada a tenencias, movimientos comerciales, operaciones durante un periodo de tiempo, transacciones operadas por las personas requeridas tanto en la misma plataforma como con otras, incluyendo tenencias de criptoactivos a distintos momentos del tiempo, datos personales asociados a las cuentas y direcciones IP utilizadas.

- Información personal y de terceros a través de ARCA: en relación a las declaraciones juradas (tanto de impuesto a las ganancias, impuesto a los bienes personales, o cedular, entre otros) a las cuales se haya encontrado obligado a declarar, como así también lo detallado vinculado a las obligadas a informar a través de regímenes de información obligatorio para las propias exchanges y wallets locales.
- Banco Central de la República Argentina (BCRA): en caso de que la propia documentación adquirida de los organismos y proveedores virtuales requeridos anteriormente sea insuficiente, es posible solicitar una Comunicación "D" relacionada a obtener detalle de billeteras virtuales como cuentas bancarias relacionadas a la persona requerida, toda vez que existiesen movimientos de fondos destinados a adquirir o vender criptoactivos de manera directa (transferencias P2P, peer-to-peer) durante el plazo establecido.

6.5. Medidas cautelares para el congelamiento e inhibición

Evaluar, en caso de requerir y necesitar, medidas cautelares para su debido congelamiento e inhibición de los criptoactivos previamente relevados, siempre y cuando los mismos estuvieran ante el riesgo de ser transferidos o liquidados. Siguiendo ese objetivo, es importante traer a colación la Guía elaborada por la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público Fiscal, en la que se establecen una serie de lineamientos a seguir para la incautación de criptoactivos en el marco de investigaciones judiciales.

Lo nombrado debe realizarse mediante un procedimiento cuidadoso y planificado, ya que, a diferencia del dinero tradicional, los activos digitales permanecen protegidos por claves privadas o "semillas". Por ese motivo, si una persona obtiene acceso a esas claves, puede disponer de los fondos de forma remota aun cuando los dispositivos físicos hayan sido secuestrados.

Medidas preventivas previas al operativo

Antes de cualquier operativo deben adoptarse medidas preventivas. Las autoridades encargadas de la investigación tienen que contar

previamente con los recursos técnicos adecuados y con las autorizaciones judiciales correspondientes para poder realizar el secuestro de los activos. Además, se recomienda actuar rápidamente, debido a que los criptoactivos pueden transferirse en cuestión de segundos hacia otras direcciones digitales, dificultando su recuperación posterior.

Selección de la billetera virtual para resguardo

Una vez tomada la decisión de avanzar con la incautación, el primer paso consiste en seleccionar la billetera virtual que se utilizará para recibir y resguardar los fondos. Se debe tener en cuenta que existen miles de criptoactivos distintos y que no todas las billeteras son compatibles con todos ellos, por lo que previamente debe analizarse qué herramientas son aptas para cada caso concreto. Se recomienda utilizar billeteras de software que permitan implementar sistemas de firma múltiple y cifrado, lo que significa que para mover los fondos será necesaria la autorización de más de una persona, agregando una capa adicional de seguridad.

Creación de la billetera de resguardo

El segundo paso es la creación de la billetera destinada al resguardo de los activos incautados. Para ello, se genera una nueva billetera a partir de una "frase semilla", que funciona como mecanismo de recuperación y acceso a los fondos. Esa información debe almacenarse en un lugar seguro y protegido contra terceros. Luego se generan las direcciones públicas correspondientes para cada tipo de criptoactivo que se pretende recibir. Los activos no se almacenan físicamente dentro del dispositivo o programa utilizado, sino que permanecen registrados en la blockchain.

Transferencia de los fondos

Los investigadores deben verificar e importar las claves privadas o semillas obtenidas durante la investigación para comprobar el

contenido y balance de las billeteras vinculadas al sospechoso. Una vez corroborada la existencia de los activos, se procede a transferir la totalidad de los fondos hacia la dirección pública creada para su resguardo oficial.

Documentación del procedimiento

Es de suma importancia documentar minuciosamente todo el procedimiento realizado. Se recomienda verificar en la blockchain que la transferencia se haya efectuado correctamente y conservar evidencia mediante capturas de pantalla, fotografías, actas e identificadores de transacción. También deben registrarse datos relevantes como las direcciones involucradas, las claves privadas, las semillas utilizadas, el tipo de criptoactivo y los balances existentes al momento de la incautación. Además, la billetera debe contar con copias de seguridad, ya sea en papel o en soportes digitales, evitando siempre que terceros puedan acceder a dicha información.

Bibliografía

Administración Federal de Ingresos Públicos. (2019). Resolución General N.º 4614/2019. Argentina.

Administración Federal de Ingresos Públicos. (2019). Resolución General N.º 4647/2019. Argentina.

Administración Federal de Ingresos Públicos. (2021). Resolución General N.º 5029/2021. Argentina.

Administración Federal de Ingresos Públicos. (2023). Resolución General N.º 5348/2023. Argentina.

Agencia de Recaudación y Control Aduanero. (16 de junio de 2022). Impuesto sobre los bienes personales. Criptomonedas. Naturaleza jurídica. Gravabilidad. Su tratamiento [Dictamen N.º 2/2022 DI ALIR]. Argentina.

Agencia de Recaudación y Control Aduanero. (2024). Resolución General N.º 5512/2024. Argentina.

Agencia de Recaudación y Control Aduanero. (2025). Resolución General N.º 5804/2025. Argentina.

Boletín Oficial de la República Argentina. (15 de abril de 1997). Impuesto sobre los bienes personales – Título VI (texto ordenado por Decreto N.º 281/97). Argentina.
Boletín Oficial de la República Argentina. (5 de diciembre de 2019). Ley de Impuesto a las Ganancias (Ley N.º 20.628). Argentina.
Comisión Nacional de Valores. (2024). Resolución General N.º 994. Argentina.
Comisión Nacional de Valores. (2025). Resolución General N.º 1058. Argentina.
Federación Argentina de Consejos Profesionales de Ciencias Económicas. (8 de diciembre de 2000). Resolución Técnica N.º 16: Marco Conceptual de las normas contables profesionales.
GAFILAT. (2021). Guía sobre aspectos relevantes y pasos apropiados para la investigación, identificación, incautación y decomiso de activos virtuales.
INTERPOL. (2021). Guía destinada a los equipos de primera intervención en análisis forense digital.
Unidad de Información Financiera. (4 de julio de 2014). Resolución N.º 300/2014. Buenos Aires, Argentina.

Stablecoins bajo la lupa: concepto, clasificación y el nuevo orden regulatorio internacional

Augusto Lombardo[1] y Nicolás Maletti[2]

Resumen

El presente trabajo se enmarca en el estudio de las stablecoins y su regulación en el derecho comparado, dada la falta de normativa legal en nuestro ordenamiento jurídico. Para ello, se explora la temática desde dos ejes: por un lado, la taxonomía técnica y operativa de estos activos, y por el otro, el complejo escenario regulatorio global.

1. Stablecoins

1.1. Concepto

El Banco Central Europeo publicó en el año 2019 un artículo llamado "En busca de estabilidad en los criptoactivos: ¿Son las stablecoins la solución?"; dentro del mismo se ensaya una definición de stablecoins como aquellas "unidades digitales de valor que no son una forma de ninguna moneda específica, sino que se basan en un conjunto de

1- Lombardo, Augusto. Abogado y escribano. Mediador. Diplomado en Análisis Económico Forense. Docente del Instituto de Seguridad Pública, sede Rosario. Trabaja en el Ministerio Público de la Acusación de la Prov. de Santa Fe desde 2014. Correo: augustolombardo45@gmail.com
2- Maletti, Nicolás. Abogado (UNR). Diplomado en Análisis Económico Forense. Especialización en Derecho Penal (UBA), en curso. Certificación en Crypto Compliance (UMSA). Trabaja en el Ministerio Público de la Acusación de la Prov. de Santa Fe, UF Villa Gobernador Gálvez. Correo: nicolasmaletti@gmail.com

herramientas de estabilización que, supuestamente, minimizan las fluctuaciones de su precio en dicha(s) moneda(s)" (Bullmann, 2019).

Considerando que en el año de publicación se trataba de abordar un concepto vanguardista, asumimos que este es demasiado amplio y resulta anticuado en la realidad de hoy. La palabra stablecoin es un anglicismo, como tantos otros, utilizado en el mundo cripto. Al traducirla literalmente, revela bastante: se trata de criptomonedas cuyo objetivo es mantener un precio estable.

Cabe destacar que existen muchas otras definiciones de moneda estable. Tomaino, en el año 2017, las conceptualizó como una "criptomoneda que tiene características de precio estable". Autores como Mita, Ito y Ohsawa profundizaron en esta noción, analizándolas no solo por su estabilidad sino por su potencial técnico como sistemas de pago descentralizados, definiéndola como "una moneda digital vinculada a otro activo estable como el oro, o las principales monedas fiduciarias como el euro, libra esterlina o el dólar estadounidense" (Makiko, 2020, 49).

Un trabajo reciente publicado por el World Economic Forum la conceptualiza como un tipo de criptomoneda vinculada a un activo de reserva específico. Al estar vinculadas a un activo real, las stablecoins pueden mantener un valor más estable, por lo que ofrecen un medio de intercambio más fiable que otras criptomonedas volátiles[3]. Así, además de haber sido creadas para minimizar la volatilidad, buscan adicionalmente contribuir a la creación de un entorno de mercado más consistente y fiable que impulse la adopción de activos digitales de forma global.

Considerando este recorrido conceptual, se propone la siguiente síntesis que logre capturar la complejidad del fenómeno a los fines de esta investigación: tipo de criptomoneda diseñada para tener un valor fijo y estable, generalmente vinculado al precio de una moneda fiduciaria (dólar, euro, etc.) o a un activo (materia prima).

1.2. Nacimiento y realidad de las stablecoins

Nacidas ante la necesidad de estabilizar el valor de las criptomonedas frente a ciclos de alta volatilidad que dificultaban su adopción de forma generalizada y cotidiana, las stablecoins experimentaron

3- World Economic Forum. (2025). https://es.weforum.org/stories/2025/04/stablecoins-por-que-las-criptomonedas-respaldadas-por-reservas-estan-en-auge/

un notable crecimiento en los últimos años. Al tener un anclaje en el mundo real y una paridad ya sea con el dólar, el oro o el euro, las monedas estables fueron expresamente diseñadas para conseguir la estabilidad de su precio; por ello han ganado su lugar en el mundo cripto. Si bien en un inicio fueron utilizadas especialmente por traders y exchanges como puente desde criptomonedas volátiles —como BTC o ETH— hacia un activo digital estable dentro del propio ecosistema, su uso se extendió y comenzaron a adoptarse también como reserva de valor (sobre todo en países con alta inflación), envío de remesas, medio de pago en transacciones internacionales, finanzas descentralizadas (DeFi) y operaciones cotidianas.

En 2014, Vitalik Buterin lanzó Ethereum, la blockchain donde se crearon las primeras monedas que traemos al estudio en este trabajo, siendo la pionera BitUSD, una stablecoin algorítmica respaldada por el propio token. La segunda lanzada al mercado ese mismo año fue NuBits, también de tipo algorítmica y que, aunque al principio contó con cierto éxito, con el correr de los años perdió la paridad con el dólar. En octubre del mismo año se lanzó Tether, moneda estable centralizada. Para comprender su naturaleza, resulta fundamental remitirse a su propia concepción institucional: Tether se define a sí misma como una plataforma basada en blockchain diseñada para facilitar el uso de monedas fiduciarias de forma digital[4].

Fue la primera stablecoin en usar el modelo de respaldo 1:1 con el dinero fiduciario (dólar): por cada token de USDT emitido, hay un dólar físico o un bono del tesoro estadounidense en una reserva bancaria. Si bien, al igual que Bitcoin, cuenta con un White Paper[5], el mismo se ha ido actualizando en sus términos de servicio, debido a que sus reservas han cambiado respecto de lo que decía el White Paper original.

Debido a que este modelo resulta menos enmarañado en cuanto al respaldo que el modelo algorítmico, Tether terminó dominando el mercado de las monedas estables. El domicilio de origen de Tether desde el momento de su creación hasta principios del año 2025 fue Hong Kong, desde donde se alejó debido a la presión regulatoria de China, país que siempre presentó obstáculos no solo para las stablecoins sino también para las criptomonedas en

4- Véase: https://tether.to/es/
5- Tether White Paper (2014/2016).

general. A principios de 2025, Tether trasladó su base principal de operaciones a El Salvador, país con leyes pro-cripto (donde Bitcoin es moneda de curso legal), buscando de esa forma apartarse de zonas con controles más severos.

Actualmente Tether es el "rey" de las stablecoins, siendo una pieza fundamental del ecosistema cripto, puesto que fue el primero en ofrecer una solución real a la demanda de dólares digitales en la blockchain.

