Investigaciones a ciegas:

¿Está preparado el Perú para enfrentar y combatir el Lavado de activos