Otra moneda estable a referir es DAI[6], que nació a fines del año 2017, descentralizada, lanzada por la organización MakerDAO[7]. Debido a cuestiones operacionales, en el año 2024 el ecosistema MakerDAO se transformó en Sky[8], a fines de eliminar falencias y ajustarse a las nuevas reglamentaciones. Este proceso no fue solo un cambio de nombre, sino que implicó una migración tecnológica y económica: la moneda estable DAI comenzó a migrar hacia USDS (Sky Dollar).

El término DAO proviene de las siglas en inglés Decentralized, Autonomous, Organization. Podría afirmarse que una DAO es una democracia digital pura, puesto que los tres pilares que la definen son: organización, en tanto se unen un grupo de personas con un objetivo común; autonomía, ya que funciona mediante contratos inteligentes que se ejecutan cuando se cumplen ciertas condiciones; y descentralidad, dado que no hay una autoridad central que tome decisiones, sino que estas se adoptan en base a los tokens de gobernanza que poseen sus miembros.

Es preciso subrayar la relevancia de la moneda estable USDC. Años posteriores al lanzamiento de Tether, cuando ya existía cierto consenso acerca de las monedas estables, Circle —una empresa estadounidense de Boston que en el año 2013 se dedicaba al intercambio de bitcoins (exchange) y a intermediar en pagos móviles (Circle Pay)— se asoció con Coinbase (el mayor exchange de criptomonedas estadounidense) en el año 2018, y juntas crearon y lanzaron la moneda. Este movimiento estratégico llevó orden, regulación y transparencia a un mercado de stablecoins que, para esos años, estaba dominado casi exclusivamente por Tether (USDT). Independientemente del dominio

6- DAI Whitepaper. https://makerdao.com/en/whitepaper/sai/
7- MakerDAO. https://docs.makerdao.com/
8- Sky (ex MakerDAO). https://makerdao.com/en/whitepaper

innegable de Tether, esta enfrentaba múltiples críticas —y posteriores demandas judiciales— por su falta de auditorías claras.

Esta flaqueza fue advertida por Circle y Coinbase, y para ganar la confianza de las instituciones financieras y los usuarios, contrataron a la firma de contabilidad Grant Thornton LLP para realizar certificaciones mensuales de sus reservas. Esto permitía a cualquier usuario verificar que, si había un millón de USDC en circulación, realmente existían los mismos bajo custodia de la empresa.

Desde el minuto cero, USDC se estructuró legalmente para evitar los problemas de Tether, por lo que se la conoce como la "stablecoin institucional", posicionándose como una opción segura para empresas, fondos de inversión y usuarios que buscaban cumplir con las leyes de Estados Unidos. Hoy se posiciona como la segunda moneda estable de mayor capitalización (detrás de la pionera Tether) y pieza fundamental de la estrategia cripto de Estados Unidos para competir con otras monedas digitales. Sin embargo, esta moneda estable también atravesó sobresaltos: en el año 2023, a raíz de la quiebra del Silicon Valley Bank, el token perdió su paridad 1:1 con el dólar estadounidense y llegó a cotizar en un mínimo histórico cercano a los 0,87-0,88 centavos de dólar. Esto se dio debido a que, luego del colapso del Silicon Valley Bank, la empresa emisora de USDC (Circle) reveló públicamente que tenía depositados dólares en efectivo que representaban aproximadamente el 8% del total de las reservas que respaldaban la stablecoin en ese momento.

Resulta imperativo destacar que la pandemia de COVID-19 actuó como catalizador determinante para la adopción masiva de estas monedas, acelerando su expansión desde nichos del mercado cripto hacia otros mercados. De allí su relevancia en la economía mundial: han acercado a millones de personas a la inclusión financiera, ya que resultan altamente atractivas para residentes de países golpeados por alta inflación (Argentina, Turquía, Venezuela, etc.), monedas débiles o volátiles, y bancos inestables o con controles de capitales desmedidos. El dinero se transfiere a través de internet por fuera del sistema bancario, lo que las hace mucho más eficientes que el sistema SWIFT (que tarda más y cobra mayores comisiones), siendo seductoras para el envío de remesas y pagos transfronterizos.

Es necesario, antes de analizar los distintos tipos de stablecoins, volcar los siguientes datos fácticos que apuntalan lo ya mencionado.

Navegando por la página web de CoinMarketCap[9], observamos que, entre los primeros veinte criptoactivos de mayor capitalización del mercado, se encuentran cinco pertenecientes al tema que nos ocupa. El listado está conformado por Tether (USDT), que ocupa el tercer lugar; en el puesto sexto encontramos a USDC; en el decimoquinto lugar se sitúa Ethena (USDe); en la posición diecisiete, DAI; y en el escalón veinte, World Liberty Financial con su moneda estable USD1.

Hoy, tras Bitcoin y Ethereum, la tercera criptomoneda por capitalización de mercado es Tether, figurando también USDC entre las diez primeras. Si se amplía el análisis a las veinte principales, aparecen USDe, DAI y USD1. Del total de las veinte criptomonedas más capitalizadas, cinco están vinculadas al dólar, lo que representa el 25% de ese grupo y refleja con claridad la madurez que alcanzó el ecosistema de stablecoins.

1.3. Clasificación

Existen diversas clasificaciones de monedas estables. Algunos autores, por ejemplo, las dividen en dos grandes categorías según cómo gestionan sus reservas. Las custodiadas dependen de un emisor centralizado que mantiene los activos de respaldo fuera de la blockchain; Tether, USDC y las stablecoins respaldadas por oro son ejemplos de este modelo. Las no custodiadas, en cambio, utilizan contratos inteligentes para administrar las reservas directamente en la cadena de bloques, sin intervención de un intermediario centralizado, siendo DAI el ejemplo más representativo.

Dirk Bullmann, un experto en la materia vinculado al Banco Central Europeo (BCE), refiere a tres dimensiones de las monedas estables: la existencia o ausencia de un emisor responsable de satisfacer cualquier reclamación asociada, la descentralización o centralización de responsabilidades en la iniciativa de las monedas estables, y los fundamentos de valor de una moneda estable en relación con su moneda de referencia (Bullmann, 2019, 9).

Pasemos ahora a la clasificación más útil para entender cómo funcionan las stablecoins: aquella basada en el mecanismo de estabilización que cada una emplea para mantener su valor fijo. Estos mecanismos varían según el tipo de activo que el emisor utiliza como

9- https://coinmarketcap.com/

reserva para respaldar sus emisiones. Bajo este criterio, se agrupan en cuatro categorías: las respaldadas por dinero fiat, las respaldadas por otros activos, las respaldadas por criptoactivos y las algorítmicas.

1. Respaldo con dinero fiat

Son aquellas que están colateralizadas con activos respaldados 1:1 por dinero fiduciario o instrumentos de deuda soberana (bonos del Tesoro estadounidense a corto plazo) bajo custodia bancaria. Esta modalidad es la más relevante de las stablecoins, atento al número de unidades emitidas dentro de esta clasificación y a la capitalización de mercado de ellas. Vale aclarar que el gran porcentaje de las monedas estables que componen esta categoría se respaldan con el dólar.

Entre las monedas estables más conocidas dentro de esta categorización encontramos a Tether, con su token USDT, y a USD Coin, con su token USDC, ambas con respecto al colateral dólar. Con respecto al colateral euro, encontramos a Celo Euro, con su moneda cEUR, y a EURS, que pertenece a STASIS EURO. Por su parte, las empresas Circle y Coinbase, además de su token USDC respaldado por el dólar, recientemente comenzaron a incursionar en el mercado europeo con el token EURC, ganándole una amplia cuota de mercado a la moneda estable EURT de Tether, la cual fue perdiendo capitalización debido a las barreras regulatorias introducidas por la Ley MiCA.

Asimismo, existen monedas estables respaldadas por el peso argentino, conocidas popularmente como "criptopesos": wARS, token que pertenece al exchange de criptomonedas Ripio, y ARST (Stellar), de la fintech Bitera.

Otra variante de criptopesos es nARS, lanzada en el año 2021 por Num Finance; su nombre proviene de la palabra "numum", que significa "moneda" en latín. La diferencia de este criptopeso con las monedas estables nombradas anteriormente radica en su respaldo, debido a que este no es ciento por ciento en pesos argentinos depositados en un banco, sino mixto, teniendo un gran porcentaje de respaldo en otras monedas estables como USDT y USDC, en pesos argentinos en un banco y en activos digitales que operan dentro de protocolos de finanzas descentralizadas (DeFi).

Todas las empresas que emiten estos tipos de monedas estables tendrían -en teoría- que tener sus reservas verificadas frecuentemente por auditores externos. Resulta imperativo destacar que, aunque el

ecosistema cuenta con un catálogo de aproximadamente ciento cincuenta monedas estables en funcionamiento, el mercado presenta una hiperconcentración en apenas una decena de protocolos, los cuales acaparan más del 90% de la capitalización total. Esta asimetría demuestra que, en el ámbito de las stablecoins, la confianza institucional y la liquidez son factores más determinantes que la mera proliferación tecnológica.

La posición hegemónica de USDT, cuya cuota de mercado supera el 60% del volumen total en circulación, da cuenta de una marcada concentración de liquidez, lo que no solo la convierte en la infraestructura vertebral de las monedas estables, sino que obliga a examinar con detenimiento ciertos aspectos institucionales de la compañía Tether.

El negocio de Tether es bien simple. Su producto estrella, USDT, es una criptomoneda estable atada al dólar: un "dólar digital". Tether imprime dólares digitales, recibe dólares reales a cambio y los invierte. Hoy existen alrededor de 190 mil millones de USDT, respaldados principalmente por bonos del Tesoro americano, oro, bitcoin y otros activos de la economía real.

El sistema bancario le dio la espalda durante muchos años a la industria cripto. Eso permitió que USDT se convirtiera en la moneda para mover dinero dentro del ecosistema. Y como ningún banco quería trabajar con cripto, se transformó en la forma de cargar dólares, tener dólares y enviar dólares. Su valor no reside en el rendimiento, sino en su red global y su liquidez: hace pocos años era impensable poder hacer una transferencia internacional inmediata, casi sin costos y sin pedirle permiso a ningún banco.

2. Respaldadas por activos

Esta categoría incluye monedas estables respaldadas por activos que se encuentran fuera de la cadena de bloques. Esos activos cuentan con un valor comercial innato y son fácilmente intercambiables, es decir, cuentan con gran liquidez en el mercado. Así, encontramos stablecoins respaldadas por oro, siendo esta la categoría más sólida fuera de las monedas nacionales. Su valor no depende de la confianza en un banco central, sino de la propia escasez física del metal. Su funcionamiento es muy simple: el token replica una onza de oro físico real, el cual se custodia en bóvedas de alta seguridad a cargo de la empresa que comercializa el token.

PAXG es emitido por Paxos Trust Company[10], institución financiera regulada por el Departamento de Servicios Financieros del Estado de Nueva York, y cada token emitido representa una onza troy de una barra de oro London Good Delivery. Otro ejemplo es la stablecoin Tether Gold (XAUt), que replica el valor de una onza troy, respaldando la emisión del token con oro físico bajo custodia de Tether.

La ventaja es indiscutible: tienen la estabilidad del oro con la liquidez de una cripto, pudiendo transferir "oro" a cualquier parte del mundo en segundos.

En esta categoría encontramos un experimento fallido: PETRO (PTR), en Venezuela. En el año 2018, el presidente Nicolás Maduro creó y colocó en circulación el activo, el cual era respaldado por las reservas de petróleo, oro, gas y diamantes de Venezuela, y que dejó de cotizar en el año 2024.

En Argentina, la empresa Agrotoken[11] fue pionera mundial en la creación de una stablecoin que tiene su valor anclado al precio de una tonelada de granos. Estas monedas están respaldadas por granos físicos depositados en acopios reales y, para que esto sea legal y seguro, usan un sistema llamado PoGR (Proof of Grain Reserve) o "prueba de reserva de granos". Esta herramienta funciona de la siguiente manera: el productor agropecuario entrega su cosecha a un acopio autorizado, el acopiador confirma que los granos se encuentran en sus depósitos emitiendo un token digital en la blockchain. Si el productor vende el token, los granos se "queman" (se liberan) para que no haya más tokens que granos reales. El valor del token sigue el precio de los granos en tiempo real y el productor mantiene su poder adquisitivo ante la suba de los commodities.

Los usos más comunes de este token son el pago de insumos (compra de maquinaria, semillas, fertilizantes, etc.) y la toma de préstamos bancarios con garantía.

3. Respaldadas por cripto

Las monedas respaldadas por una reserva sobrecolateralizada de otras criptomonedas consiguen la estabilidad del valor a partir de un contrato inteligente que permite a los tenedores alterar el colateral

10- https://www.paxos.com/
11- https://landing.agrotoken.oaro.net/

depositado de manera automática, en caso de que se altere el ratio de colateralización.

En este caso no se cuenta con una empresa privada que emite, recibe y guarda en una bóveda. Existe un contrato inteligente donde se deposita una cantidad determinada de criptomonedas que se bloquean; luego, el contrato inteligente emite una cantidad de moneda estable (porcentaje inferior a lo depositado) y la entrega al depositario.

El problema surge cuando la criptomoneda dejada como colateral comienza a mermar en su cotización (algo más que común). Ante esta coyuntura existen algunas alternativas: la primera es no actuar; ante la baja repentina o paulatina de la moneda bloqueada como colateral y la pérdida del ratio de colateralización, el smart contract liquidará el activo, cobrará la deuda más los intereses correspondientes y, en caso de existir sobrante de colateral, este pertenecerá al depositario, quien podrá retirarlo. Otro camino posible es inyectar más colateral al smart contract, para robustecer la posición y evitar ser liquidado. Por último, se puede cancelar un porcentaje del préstamo contraído, mejorando de esta forma el ratio de colateralización.

Si bien existen varias stablecoins dentro de esta clasificación, la más conocida e importante por su cuota de mercado es DAI. En este caso, mayormente se utiliza Ethereum; el ratio de colateralización es aproximadamente del 150%, es decir, si se solicitan al smart contract 100 monedas estables de DAI (que replican el valor de un dólar), se requiere dejar como colateral la fracción de ETH equivalente a 150 dólares. Algo novedoso es que se puede solicitar DAI bloqueando USDC o USDT; en ese caso, como también son monedas estables pero respaldadas por dinero fiat, el ratio es 1:1. También se puede colateralizar con la criptomoneda LINK y con bonos del Tesoro de EE.UU., créditos comerciales, etc.

Si bien DAI fue la primera de esta clase de monedas, no es la única. LUSD se puede obtener con respaldo únicamente en Ethereum, y su ventaja es que el ratio de colateralización es muy bajo (110%), es decir, por cada 110 dólares de ETH se pueden obtener 100 dólares de LUSD. Otra es GHO, lanzada por Aave (protocolo de liquidez descentralizado), que utiliza como respaldo cualquier criptomoneda que ya se tenga depositada en Aave.

4. Respaldadas en algoritmos

Nos sumergimos en la clasificación más controversial: las stablecoins algorítmicas son una categoría fascinante —y a veces peligrosa— que en alguna oportunidad ha hecho temblar al mundo cripto.

Son monedas estables descentralizadas que no están respaldadas por ningún otro activo; su estabilidad depende de una combinación compleja de algoritmos y contratos inteligentes para mantener el precio fijo. Es decir, su estabilidad depende de matemáticas, incentivos de mercado y código.

Ante un aumento de la demanda de la moneda estable, el algoritmo crea nuevas monedas, lo que hace que el precio baje. En caso de que la moneda esté perdiendo la paridad (peg) de 1:1 porque está bajando de precio, el algoritmo, en este caso, compra monedas estables para reducir la oferta, haciendo que la moneda suba de precio. Hasta aquí, un juego simple de oferta y demanda donde el trabajo del algoritmo es ampliar o contraer la oferta de la moneda en función de su precio.

Robert Sams[12], conocido como el padre de las criptomonedas algorítmicas, introdujo el concepto de acciones de señoreaje en el año 2014. Este documento fue en un primer momento muy elogiado por su enfoque descentralizado, pero con el correr de los años, y debido a diversos proyectos fallidos que replicaron su teoría, fue perdiendo popularidad entre la comunidad cripto.

El mismo año se creó NuBits, que introdujo monedas algorítmicas. ¿Pero qué pasó con ella? Esta stablecoin se regía por el controvertido sistema de señoreaje, que finalmente provocó que perdiera el 94% de su valor.

Al hablar de esta clasificación de monedas estables hay que mencionar a Terra Luna. Dentro de su ecosistema encontramos dos monedas: UST, que era en teoría su moneda estable, y LUNA, el token de respaldo. La empresa detrás de ello fue creada en el año 2018, con sede central en Corea del Sur, y fundada por Do Kwon (actualmente preso). En abril de 2019 publicó su white paper[13] y lanzó su stablecoin, que cotizó hasta mayo de 2022, cuando los principales exchanges del sistema comenzaron a deslistarla.

12- Robert Sams, economista inglés, autor del influyente white paper que introdujo el concepto de acciones de señoreaje en el ecosistema cripto.

13- Emergency Management and Recovery of Luna Classic. https://www.researchgate.net/publication/361785716

El token LUNA, que actuaba como respaldo de la stablecoin UST, era el que absorbía la volatilidad; no era un colateral físico (como dólares en un banco u oro en una bóveda), sino un activo cuyo valor respaldaba algorítmicamente la estabilidad de UST. Grandes tenedores del token vendieron sus posiciones, generando una pérdida de confianza cada vez mayor, a medida que más tenedores replicaban el mismo accionar, produciéndose de esa forma el fallo y su posterior ocaso. Puede hacerse una comparación, a grandes rasgos, con una corrida bancaria (el corralito del 2001). Cuando el precio de UST empezó a caer, la gente perdió la fe y comenzó a intercambiar sus UST por LUNA para poder salir del sistema; ante esta conducta sistemática de miles de personas, el algoritmo imprimió millones de nuevos LUNA para poder cumplir con la demanda, lo que generó que el precio de LUNA se desmoronara estrepitosamente (dada la alta oferta), y ante ello, LUNA ya no pudo respaldar el valor de UST.

En el estudio elaborado por Nejadmalayeri y otros en Monedas estables: pasado, presente y futuro (2022), se habla de dependencia circular al explicar el colapso de LUNA-Terra. Por su parte, meses antes del fallo, los usuarios mostraron un apetito de compra voraz debido al interés que generaba el token UST al ser depositado en un protocolo de finanzas descentralizadas (DeFi) que otorgaba un 19,5% de interés anual.

La mayoría de los autores estudiados coinciden en que el error de Terra fue su colateralización endógena: el valor de su stablecoin UST dependía de la demanda de su propio activo de respaldo, LUNA, creando una vulnerabilidad matemática que, ante una pérdida de confianza, llevó a una "espiral de la muerte".

a) PEG

El PEG es lo que se conoce como "el mecanismo de paridad". Si una moneda tiene un "PEG con el dólar", significa que su objetivo es valer siempre 1 dólar; podríamos mencionar como ejemplo el peso argentino en la década de 1990: "1 peso, 1 dólar". Puede ocurrir, como en el caso de Terra Luna, que el PEG se rompa (pierda la paridad); esto se conoce como DE-PEG. El PEG actúa como un indicador de confianza, y la pérdida de este es una señal de alerta.

Este fenómeno se observa con relativa frecuencia en las monedas estables, sobre todo en los días u horas de mucha volatilidad, en los

que, a los pocos minutos, el valor se estabiliza de inmediato en un dólar. El problema radica cuando una stablecoin pierde el PEG y no logra volver a un dólar en un tiempo prudencial.

b) Espiral de la muerte

Este fenómeno, conocido como bucle de retroalimentación negativa, podría explicarse de forma sencilla como la pérdida de confianza en el compromiso de convertibilidad, que provoca una corrida sobre el activo de referencia. Como bien señalan autores como Catalini y De Gortari (2021), este fenómeno se desencadena si los mecanismos de mercado fallan en absorber el exceso de oferta, lo que deriva en una pérdida permanente de la paridad, o de-peg, del activo.

Como se ha dicho anteriormente, el problema radica en la confianza: si los usuarios dejan de creer que el sistema funciona, el precio de la stablecoin cae por debajo de su paridad, es decir, cae por debajo de 1; el algoritmo comienza a emitir masivamente el token de respaldo para absorber la caída; acto seguido, como existen demasiados tokens de respaldo en el mercado, su valor se desploma; al valer menos el respaldo, la pérdida de confianza se profundiza, provocando una caída total de ambos activos a cero.

c) Actualidad de las monedas algorítmicas

Tras el colapso del ecosistema Terra en 2022, el sector viró hacia modelos más conservadores. Diversas regulaciones en distintas partes del mundo prohibieron la emisión de este tipo de stablecoins debido a su elevado riesgo, y las que sobrevivieron mutaron: ya no existen stablecoins cien por ciento algorítmicas, sino híbridas, que combinan respaldo en activos con un componente algorítmico.

Aun así, estas monedas han perdido la mayor parte de la cuota de mercado que alguna vez tuvieron. Un ejemplo actual es Frax, proyecto que combina respaldo parcial en otras stablecoins (USDC) con un mecanismo algorítmico, y que hoy ocupa el puesto 120 según CoinMarketCap. Otra es USDD, dentro del ecosistema de Tron, moneda estable con mecanismos algorítmicos de emisión y quema similares al antiguo modelo de Terra, aunque con un respaldo más diversificado, y que se encuentra en el puesto 55 según CoinMarketCap.

Cabe hacer mención, además, a una moneda estable "no estable": el token es Ampl y el proyecto se llama Ampleforth. Este token no

intenta valer siempre 1:1, sino que la cantidad de monedas que una persona posee cambia día a día para que el precio busque el equilibrio. Esta moneda es extremadamente volátil y en la actualidad no ingresa entre las mil primeras según CoinMarketCap.

2. El nuevo marco regulatorio global

2.1. Primeras aproximaciones político-legislativas

Para comprender cómo se fue construyendo el marco regulatorio en esta materia, conviene partir de tres cuestiones fundamentales.

La primera es que, por su naturaleza descentralizada y su origen privado, los criptoactivos operaron durante años sin regulación estatal. Desde sus comienzos hasta su popularización en el comercio internacional, los conflictos se resolvían dentro de la propia comunidad, que definía sus propias normas bajo los principios de descentralización y autonomía. Cada usuario era responsable de la custodia y el uso de sus fondos. Esa etapa inicial fue, en esencia, un período de anarquía y vacío legal.

La segunda cuestión surge de una necesidad práctica: a medida que los usuarios buscaron custodiar sus fondos e intercambiar activos digitales de forma más sencilla, comenzaron a aparecer los exchanges, denominados en nuestro país "proveedores de servicios de activos virtuales". Estos actores se volvieron centrales en el ecosistema, al ofrecer servicios de custodia e intercambio de criptoactivos a cambio de una comisión.

En tercer lugar, como sucede en la gran mayoría de los tópicos, el Estado suele llegar luego. En este caso, las primeras regulaciones provinieron de diferentes organismos internacionales, y respecto de los Estados nacionales, aún hoy en día no cuentan con una regulación unificada.

Como podemos observar, esta maraña de cuestiones de soberanía, que abarca desde lo más primordial, es decir, si están permitidos o no los criptoactivos y, en su caso, cuáles, hasta la pregunta de quién es el emisor de esos criptoactivos y qué repercusiones traerá en el mercado interno, constituye el conjunto de interrogantes y problemáticas que los Estados fueron observando a la hora de intentar abordarlas.

Frente a ello, encontramos Estados que establecieron diferentes tipos de limitaciones y otros que plantearon la prohibición total, siendo esta última postura minoritaria a nivel mundial.

1. Reglamento MiCA (Markets in Crypto-Assets) 2023/1114

Para analizar el Reglamento 2023/1114, denominado "Ley MiCA", debemos primero comprender en qué contexto se define esta regulación, desde lo histórico hasta lo coyuntural. La Unión Europea —en adelante, U.E.— es la organización de Estados dentro de la cual los diferentes Estados parte logran establecer una serie de normas unificadas y uniformes sobre diferentes aspectos de la vida en sociedad, mediante la concesión de facultades (en detrimento de su propia soberanía). Entre las principales restricciones se destaca la imposibilidad de emitir moneda, salvo el caso puntual de Dinamarca, que mantuvo esa facultad mediante reserva. Un ejemplo de las controversias que se dieron a raíz de ello se registró en el año 2021, con la declaración de inconstitucionalidad por parte del Tribunal Constitucional de Polonia respecto del art. 19 del Tratado de la Unión Europea[14]. Con estas disputas en desarrollo, en el año 2024, por resolución C/2024/4209, el Parlamento Europeo reafirmó la implementación del principio de primacía del derecho de la U.E.[15]

Establecido el órgano jurídico supraestatal que lleva a cabo dichas resoluciones, cabe preguntarnos: ¿cómo fue el desarrollo de la legislación en materia de activos digitales o criptoactivos en la U.E.?[16]

Primero cabe referir que la Directiva 2018/843[17] realizó una enmienda a la Directiva 2015/849[18] y estableció la definición de "monedas virtuales" como:

> "...una representación digital de valor que no es emitida ni garantizada por un banco central o una autoridad pública, no está necesariamente vinculada a una moneda legalmente establecida y no tiene la condición jurídica de moneda o dinero, pero que es aceptada por personas físicas o jurídicas como medio de intercambio y que puede transferirse, almacenarse y negociarse por vía electrónica..."

14- Diario Oficial de la Unión Europea, 30/03/2010, p. 15.
15- European Parliament resolution (C/2024/4209).
16- Diario Oficial de la Unión Europea.
17- Directiva (EU) 2018/843.
18- Directiva (UE) 2015/849.

Con la ley Pacte, Francia modificó en 2019 la legislación vigente sobre inversiones extranjeras, quedando los proveedores de servicios de activos digitales sujetos a la misma. Así, Francia fue el primer país en aplicar en territorio europeo la obligatoriedad de inscripción para operar en su territorio mediante el régimen PSAN[19]. Con estos antecedentes, el 31 de mayo de 2023, el Parlamento Europeo y el Consejo firmaron el reglamento 2023/1114, denominado Ley MiCA, por sus siglas en inglés "Markets in Crypto-Assets". Un año después se dio inicio a la aplicación de los Títulos III y IV, referidos específicamente a la regulación de la oferta pública y emisión de las stablecoins[20].

¿Qué se busca con esta normativa unificada? Garantizar el correcto funcionamiento de los mercados de criptoactivos, la integridad del mercado y la estabilidad financiera en la U.E., así como la protección de los titulares de criptoactivos, en particular los titulares minoristas, desde la órbita supraestatal.

Asimismo, encontramos la definición de "criptomonedas estables" como aquellas que "buscan mantener el valor estable en relación con una moneda oficial o uno o varios activos a través de protocolos que prevén el aumento o disminución de la oferta de tales criptoactivos en respuesta a los cambios en la demanda" (art. 41, Reglamento 2023/1114). Se establece, además, una serie de obligaciones para los emisores según las categorías propuestas por la normativa[21].

Es dable destacar que las dos principales categorías que encontramos en la Ley son los denominados Tokens Referenciados a Activos (Asset-Referenced Tokens) y, por otro lado, los EMT o Tokens de Dinero Electrónico (Electronic Money Tokens). Referenciado en esta última categoría, Tether se encontraría naturalmente incorporado.

¿Cuáles son los requisitos para los emisores? En primer lugar, deben ser personas jurídicas establecidas regularmente en la U.E., y tienen como deber presentar un denominado White Paper donde detallen los objetivos del proyecto, a los fines de que sean analizados por los diferentes órganos de control estatales, para obtener la denominada licencia CASP (Crypto-Asset Service Provider). Esta licencia, que puede ser otorgada en cualquiera de los Estados parte, genera la posibilidad de operar legalmente en cualquiera de los 27 países miembros.

19- Ley N.º 2019-486 (Francia).
20- Final Report Draft Regulatory Technical Standards under MiCAR (19/06/2024).
21- Ídem.

Esta normativa está enfocada en establecer pautas claras a la hora de operar con criptoactivos de manera legal, generando seguridad y estabilidad jurídica, y transparencia a la hora de la aplicación e interpretación de este tipo de operaciones. Al momento de esta publicación encontramos que la Ley MiCA se encuentra en aplicación, y ya observamos los primeros impactos políticos y geopolíticos, dado que la normativa no ha dado sus primeros pasos de manera pacífica.

El 01/07/2026 entró en vigencia la disposición según la cual la autorización de un Estado miembro de la Unión Europea a un exchange para operar genera "automáticamente" la posibilidad de operar en los demás países miembro. Esta facultad cobró principal relevancia porque Binance, el exchange más grande del mundo, en los últimos días recibió el rechazo de su autorización por parte de Grecia. Desde la óptica legal, Grecia contaría con la facultad de inhabilitar a Binance para operar en territorio de la U.E. Si bien el rechazo no llegó a concretarse, atento a que la empresa retiró la solicitud, comienzan a observarse las implicancias prácticas y la problemática de esta normativa.

2.2. Ley Genius y Ley Clarity Act

Cuando hablamos de regulación en los Estados Unidos de Norteamérica, debemos comprender que estamos frente a un sistema federal, tal como se establece en la Décima Enmienda[22].

El primer antecedente en materia regulatoria fue una regulación estatal de junio de 2015, cuando el Departamento de Servicios Financieros (DFS) de Nueva York publicó las reglas finales sobre monedas virtuales. Bajo la norma 23 NYCRR Part 200[23], estableció la BitLicense y, con ella, reglas y estándares férreos a la hora de emitir la licencia de monedas virtuales, principalmente requisitos altos en materia de prevención del lavado de dinero, capitalización, protección del consumidor y ciberseguridad. Luego, se destaca en materia interpretativa la publicación de la SEC acerca de "The DAO" en el año 2017[24].

En 2018, en el estado de Nueva York, se estableció un "estándar de auditoría de reservas" (con el caso Circle). Por su parte, el Departamento de Servicios Financieros (DFS)[25] autorizó a Gemini Trust

22- Constitución de los Estados Unidos.
23- Departamento de Finanzas de New York. Virtual Currency Business Licensing (2015).
24- SEC. Informe THE DAO (2017).
25- Departamento de Finanzas de New York. DFS Authorizes Gemini Trust Company (2018).

Company a ofrecer productos y servicios adicionales relacionados con las monedas virtuales, convirtiéndose en el primer custodio y plataforma de intercambio autorizado en recibir la aprobación del DFS para operar con la moneda digital Zcash en Nueva York.

Corría el año 2020 cuando los bancos tradicionales empezaron a tomar conciencia de las stablecoins, de las diferentes tecnologías (algunas DeFi) y de sus repercusiones económicas. En dicho año, la Office of the Comptroller of the Currency (OCC) emitió pautas interpretativas mediante las cuales se permitió a los bancos nacionales custodiar criptoactivos y usar stablecoins como métodos de pago[26]. Ese mismo año, en septiembre, la OCC autorizó a mantener reservas de activos que respaldan a las stablecoins[27]. Ya en enero de 2021 procedería a esclarecer que las entidades bancarias pudieran participar como nodos en redes de verificación independientes y utilizar stablecoins de pago.

En el año 2021, el President's Working Group on Financial Markets (PWG) publicó un reporte definitivo sobre las stablecoins, recomendando que los emisores debieran ser instituciones bancarias (aseguradas por la FDIC), es decir, categorizándolas como "instituciones de depósito" aseguradas, para evitar inestabilidades económicas y riesgos de posibles corridas.

El año 2022 fue clave en el marco regulatorio: la presidencia a cargo de Joe Biden emitió una orden dirigida a todas las agencias, en el marco de una estrategia nacional. La orden ejecutiva N.º 14067[28] buscó el desarrollo "responsable" de los activos digitales, priorizando la estabilidad financiera, la prevención de delitos y la exploración de una moneda digital (CBDC) del banco central de los Estados Unidos.

En esos momentos, la Reserva Federal (FED) limitó las actividades de los bancos miembros en el sector cripto, lo que generó que posteriormente este sector introdujera propuestas legislativas en la Clarity Act 2023. Mientras tanto, en el estado de Nueva York se estableció la primera guía formal sobre la calidad de las reservas (T-Bills y efectivo)[29].

26- OCC. Carta interpretativa N.º 1170 (2020).
27- OCC. Federally Chartered Banks and Thrifts May Engage in Certain Stablecoin Activities (2020).
28- Orden ejecutiva N.º 14067 (2022).
29- Departamento de Finanzas de New York. Guía regulatoria sobre stablecoins (2022).

En 2023, PayPal, la empresa de pagos digitales, ejerció presión sobre los legisladores ante el lanzamiento de PYUSD. Como resultado, se presentó formalmente la Clarity for Payment Stablecoins Act, con el fin de crear un marco federal que no dependa solamente de los estados[30].

En 2024 encontramos uno de los elementos claves que enmarcaron la visión de la Securities and Exchange Commission (SEC) en el caso contra Binance Holdings Limited. Ese año, la SEC demandó a Binance Holdings y a su fundador Changpeng Zhao por tres motivos: haber ofrecido y vendido criptoactivos —entre ellos la stablecoin BUSD— sin registro previo; operar como plataforma de intercambio sin estar registrada como exchange o broker; y haber realizado declaraciones falsas a los inversores, lo que podría configurar fraude.

En cuanto a BUSD en particular, la SEC argumentó que constituía un contrato de inversión y, por lo tanto, una security bajo el criterio del Test de Howey, establecido por la Suprema Corte en SEC v. W.J. Howey Co. Según ese test, existe una security cuando hay una expectativa de ganancias proveniente de una empresa común que depende del esfuerzo de terceros. Al calificar BUSD bajo esa definición, la SEC reclamaba jurisdicción sobre el activo. La defensa impugnó la demanda argumentando problemas de aplicación extraterritorial de la jurisdicción de la SEC, y la Corte consideró que los argumentos presentados por la SEC eran insuficientes, fallando a favor de la defensa[31]. En este antecedente es necesario aclarar que la cuestión no se encuentra saldada jurisprudencialmente.

En 2025, el presidente Trump firmó una nueva orden ejecutiva revocando la orden N.º 14067, estableciendo una prioridad para el dólar digital privado (stablecoins) por sobre las CBDC (las stablecoins emitidas por los propios bancos centrales). En julio de ese mismo año, el proyecto de la "Ley GENIUS" dejó atrás las diferentes normativas de referencia estaduales y centró en una unificación legislativa los estándares aplicables, siendo el primer gran paso legislativo en los Estados Unidos hacia la regulación de las stablecoins, sumando al país a una lista de estados que buscan establecer supervisión y estabilidad en el ecosistema de activos digitales en expansión. El objetivo de la ley es ofrecer un marco regulatorio claro para la industria, pero

30- Congreso de los Estados Unidos. H.R.4766 (2023).

31- Fondo, Kim. Stablecoins Unlikely to Be Subject to the SEC's Jurisdiction (26/07/2024).

principalmente para el sector bancario o de comercio tradicional. El cumplimiento bajo GENIUS exige que los futuros emisores de stablecoins establezcan una entidad regulada localmente, sujeta al espectro completo de normas, que abarca desde estándares de confianza, transparencia, divulgación y rendición de cuentas, hasta estricta adhesión a las obligaciones de prevención de lavado de dinero, financiamiento del terrorismo y sanciones.

¿Cuáles son los "Permitted Issuers"? Son tres categorías: las subsidiarias de instituciones depositarias aseguradas; los denominados Federal Qualified Issuers, bajo supervisión directa de la OCC; y los State Qualified Issuers, entidades con licencia a nivel estatal[32]. El proyecto de Ley GENIUS no prohíbe por completo que existan stablecoins con o sin respaldo, pero sí exige un estudio exhaustivo por parte del Departamento del Tesoro sobre las monedas estables con garantía endógena, respaldadas por otros activos digitales creados por el mismo emisor, en la Sección 14. Si bien ya se habían observado avances con las regulaciones en Nueva York, esta regulación estableció un estándar nacional en materia de "calidad de las reservas". La autorización para emitir requiere que las reservas mantengan, como mínimo, la paridad 1:1 con las stablecoins en circulación; para garantizar esta liquidez, se establece la obligatoriedad de mantener reservas en dólares estadounidenses/bonos de la Reserva Federal, bonos del Tesoro de los Estados Unidos (a corto plazo) y acuerdos de recompra (siempre que se encuentren respaldados por el Tesoro). A su vez, establece controles exhaustivos (informes públicos periódicos, auditorías anuales, entre otros)[33]. En el año 2026 nos encontramos en la fase de implementación de la Ley GENIUS. Con esta regulación, las stablecoins son clasificadas como instrumentos bancarios y no como securities, lo que genera una mayor soberanía del dólar en la economía digital, reposicionándolo como la moneda de respaldo a nivel internacional. La propia naturaleza del ordenamiento jurídico norteamericano impone que la Ley GENIUS fije las pautas que los diferentes estados parte pueden ir adoptando. Hay estados que pueden ir flexibilizando o incluso robusteciendo las regulaciones y exigencias a la hora de legislar, siempre y cuando se ajusten a los lineamientos constitucionales (Décima Enmienda).

32- Congreso de los Estados Unidos. S.1582.

33- Congreso de los Estados Unidos. GENIUS Act of 2025.

Más allá de la disputa de política económica que se está librando, ambas normativas buscan la integración entre los bancos tradicionales/fintechs, bajo el amparo de la Ley GENIUS, y de los exchanges, a partir —en caso de que suceda— de la Clarity Act. Ambas normativas son claves y deberían interpretarse en conjunto para resolver la tensión entre los diferentes actores del mercado bursátil en los Estados Unidos.

2.3. Regulaciones en China y Rusia

En Oriente, dos grandes contrapesos del mundo occidental son China y Rusia. Rusia, país de ubicación euroasiática históricamente considerado europeo, debió replantear su postura frente a los criptoactivos a raíz de crecientes tensiones geopolíticas: su negativa a integrarse a la U.E., la expansión de la OTAN y, más recientemente, la guerra por la anexión de Ucrania.

El recorrido ruso siguió el patrón común a otras grandes potencias: primero, los criptoactivos fueron vistos como una amenaza a la estabilidad macroeconómica, postura esperable en un sistema financiero ultraconservador y altamente regulado. Luego, como ocurrió en la mayoría de los países, la presión de la modernidad terminó imponiéndose.

La adopción a nivel mundial de las stablecoins generó que el gobierno central ruso tuviera que abordar el asunto y promulgara, en 2020, la Ley Federal sobre Activos Financieros Digitales, Moneda Digital. La ley 259-FZ[34] establece un "régimen mixto", es decir, deja atrás la prohibición total para pasar a un sistema de autorización con gran injerencia estatal, principalmente bajo el control férreo del Banco Central Ruso. Mediante esta normativa se autoriza "la emisión de activos digitales que representan: a) derechos de crédito; o b) participación en empresas, siempre y cuando el emisor sea una entidad autorizada por el Banco Central Ruso".

La particularidad que establece esta normativa se encuentra en su art. 3.1, inc. 12: queda prohibido aceptar "activos financieros digitales" como medio de pago o cualquier otra forma de contraprestación por bienes, trabajo o servicios prestados, así como de cualquier otra manera que implique el pago mediante activos financieros digitales.

34- Gobierno de la Federación Rusa. Ley Federal N.º 259-FZ (31/07/2020).

Con ello, la postura del gobierno nacional y de las políticas aplicadas por el Banco Central Ruso siguieron una línea "anti-stablecoin" atada al rublo, entendiendo que dicha emisión podría generar desajustes macroeconómicos (entre los cuales estaría la inflación).

En el año 2020 se dio inicio a la guerra de Ucrania, y Rusia comenzó a sufrir una serie de sanciones económicas y pérdida de mercados a nivel mundial. Los países europeos dejaron de consumir uno de los recursos más importantes para la economía rusa, como lo es el gas. Estas circunstancias fueron generando cimbronazos en la economía rusa ante la imposibilidad de realizar pagos mediante el sistema bancario tradicional SWIFT (Society for Worldwide Interbank Financial Telecommunication), lo que llevó al gobierno a ampliar la mirada acerca de las stablecoins y los criptoactivos.

Actualmente, el Banco Central Ruso (BCR) está autorizando a determinadas empresas y bancos a realizar pruebas de liquidación de comercio exterior utilizando stablecoins, pero siempre bajo supervisión estatal[35].

Se consolida esta postura cuando, con la 259-FZ, se establece la utilización de las stablecoins para pagos internacionales, permitiendo sortear las sanciones económicas que pesan en la actualidad. Con esta normativa se equipara a la noción jurídica de "divisas" utilizadas para el comercio exterior la utilización de las stablecoins. En octubre de 2025, la stablecoin A7A5, vinculada al rublo, fue aprobada para su uso en el comercio exterior, convirtiéndose en el primer piloto de esta política[36].

A su vez, desde el BCR se busca fomentar la utilización de lo que denominan "stablecoin soberana", término con el que se refieren al rublo digital, que, por cuestiones conceptuales y por su naturaleza, es más similar a una CBDC que a una stablecoin, aunque técnicamente siguen considerándose dinero de curso legal, algo similar al dinero electrónico.

Con esto encontramos una muestra de una respuesta intermedia a la hora de la regulación, haciendo foco no tanto en los derechos de los usuarios y de los exchanges mixtos, sino en la utilidad soberana que puede dárseles a este tipo de activos. Ahora bien, ¿cuál es el panorama en el gigante asiático de la República Popular China? En

35- Binance. Rusia considera la legalización permanente de las monedas estables.
36- Gate News. Rusia planea implementar la Ley de monedas estables.

este caso particular no encontramos una regulación en la materia, sino una serie de actos administrativos denominados "avisos", emitidos por la máxima autoridad en materia económica, el Banco Popular de China (PBOC).

Desde 2017, el órgano regulador estableció su postura, prohibiendo el crypto trading, los exchanges y la minería, política que se mantiene hasta la fecha. Sin embargo, los tribunales chinos fijaron una distinción clave: aunque las criptomonedas no pueden funcionar como dinero, los particulares pueden seguir poseyendo activos digitales como propiedad legítima. Un informe judicial de 2023 confirmó esta protección.

En resumen, los ciudadanos pueden poseer criptomonedas, pero no pueden utilizarlas como moneda. Con el aumento de la demanda de monedas estables en todo el mundo, la postura de China contrasta ahora claramente con la de otras regiones. Mientras muchos países exploran nuevas regulaciones sobre las criptomonedas, Pekín sigue aplicando una política de tolerancia cero. Actualmente, el mensaje del Banco Popular de China es sencillo: las monedas digitales pueden crecer en otros lugares, pero en China continental la puerta permanece firmemente cerrada[37].

Este es el último paso de un proyecto que se viene desarrollando desde hace varios años: mantener las criptomonedas especulativas fuera del sistema financiero formal, al tiempo que se promueve activamente el uso del e-CNY, la CBDC soberana emitida por el Banco Central de China. En enero de 2026, el Banco Popular de China autorizó a los bancos comerciales a pagar intereses sobre las carteras de yuan digital, en un intento por hacer que la moneda digital del banco central resultara más atractiva para los inversores. En este mismo sentido, en febrero de este año, el Banco Popular de China (PBOC), en conjunto con la Comisión de Seguridad Regulatoria de China —de forma similar a la postura rusa de protección de la soberanía monetaria— incorporó la prohibición de la emisión de cualquier tipo de stablecoin.

Es decir, China ha adoptado un enfoque basado en la adopción del e-CNY o yuan digital, un instrumento más similar a una CBDC que a una stablecoin, manteniendo así el poder de emisión y control sobre las diferentes variables macroeconómicas.

37- Binance. China Central Bank Reaffirms Ban on Stablecoins and Crypto Payments (2025).

1. Otras regulaciones importantes

Para completar el panorama de regulaciones, mencionaremos otros países económicamente importantes en el mapa mundial. En el Reino Unido, el Banco de Inglaterra (BoE), en el marco de la Ley de Propiedad (Activos Digitales)[38], apunta a implementarse en 2026. La autoridad encargada de la supervisión de la aplicación de las normas es la Financial Conduct Authority (FCA). En las primeras etapas, las empresas cripto debían registrarse ante la FCA (de forma similar a la CNV en nuestro país) para adecuarse. La FCA estableció, para impulsar las stablecoins, un sandbox regulatorio que permite a las compañías locales probar pagos con estos activos[39].

Una de las claves de la propuesta es la distinción entre las stablecoins sistémicas y las no sistémicas. Las primeras son aquellas con potencial para ser ampliamente utilizadas en pagos cotidianos, tanto minoristas como corporativos, y cuya interrupción podría generar efectos de contagio en el sistema financiero.

Las segundas se limitan a usos cripto o a pagos de alcance reducido, sin impacto macroeconómico significativo. Las no sistémicas quedarán bajo la supervisión exclusiva de la FCA, mientras que las sistémicas serán reguladas de manera conjunta por la FCA y el Banco de Inglaterra. Con esta diferenciación, el Reino Unido adopta un enfoque prudencial que no depende del tipo de activo, sino del riesgo que su uso puede generar. Para afrontar posibles riesgos de desintermediación bancaria, el documento introduce límites de tenencia: en pagos minoristas, los particulares no podrán mantener más de 20.000 libras por cada stablecoin sistémica, mientras que, para las empresas, el límite será de 10.000 millones de libras. No obstante, se prevén exenciones para comercios y operadores que necesiten saldos superiores para su actividad diaria. Dichos límites pretenden evitar que un uso masivo de stablecoins desvíe grandes depósitos desde los bancos comerciales hacia emisores privados, y evitar el impacto sobre la oferta de crédito y la estabilidad del sistema financiero. El corazón del nuevo marco regulatorio reside en el modelo de activos de respaldo exigido a los emisores sistémicos. El Banco de Inglaterra propone que al menos el 40% de los fondos que respaldan cada unidad de stablecoin se mantenga en depósitos no remunerados

38- Mori, Blanco. Regulación de stablecoins en el Reino Unido. Beincrypto (2025).
39- Iproup. El Reino Unido avanza con la regulación cripto (2025).

directamente en el banco central, una política destinada a garantizar liquidez inmediata ante picos de reembolso[40].

Bajo el marco propuesto, las empresas se enfrentarían a pesadas obligaciones de reservas, incluyendo una estipulación para mantener un mínimo del 40% de sus reservas en depósitos no remunerados en el Banco de Inglaterra, complementado hasta en un 60% con valores gubernamentales británicos a corto plazo. Si bien estas medidas buscan mitigar riesgos sistémicos, podrían paradójicamente limitar a las empresas nacionales, socavando su competitividad en un mercado global cada vez más exigente[41]. Actualmente rige la Financial Services and Markets Act 2023 y su posterior modificación, promulgada en febrero de 2026, que actualiza la norma regulada en 2023. Con ello, el Reino Unido pretendió incorporar una normativa más flexible para competir con la nueva regulación MiCA.

2.4. Regulación argentina

La regulación en materia de criptoactivos o de activos digitales en nuestro país solo alcanza a la materia tributaria. Y, frente al vacío legal, podemos afirmar que la utilización de las stablecoins está permitida, siendo Argentina uno de los países con mayor nivel de adopción de estas monedas[42].

Cabe destacarse que recién en el año 2024, mediante la sanción y promulgación de la Ley N.º 27.739, se designó como órgano de regulación a la Comisión Nacional de Valores (CNV), estableciendo la categoría de proveedor de servicios de activos virtuales, diferente de las figuras de intermediación financiera que ya existían en nuestro país, aunque sin constituirla en un ente regulador integral de los "activos virtuales" propiamente dichos, salvo en el caso en que dichos activos virtuales constituyan valores negociables ofrecidos públicamente, lo que implicaría que estén regidos por la Ley de Mercado de Capitales (Ley N.º 26.831).

Esto trajo consigo la creación de un registro de proveedores de servicios de activos virtuales, bajo la órbita de la CNV, y, a su vez, la obligación de inscripción para todos los exchanges argentinos y de capitales extranjeros que operen en nuestro país. Mediante la

40- Observatorio Blockchain. Marco de Reino Unido para stablecoins (2025).
41- OneSafe. La cuerda floja regulatoria del Reino Unido (2025).
42- Bloomberg Línea. BCRA prohíbe operaciones cripto de bancos argentinos.

Resolución 994/24 se reglamentó la Ley 27.739 y se establecieron penalidades en caso de incumplimiento[43]. La Resolución 1058/25 estableció la obligatoriedad de la inscripción como persona jurídica en nuestro país y el establecimiento de los montos mínimos de reservas que deben poseer los proveedores.

El último proyecto de creación de una stablecoin argentina surgió con el activo virtual "ARGt", que fue intimado por la CNV por no ajustarse a las leyes cambiarias de nuestro país (principalmente en el enfoque de intermediación financiera no autorizada). El esquema de funcionamiento informado incorpora una promesa o expectativa de rendimiento vinculada a la tenencia del activo virtual ARGt, circunstancia que encuadraría en la figura de un contrato de inversión, incluido en la definición de valor negociable prevista en el artículo 2º de la Ley N.º 26.831 de Mercado de Capitales, lo que deriva en su calificación como valor negociable sujeto al régimen de oferta pública[44].

En resumen, el vacío normativo y la falta de unificación de las competencias de control hacen que nuestro país se encuentre inmerso en una incertidumbre normativa que únicamente podrá superarse con una legislación mucho más transparente, y no mediante la apelación a resoluciones interpretativas del órgano de control, en este caso la CNV.

Consideramos que Argentina tiene un potencial enorme en el desarrollo de estas nuevas tecnologías y que puede convertirse en punta de lanza en Latinoamérica.

3. Conclusiones

El ecosistema de las stablecoins no solo representa una evolución tecnológica, sino un cambio de paradigma en la arquitectura financiera global. A lo largo de este estudio hemos analizado cómo las stablecoins han logrado resolver muchas de las deficiencias de los sistemas de pago tradicionales. Si bien el orden regulatorio internacional intenta alcanzar la velocidad de la innovación cripto, la dinámica de los usuarios permanece constante en su búsqueda de agilidad. Como bien se suele decir, mover dinero es como el agua fluyendo en

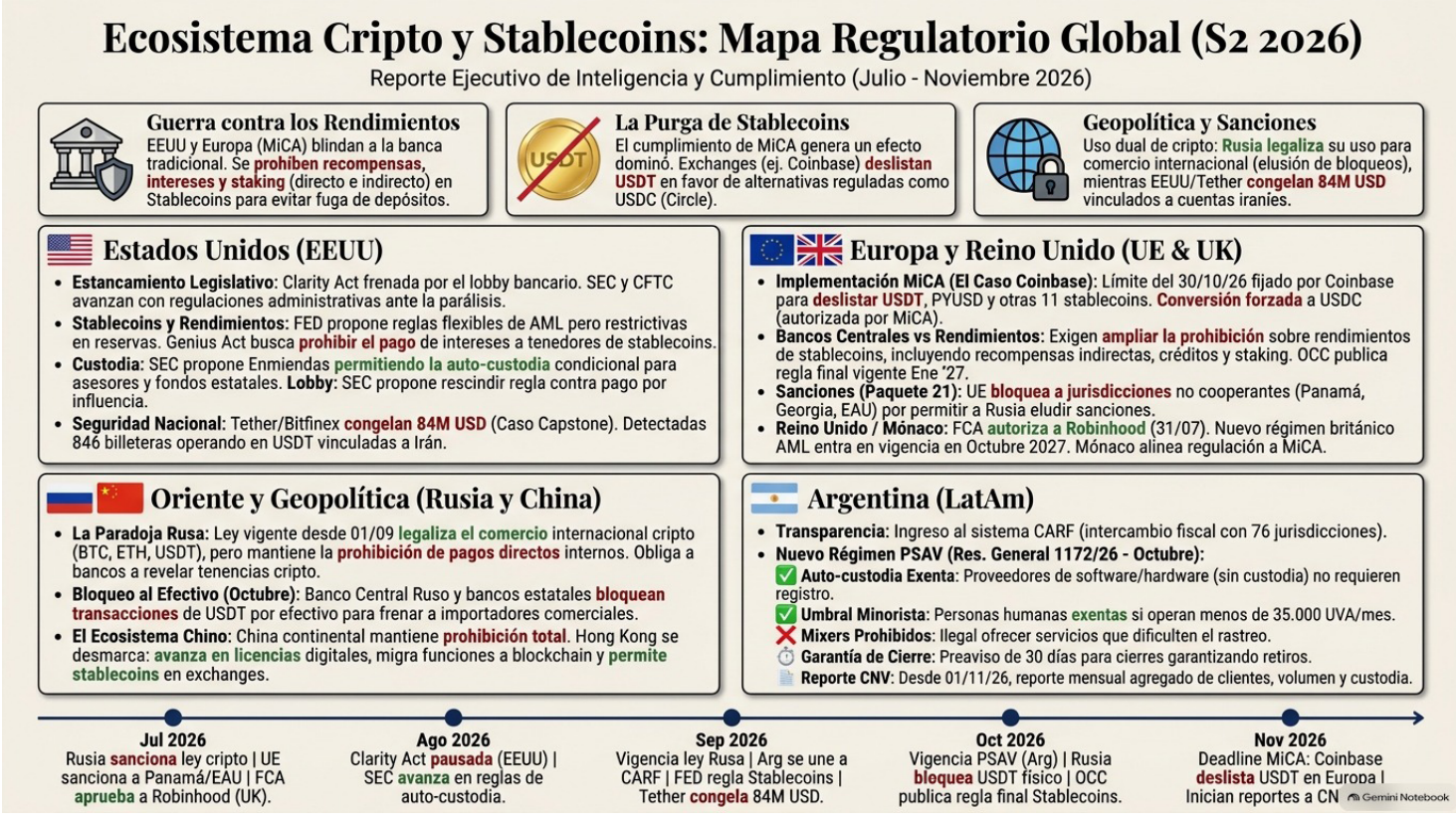
43- Marval. Se reglamenta la inscripción de los PSAV (25/03/2024).
44- Gobierno Argentino. Cese de oferta pública irregular y negociación de stablecoins.

una montaña: siempre encuentra la ruta más rápida, y hoy esa ruta son las stablecoins.

Las monedas estables no son solo una moda pasajera, sino que se están convirtiendo en instrumentos financieros fundamentales en el mercado de las criptomonedas. Su creciente capitalización de mercado indica una evidente adopción y confianza entre los usuarios, independientemente de los esfuerzos de algunos reguladores. Tanto si se trata de un trader, un inversor o simplemente alguien que busca escapar de la volatilidad, las monedas estables ofrecen una solución viable.

En el contexto del auge de los pagos digitales, los bancos centrales están respondiendo al rol cambiante del dinero tradicional desarrollando la idea de emitir sus propias monedas digitales (CBDC). Si bien no existe una decisión unánime entre los bancos centrales sobre la emisión y el diseño de las CBDC, en general las autoridades de dichas instituciones las consideran una forma de popularizar sus monedas en el contexto de la digitalización de la economía global. Al mismo tiempo, los países en desarrollo están interesados en las CBDC emitidas por el banco central como herramienta para aumentar la inclusión financiera, mientras que los países desarrollados las ven como una oportunidad para mejorar la seguridad de los pagos.

En este escenario, es tarea de los legisladores y reguladores asegurar que este cauce tecnológico desemboque en un sistema financiero más inclusivo y robusto. Esto solo será posible mediante la creación de normas claras y precisas que eliminen cualquier margen de ambigüedad, brindando la seguridad jurídica necesaria para que la adopción sea verdaderamente masiva. Solo a través de un marco legal transparente se podrá generar la confianza suficiente para que estos activos sean integrados plenamente, tanto por los ciudadanos en su cotidianeidad como por empresas, entidades financieras y naciones en sus estructuras económicas fundamentales.


Ecosistema Cripto y Stablecoins: Mapa Regulatorio Global (S2 2026)
Reporte Ejecutivo de Inteligencia y Cumplimiento (Julio - Noviembre 2026)
Guerra contra los Rendimientos
EEUU y Europa (MiCA) blindan a la banca tradicional. Se prohiben recompensas, intereses y staking (directo e indirecto) en Stablecoins para evitar fuga de depósitos.
La Purga de Stablecoins
El cumplimiento de MiCA genera un efecto dominó. Exchanges (ej. Coinbase) deslistan USDT en favor de alternativas reguladas como USDC (Circle).
Geopolítica y Sanciones
Uso dual de cripto: Rusia legaliza su uso para comercio internacional (elusión de bloqueos), mientras EEUU/Tether congelan 84M USD vinculados a cuentas iranies.
Estados Unidos (EEUU)
Estancamiento Legislativo: Clarity Act frenada por el lobby bancario. SEC y CFTC avanzan con regulaciones administrativas ante la parálisis.
Stablecoins y Rendimientos: FED propone reglas flexibles de AML pero restrictivas en reservas. Genius Act busca prohibir el pago de intereses a tenedores de stablecoins.
Custodia: SEC propone Enmiendas permitiendo la auto-custodia condicional para asesores y fondos estatales. Lobby: SEC propone rescindir regla contra pago por influencia.
Seguridad Nacional: Tether/Bitfinex congelan 84M USD (Caso Capstone). Detectadas 846 billeteras operando en USDT vinculadas a Irán.
Europa y Reino Unido (UE & UK)
Implementación MiCA (El Caso Coinbase): Límite del 30/10/26 fijado por Coinbase para deslistar USDT, PYUSD y otras 11 stablecoins. Conversión forzada a USDC (autorizada por MiCA).
Bancos Centrales vs Rendimientos: Exigen ampliar la prohibición sobre rendimientos de stablecoins, incluyendo recompensas indirectas, créditos y staking. OCC publica regla final vigente Ene '27.
Sanciones (Paquete 21): UE bloquea a jurisdicciones no cooperantes (Panamá, Georgia, EAU) por permitir a Rusia eludir sanciones.
Reino Unido / Mónaco: FCA autoriza a Robinhood (31/07). Nuevo régimen británico AML entra en vigencia en Octubre 2027. Mónaco alinea regulación a MiCA.
Oriente y Geopolítica (Rusia y China)
La Paradoja Rusa: Ley vigente desde 01/09 legaliza el comercio internacional cripto (BTC, ETH, USDT), pero mantiene la prohibición de pagos directos internos. Obliga a bancos a revelar tenencias cripto.
Bloqueo al Efectivo (Octubre): Banco Central Ruso y bancos estatales bloquean transacciones de USDT por efectivo para frenar a importadores comerciales.
El Ecosistema Chino: China continental mantiene prohibición total. Hong Kong se desmarca: avanza en licencias digitales, migra funciones a blockchain y permite stablecoins en exchanges.
Argentina (LatAm)
Transparencia: Ingreso al sistema CARF (intercambio fiscal con 76 jurisdicciones).
Nuevo Régimen PSAV (Res. General 1172/26 - Octubre):
✅ Auto-custodia Exenta: Proveedores de software/hardware (sin custodia) no requieren registro.
✅ Umbral Minorista: Personas humanas exentas si operan menos de 35.000 UVA/mes.
❌ Mixers Prohibidos: Ilegal ofrecer servicios que dificulten el rastreo.
⏱ Garantía de Cierre: Preaviso de 30 días para cierres garantizando retiros.
📄 Reporte CNV: Desde 01/11/26, reporte mensual agregado de clientes, volumen y custodia.
Jul 2026
Rusia sanciona ley cripto | UE sanciona a Panamá/EAU | FCA aprueba a Robinhood (UK).
Ago 2026
Clarity Act pausada (EEUU) | SEC avanza en reglas de auto-custodia.
Sep 2026
Vigencia ley Rusa | Arg se une a CARF | FED regla Stablecoins | Tether congela 84M USD.
Oct 2026
Vigencia PSAV (Arg) | Rusia bloquea USDT físico | OCC publica regla final Stablecoins.
Nov 2026
Deadline MiCA: Coinbase deslista USDT en Europa | Inician reportes a CN
Gemini Notebook

Bibliografía

Ante, L., Fiedler, I., Willruth, J. M., & Steinmetz, F. (2023): A Systematic Literature Review of Empirical Research on Stablecoins. *FinTech*, 2(1), 34-47. https://doi.org/10.3390/fintech2010003

Arner, D. y otros. (2020): Stablecoins: risks, potential and regulation. *BIS Working Papers No 905*. Bank for International Settlements. www.bis.org

Ayuso, J. y Conesa, C. (2020). Una introducción al debate actual sobre la moneda digital de banco central (CBDC). *Documentos Ocasionales Nº. 2005*. Banco de España., Available at SSRN: https://ssrn.com/abstract=3617558 o http://dx.doi.org/10.2139/ssrn.3617558

Banco de Pagos Internacionales, Banco de Canadá, Banco Central Europeo, Banco de Inglaterra. (2020). Monedas digitales de los bancos centrales: principios fundamentales y características principales.

Bullmann, D.; Klemm, J.; Pinna, A. (2019): In search for stability in crypto-assets: Are stablecoins the solution? *ECB Occasional Paper, Nº. 230*, European Central Bank (ECB), Frankfurt a. M., https://doi.org/10.2866/969389

Catalini, C. y de Gortari, A. (2021): *On the Economic Design of Stablecoins*. Available at SSRN: https://ssrn.com/abstract=3899499 o http://dx.doi.org/10.2139/ssrn.3899499

Chen, J. (2025): "Stablecoins: Mechanisms, Applications, and Regulation." *Scholarly Review Journal*. Scholarly Debut. https://doi.org/10.70121/001c.143048

DAFI. (2017). Guía de Investigación Financiera. Ministerio Público Fiscal.

Dionysopoulos, L.; Marra, M. y Urquhart, A. (2023): Central bank digital currencies: A critical review, *International Review of Financial Analysis*, Volume 91, Available at SSRN: https://ssrn.com/abstract=4354985 o http://dx.doi.org/10.2139/ssrn.4354985

Feingold, S. (2025). Stablecoins: por qué las criptomonedas respaldadas por reservas están en auge. *World Economic Forum*. https://es.weforum.org/stories/2025/04/stablecoins-por-que-las-criptomonedas-respaldadas-por-reservas-estan-en-auge/

Fondo Monetario Internacional. (2025). Implicaciones para la integridad financiera de las monedas digitales de bancos centrales minoristas.

Hafner, M., Henriques Pereira, M., Dietl, H., & Beccuti, J. (2024). The Four Types of Stablecoins: A Comparative Analysis. *Ledger*, 9. https://doi.org/10.5195/ledger.2024.326

Kochergin, D. & Ivanova, A., 2022. "Stablecoins: Clasificación, características funcionales y perspectivas de desarrollo", *Journal of the New Economic Association*, vol. 53(1), pp. 100-120. New Economic Association. DOI: 10.31737/2221-2264-2022-53-1-5

Le Grand Continent. (2025, 7 de abril). Por qué el dólar estadounidense seguirá dominando el mundo: geopolítica de las stablecoins. https://legrandcontinent.eu/es/2025/04/07/por-que-el-dolar-estadounidense-seguira-dominando-el-mundo-geopolitica-de-las-stablecoins/

Makiko, M. y otros. (2020). ¿Qué es una stablecoin?: Un estudio sobre los mecanismos de estabilización de precios para sistemas de pago descentralizados.

Nejadmalayeri, A. (2022): Stablecoins – Past, Present, and Future. *Blockchain Governance Initiative Network SR 010*. Available at SSRN: https://ssrn.com/abstract=4226071 o http://dx.doi.org/10.2139/ssrn.4226071

Ozturkcan, S.; Senel, K. y Ozdinc, M. (2022): Framing the Central Bank Digital Currency (CBDC) Revolution. *Technology Analysis & Strategic Management*, Available at SSRN: https://ssrn.com/abstract=4166704

Tether. (2014/2016). White Paper.

Tomaino, N. (2017). The State of Stablecoins. The Control.

No es disrupción, es adaptación: tensiones del ecosistema cripto en Argentina

Carlos Emanuel Monzón[1]

Resumen

El auge de las stablecoins en Argentina surge como una respuesta innovadora frente a la inflación, las restricciones cambiarias y la desconfianza en las instituciones financieras, constituyendo una de las transformaciones más relevantes del ecosistema financiero digital en los últimos años. Sin embargo, detrás de las promesas de autonomía, inclusión y descentralización emergen contradicciones que desafían algunas de las narrativas más difundidas sobre el ecosistema cripto.

El artículo analiza las principales tensiones que atraviesan este fenómeno, desde la dependencia de estructuras centralizadas y la concentración en usuarios ya bancarizados hasta los desafíos regulatorios y los nuevos riesgos asociados a su expansión. Más que describir el crecimiento de los criptoactivos, el trabajo invita a repensar qué transformaciones están produciendo realmente en la economía argentina.

1. Introducción

En las últimas décadas, Argentina ha atravesado un proceso persistente de inestabilidad económica, caracterizado por elevados niveles

1- Magíster en Finanzas y Licenciado en Administración y Gestión Empresarial por la Universidad Nacional de San Martín (UNSAM). El presente artículo se basa en los resultados de la tesis "Activos digitales en economías inestables, centrada en el análisis del uso de stablecoins en Argentina durante el período 2020-2025". Correo: monzon.carlos.emanuel@gmail.com

de inflación, restricciones cambiarias y una erosión sostenida de la confianza en el sistema financiero formal. En este contexto, los comportamientos económicos de los agentes no pueden entenderse únicamente como respuestas coyunturales, sino como parte de una lógica más amplia de adaptación frente a la incertidumbre.

En efecto, la reiteración de episodios de crisis ha dado lugar a la consolidación de una cultura económica defensiva, desconfiada y dolarizada, en la que predominan estrategias orientadas a preservar valor y reducir la exposición al riesgo monetario. Entre ellas se destacan la dolarización informal, el ahorro fuera del sistema bancario y la progresiva flexibilización de los límites entre economía formal e informal.

Es en este marco donde los activos digitales, y en particular las stablecoins, adquieren relevancia. Su expansión reciente no responde únicamente a la incorporación de nuevas tecnologías, sino a su capacidad de articular necesidades preexistentes: estabilidad, accesibilidad y autonomía frente a un entorno percibido como inestable. Sin embargo, este desarrollo no está exento de ambigüedades.

De hecho, el crecimiento del ecosistema cripto en Argentina plantea una paradoja central: los mismos instrumentos que se presentan como alternativas de descentralización y autonomía financiera tienden, en la práctica, a concentrarse en infraestructuras altamente centralizadas y en perfiles de usuarios específicos. Esta tensión no solo desafía las narrativas dominantes sobre innovación e inclusión, sino que también introduce nuevos interrogantes respecto de su funcionamiento efectivo.

Al mismo tiempo, la magnitud del fenómeno evidencia una transformación más profunda en las prácticas económicas. El uso extendido de stablecoins como sustituto funcional del dólar en contextos de restricción cambiaria pone de relieve su rol como mecanismo de adaptación frente a limitaciones estructurales del sistema financiero local. No obstante, esta misma dinámica tensiona los marcos regulatorios existentes, que enfrentan dificultades para capturar un fenómeno que combina trazabilidad tecnológica con formas persistentes de opacidad operativa.

Desde la perspectiva de la criminalidad económica, este escenario adquiere particular relevancia. La coexistencia entre circuitos formales e informales, la intermediación a través de plataformas globales y la

fragmentación de las capacidades de supervisión estatal configuran un entorno en el que los riesgos no solo se transforman, sino que también se redistribuyen. En este sentido, el análisis del ecosistema cripto excede la discusión tecnológica y se inscribe en un problema más amplio vinculado a la gobernanza económica contemporánea.

En función de ello, el presente artículo propone analizar las principales tensiones que estructuran el ecosistema cripto en Argentina, poniendo el foco en sus contradicciones internas y en sus implicancias regulatorias. Más que describir un fenómeno en expansión, se busca problematizar sus límites y explorar en qué medida estas dinámicas reproducen o redefinen los patrones históricos de relación entre los agentes económicos, el dinero y el Estado.

2. Marco conceptual: ecosistema cripto, regulación y riesgo

El análisis del ecosistema cripto exige superar las definiciones puramente técnicas y situar estos desarrollos en el cruce entre economía, tecnología y regulación. En términos generales, los activos digitales pueden entenderse como unidades de valor que se almacenan y transfieren de manera electrónica. Dentro de ellos, los criptoactivos se caracterizan por el uso de tecnologías criptográficas para validar transacciones. Si bien estos desarrollos se originan en infraestructuras basadas en redes descentralizadas, en la práctica su funcionamiento y circulación pueden involucrar diversos grados de intermediación y centralización. Sin embargo, esta definición resulta insuficiente para captar la complejidad del fenómeno en contextos como el argentino.

En efecto, la adopción de estos instrumentos no responde únicamente a sus propiedades tecnológicas. En entornos de inestabilidad macroeconómica, los activos digitales adquieren una función que trasciende lo financiero: se integran en estrategias más amplias de protección, autonomía y resistencia frente a instituciones percibidas como frágiles o invasivas. En este sentido, las stablecoins —especialmente aquellas vinculadas al dólar— no solo operan como instrumentos digitales, sino como una extensión funcional de la dolarización informal, adaptada a un entorno tecnológico.

Este punto resulta central para comprender una de las tensiones estructurales del ecosistema. Si bien la narrativa fundacional de los criptoactivos se asocia a la descentralización y a la reducción de la intermediación financiera tradicional, en la práctica su utilización cotidiana se encuentra mediada por actores que facilitan el acceso, la operatoria y la custodia de activos digitales. Además, en determinados segmentos del ecosistema —particularmente en el caso de las stablecoins de mayor adopción (USDT y USDC)— el funcionamiento depende de estructuras de emisión e infraestructura que presentan distintos grados de centralización.

Esta diferencia entre diseño y funcionamiento efectivo no es meramente operativa, sino que redefine el alcance real de la autonomía financiera que el ecosistema cripto proyecta, evidenciando que, más que eliminar intermediarios, el ecosistema tiende a reconfigurarlos.

Desde la perspectiva regulatoria, esta transformación plantea desafíos igualmente significativos. El desarrollo del ecosistema cripto se produjo, en gran medida, por fuera de los marcos jurídicos tradicionales, lo que dio lugar a espacios de innovación pero también a zonas grises en materia de supervisión. En Argentina, este proceso comenzó a revertirse con la incorporación de definiciones específicas para "activos virtuales" y "proveedores de servicios sobre activos virtuales" (PSAV) en la Ley 27.739, ampliando el universo de sujetos alcanzados por la normativa de prevención de lavado de activos.

No obstante, esta institucionalización no resuelve las tensiones de fondo. Por el contrario, introduce una nueva complejidad: mientras la regulación tiende a focalizarse en los intermediarios —donde la supervisión resulta operativamente viable—, los activos en sí mismos permanecen en gran medida fuera de un control directo. Esto genera una asimetría regulatoria en la que se controlan los puntos de acceso, pero no necesariamente la circulación posterior de los activos, lo que limita la efectividad de los mecanismos de supervisión.

En este contexto, los riesgos asociados al ecosistema cripto no pueden analizarse exclusivamente en términos tecnológicos. Desde la óptica de la criminalidad económica, estos instrumentos se insertan en un entramado más amplio que incluye delitos financieros, lavado de activos y aprovechamiento de vacíos regulatorios. La capacidad de transferir valor de manera transfronteriza, la coexistencia de trazabilidad técnica con dificultades de identificación efectiva de usuarios, y

la fragmentación de los marcos normativos configuran un escenario particularmente desafiante para los sistemas tradicionales de control.

Sin embargo, sería reduccionista interpretar estos riesgos únicamente como una anomalía del sistema. En muchos casos, estas dinámicas reflejan las mismas tensiones que ya existían en los circuitos financieros tradicionales, ahora reconfiguradas en un entorno digital. La informalidad, la búsqueda de resguardo de valor y la evasión de controles no son fenómenos nuevos, sino prácticas que encuentran en las nuevas tecnologías canales más eficientes de operación.

De este modo, el ecosistema cripto no puede entenderse como un espacio completamente disruptivo ni como una simple extensión del sistema financiero existente. Se trata, más bien, de un campo híbrido donde conviven lógicas de descentralización con estructuras centralizadas, innovaciones tecnológicas con prácticas históricas, y promesas de inclusión con nuevas formas de segmentación. Este carácter contradictorio justifica abordarlo no como un objeto cerrado, sino como un proceso en tensión permanente.

3. Tensiones estructurales del ecosistema cripto en Argentina

3.1. Autonomía financiera proyectada vs. dolarización centralizada

El desarrollo del ecosistema cripto en Argentina se encuentra atravesado por una tensión estructural entre la autonomía financiera que estos instrumentos proyectan y las formas concretas que adopta su utilización en la práctica. Mientras que la narrativa fundacional de los criptoactivos se asocia a la descentralización y a la posibilidad de reducir la dependencia de intermediarios financieros tradicionales, su adopción efectiva en contextos como el argentino responde a lógicas significativamente distintas.

En efecto, la utilización cotidiana de criptoactivos no está guiada prioritariamente por la búsqueda de autonomía tecnológica o financiera, sino por la necesidad de acceder a instrumentos que permitan preservar valor en un entorno de inestabilidad macroeconómica. En este contexto, las stablecoins se consolidan como el principal caso de

uso del ecosistema, no tanto por su arquitectura, sino por su capacidad de replicar funciones asociadas al dólar: estabilidad relativa, resguardo de valor y facilidad de acceso en entornos restrictivos.

Sin embargo, este predominio no es neutro desde el punto de vista estructural. Las stablecoins más utilizadas en Argentina —particularmente USDT y USDC— se caracterizan por su anclaje al dólar, su baja volatilidad y, fundamentalmente, por los altos niveles de liquidez que ofrecen frente a alternativas descentralizadas. Estas condiciones, que explican su difusión masiva, están directamente asociadas a esquemas de emisión centralizados, en los que empresas como Tether y Circle concentran funciones críticas vinculadas a la creación, el respaldo y la gobernanza de los activos.

De este modo, se configura una paradoja central: los instrumentos que, en términos funcionales, permiten a los usuarios escapar de las restricciones del sistema financiero local son, al mismo tiempo, aquellos que implican mayores niveles de dependencia respecto de actores específicos. La búsqueda de estabilidad y liquidez —características clave en un contexto de cultura económica defensiva, desconfiada y dolarizada— conduce a privilegiar soluciones que reproducen formas de centralización y de menor autonomía, aunque en infraestructuras tecnológicamente distintas.

En este sentido, la autonomía financiera asociada al ecosistema cripto no desaparece, pero adquiere un carácter relativo y condicionado. Más que eliminar intermediarios, el sistema tiende a reconfigurar sus formas, desplazando el eje desde las instituciones bancarias tradicionales hacia nuevos actores que operan en mercados globales y bajo marcos regulatorios externos. Esta transformación no implica necesariamente una mayor independencia, sino una redistribución de las dependencias, ahora ancladas en la liquidez, la menor volatilidad y la necesidad de acceso a instrumentos dolarizados.

En definitiva, la evidencia sugiere que el ecosistema cripto en Argentina no se organiza en torno a la promesa de descentralización, sino en función de una lógica pragmática de dolarización digital. Esta dinámica no solo redefine el alcance real de la autonomía financiera que estos instrumentos proyectan, sino que también plantea interrogantes relevantes sobre su rol en la reconfiguración de las relaciones entre usuarios, intermediarios y soberanía monetaria.

3.2. Inclusión financiera proyectada vs. concentración en usuarios bancarizados

El discurso en torno al ecosistema cripto suele asociarlo con un potencial democratizador, particularmente en contextos de alta informalidad y baja bancarización. En esta narrativa, los activos digitales —en especial las stablecoins— aparecen como herramientas capaces de ampliar el acceso a servicios financieros, facilitando el ahorro, las transferencias y la participación en la economía digital para sectores históricamente excluidos.

Esta visión encuentra sustento en distintas voces del ecosistema, que destacan su capacidad para habilitar nuevas formas de acceso. La posibilidad de operar sin requerir una cuenta bancaria tradicional, junto con la reducción de costos en transferencias internacionales y la disponibilidad de herramientas digitales, configura un escenario que, en principio, resultaría más inclusivo que el sistema financiero convencional.

Sin embargo, cuando se analiza la adopción efectiva, emergen tensiones significativas que relativizan esta narrativa. La evidencia empírica disponible —basada en un análisis cualitativo y cuantitativo de alcance acotado— muestra que el uso de stablecoins en Argentina no se distribuye de manera homogénea, sino que se concentra principalmente en usuarios que ya se encuentran integrados al sistema financiero formal. Esta concentración sugiere que, al menos en su fase actual, estos instrumentos funcionan más como herramientas de optimización para usuarios bancarizados que como mecanismos de inclusión para los sectores excluidos.

Esta dinámica puede explicarse por múltiples factores. En primer lugar, el acceso efectivo a estos instrumentos requiere condiciones previas que no se encuentran universalmente distribuidas, tales como conectividad, dispositivos tecnológicos y conocimientos básicos de operación digital. En segundo lugar, la complejidad del ecosistema, junto con los riesgos asociados, limita su adopción por parte de usuarios con menor educación financiera, reproduciendo así desigualdades preexistentes.

A ello se suma un elemento conceptual relevante: la propia noción de inclusión financiera puede resultar insuficiente para capturar la complejidad del fenómeno. En muchos casos, la inclusión suele

pensarse como un proceso lineal, en el que el acceso a una herramienta financiera equivale automáticamente a estar "dentro" del sistema. Sin embargo, esta mirada tiende a invisibilizar diferencias importantes en las condiciones de acceso, uso y protección entre los distintos segmentos de usuarios.

En este sentido, las stablecoins parecen operar más como una puerta de entrada a circuitos financieros más complejos que como una solución integral a la exclusión. Si bien permiten a ciertos usuarios ampliar sus opciones de ahorro e inversión, no eliminan las barreras estructurales que limitan el acceso de amplios sectores de la población. Por el contrario, su adopción puede reforzar dinámicas de segmentación, en las que los beneficios del ecosistema se concentran en perfiles con mayor capacidad de adaptación tecnológica y financiera.

En definitiva, la tensión entre inclusión proyectada y concentración real pone en evidencia uno de los límites estructurales del ecosistema cripto en Argentina. Lejos de constituir un mecanismo universal de democratización financiera, su desarrollo actual parece estar más vinculado a la reconfiguración de prácticas dentro de segmentos ya integrados que a la incorporación efectiva de nuevos usuarios.

3.3. Riesgo creciente vs. protección limitada del usuario

El crecimiento del ecosistema de stablecoins en Argentina plantea riesgos que trascienden la volatilidad de los activos y se concentran en aspectos operativos, regulatorios y tecnológicos. Estos riesgos afectan tanto a los usuarios como a los intermediarios y se vinculan con la falta de regulación clara, la sofisticación de los delitos financieros y las asimetrías de información. En este sentido, la expansión del uso no ha sido acompañada por un desarrollo equivalente de mecanismos de protección, configurando una primera tensión entre adopción creciente y resguardo insuficiente.

Una de las dimensiones centrales de este proceso se vincula con la facilidad de acceso al mercado. La posibilidad de operar en entornos no regulados —incluyendo transacciones entre pares o a través de intermediarios informales— reduce las barreras de entrada pero, al mismo tiempo, incrementa la exposición a riesgos. De este modo, una de las principales ventajas del ecosistema —su accesibilidad— se convierte también en un factor que amplía la vulnerabilidad de los

usuarios, al facilitar la migración hacia circuitos con menores niveles de supervisión.

Este escenario introduce un problema estructural: la coexistencia entre espacios regulados y no regulados genera incentivos desalineados, en los que los usuarios pueden optar por entornos más flexibles pero menos seguros. Si bien la normativa vigente ha avanzado en la incorporación de intermediarios dentro de esquemas de control, persiste una tensión entre regulaciones basadas en riesgo y exigencias formales que, en algunos casos, terminan desplazando a los usuarios hacia circuitos informales.

A su vez, la adopción de criptoactivos amplifica tipologías específicas de riesgo, particularmente en materia de prevención de lavado de activos y operaciones transfronterizas. La velocidad de las transacciones, su carácter global y la posibilidad de combinar canales formales e informales dificultan los procesos de trazabilidad efectiva, generando zonas de opacidad que pueden ser aprovechadas tanto para la circulación de fondos de origen dudoso como para la ejecución de esquemas fraudulentos.

En este punto emerge una segunda tensión relevante: si bien el uso de tecnologías digitales permite, en principio, un mayor nivel de registro y seguimiento de las transacciones, en la práctica estos mecanismos resultan limitados. Ello se debe a la combinación de canales formales e informales, a la heterogeneidad de los controles en los puntos de acceso al sistema y a la falta de marcos regulatorios plenamente desarrollados.

Otra dimensión crítica se relaciona con la naturaleza de los instrumentos más utilizados. Una parte significativa del uso local se concentra en stablecoins emitidas por entidades centralizadas. Esta característica introduce riesgos específicos vinculados al control sobre los activos, incluyendo la posibilidad de congelamiento de fondos o de decisiones unilaterales por parte de los emisores. En contextos donde estos actores operan bajo jurisdicciones extranjeras, los usuarios locales carecen de mecanismos claros de protección o reclamo, lo que amplifica su exposición.

A ello se suman factores operativos como la falta de transparencia en costos y comisiones, que refuerzan las asimetrías de información dentro del ecosistema y dificultan la toma de decisiones informadas por parte de los usuarios.

En definitiva, los riesgos asociados a las stablecoins en Argentina no responden a un único factor, sino a la interacción entre variables tecnológicas, regulatorias y sociales. Esta complejidad refleja una tensión estructural: a medida que el ecosistema se expande y facilita el acceso, también incrementa su superficie de riesgo, sin que exista un correlato equivalente en términos de mecanismos efectivos de protección.

3.4. Regulación fragmentada vs. límites estructurales del control estatal

El avance regulatorio del ecosistema cripto en Argentina no puede entenderse como un proceso de ausencia normativa, sino como una forma de regulación parcial que refleja tanto avances institucionales como limitaciones estructurales. En los últimos años, el Estado ha incorporado progresivamente a los actores más visibles del sistema —particularmente los intermediarios— dentro de esquemas de supervisión, adoptando estándares internacionales en materia de prevención de lavado de activos y control operativo.

Sin embargo, este proceso convive con un vacío significativo en relación con los instrumentos utilizados. Mientras que los proveedores de servicios sobre activos virtuales han sido objeto de regulación, los activos en sí mismos no cuentan con un encuadre normativo específico proporcional a su creciente relevancia económica. Esta disociación genera una primera tensión estructural: un sistema parcialmente regulado en el que se controlan los puntos de acceso, pero no el funcionamiento integral del ecosistema.

Esta fragmentación no responde únicamente a una falta de desarrollo normativo, sino a dificultades más profundas para adaptar marcos regulatorios tradicionales a un fenómeno que combina características descentralizadas, actores globales y estructuras híbridas de intermediación.

A ello se suma una segunda tensión, vinculada a la dimensión internacional del fenómeno. El desarrollo de estándares regulatorios globales, impulsados por organismos internacionales y jurisdicciones centrales, introduce presiones hacia la convergencia normativa a nivel local. En este sentido, la regulación aparece como un proceso en gran medida inevitable, no solo por los riesgos asociados al ecosistema, sino también por la necesidad de evitar sanciones o desalineamientos con marcos internacionales.

Sin embargo, esta inevitabilidad no se traduce en un consenso claro sobre su alcance ni sobre su efectividad. La regulación aparece simultáneamente como una demanda y como un objeto de crítica dentro del propio ecosistema. Por un lado, distintos actores impulsan la necesidad de contar con marcos normativos previsibles que reduzcan riesgos, faciliten el acceso a financiamiento y otorguen mayor legitimidad institucional. Por el otro, persisten cuestionamientos respecto de su utilidad, en la medida en que puede generar una falsa sensación de seguridad sin abordar los problemas estructurales vinculados a la centralización, la opacidad y la limitada protección del usuario.

Esta ambivalencia se profundiza al considerar los límites estructurales del control estatal. La naturaleza transnacional de los activos digitales, la centralización de los emisores en jurisdicciones extranjeras y la posibilidad de operar por fuera de intermediarios regulados dificultan la capacidad de los Estados para ejercer un control integral.

Esta tensión se vuelve particularmente relevante en el caso argentino, donde la regulación de activos digitales se inserta en un contexto marcado por la inestabilidad macroeconómica, la dolarización estructural y la desconfianza en las instituciones financieras. En este escenario, reconocer plenamente el rol de las stablecoins como medio de pago o reserva de valor implicaría, en la práctica, convalidar una forma de dolarización digital que podría afectar la soberanía monetaria y la capacidad de intervención del Estado.

Por el contrario, mantener un enfoque restrictivo o ambiguo en la regulación implica aceptar la existencia de un sistema paralelo que opera en zonas grises, con menores niveles de supervisión y mayores riesgos para los usuarios. De este modo, la política regulatoria enfrenta un dilema estructural: regular con mayor profundidad puede implicar legitimar dinámicas que tensionan el orden monetario, mientras que no hacerlo refuerza la fragmentación y debilita la capacidad de control.

En definitiva, la regulación fragmentada del ecosistema cripto refleja tanto el intento de adaptación de los marcos normativos existentes como la imposibilidad de ejercer un control integral sobre un sistema global, descentralizado en su diseño y centralizado en su funcionamiento práctico.

4. Reflexiones finales

El análisis del ecosistema cripto en Argentina permite identificar una serie de tensiones estructurales que atraviesan tanto su funcionamiento como su interpretación. Lejos de consolidar las promesas que suelen asociarse a estos desarrollos, la evidencia muestra que dichas promesas se reconfiguran en la práctica en formas más complejas y, en muchos casos, contradictorias.

En términos de autonomía, los criptoactivos en Argentina no parecen estar impulsando una descentralización plena, sino que se integran en dinámicas de dolarización digital que reproducen nuevas dependencias, particularmente en torno a emisores y estructuras centralizadas. Del mismo modo, la narrativa de inclusión financiera convive con patrones de adopción concentrados en usuarios ya bancarizados, lo que sugiere que estos instrumentos funcionan más como herramientas de eficiencia dentro del sistema que como mecanismos efectivos de incorporación de sectores excluidos.

Esta lógica se replica en el plano de los riesgos. A medida que el ecosistema se expande y facilita el acceso, también incrementa su superficie de vulnerabilidad, sin que exista un desarrollo equivalente de mecanismos de protección. La creciente complejidad operativa, la combinación de canales formales e informales y la centralización de actores clave configuran un entorno donde los riesgos no solo persisten, sino que tienden a amplificarse.

Finalmente, en el plano regulatorio, el desafío no se limita a la ausencia de normas, sino a la propia naturaleza del fenómeno. La regulación existente, centrada en intermediarios, resulta necesariamente fragmentaria frente a un ecosistema global y dinámico. A su vez, la presión por regular —impulsada tanto por organismos internacionales como por actores del propio mercado— convive con críticas sobre su efectividad y con límites estructurales que restringen la capacidad de control estatal.

El dilema no es únicamente cómo regular, sino hasta qué punto la regulación puede capturar un sistema que desborda los marcos tradicionales, especialmente en economías atravesadas por procesos de dolarización y desconfianza institucional. A ello se suma una dimensión adicional: el potencial impacto sobre la soberanía

monetaria. Reconocer o integrar plenamente a estos instrumentos dentro del sistema financiero puede implicar, en la práctica, convalidar formas de dolarización digital que reducen la capacidad del Estado para administrar la política monetaria.

Desde esta perspectiva, la regulación no solo enfrenta límites técnicos o jurídicos, sino también dilemas económicos y políticos: avanzar en su desarrollo puede resultar funcional a la estabilidad del ecosistema, pero al mismo tiempo puede consolidar dinámicas que, desde el punto de vista estatal, podrían resultar difíciles de sostener.

En conjunto, estas tensiones sugieren que el ecosistema cripto en Argentina no constituye una ruptura con el sistema financiero existente, sino una reconfiguración de sus lógicas estructurales en un nuevo entorno tecnológico. Más que explicar la dinámica económica local, estos desarrollos parecen estar condicionados por ella: no se trata de un fenómeno disruptivo, sino de una adaptación a una economía caracterizada por la inestabilidad, la dolarización y la desconfianza institucional.

En este contexto, lejos de ofrecer una solución estructural, los activos digitales tienden a integrarse en las mismas lógicas que buscan superar, complementando y tensionando al sistema financiero tradicional.

Bibliografía

Aginsky, A. (2023). *Blockchain por y para abogados*. https://es.scribd.com/document/747664528/Blockchain-por-y-para-abogadas-y-abogados

Argentina. Congreso de la Nación. (2024). Ley 27.739. Modificaciones a la Ley 25.246 (PLA/FT). https://www.mpf.gob.ar/procelac-mercado-de-capitales/normativa/ley-27-739-modificacion-para-operar-en-el-ambito-de-mercado-de-capitales/

Catalini, C. y Gans, J. S. (2016). Some simple economics of the blockchain. *MIT Sloan Research Paper No. 5191-16*. MIT Sloan School of Management. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2874598

Chainalysis. (2024). La búsqueda de estabilidad económica en América Latina: el auge de las monedas estables

en medio de la volatilidad. https://www.chainalysis.com/blog/2024-latin-america-crypto-adoption/

Comisión Nacional de Valores. (2024). Resolución General 994/2024. Registro de Proveedores de Servicios de Activos Virtuales (PSAV). https://www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-994-2024-397598

Comisión Nacional de Valores. (2025). Resolución General 1058/2025. Reglamentación PSAV: registro, supervisión y control. https://www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-1058-2025-410635

Financial Action Task Force. (2023). Virtual assets: Targeted update on implementation of the FATF Standards on VAs and VASPs. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2023.html

Luzzi, M. y Wilkis, A. (2019). *El dólar: Historia de una moneda argentina (1930–2019)*. Crítica.

Monzón, C. E. (2026). *Activos digitales en economías inestables: El potencial de las stablecoins en Argentina (2020–2025).* [Tesis de maestría, Universidad Nacional de San Martín].

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf

Sahay, R., Čihák, M., N'Diaye, P., Barajas, A., Mitra, S., Kyobe, A., Mooi, Y. N. y Yousefi, S. R. (2015). Financial inclusion: Can it meet multiple macroeconomic goals? *IMF Staff Discussion Note No. 15/17*. International Monetary Fund. https://www.imf.org/external/pubs/ft/sdn/2015/sdn1517.pdf

ISBN 978-631-92038-3-7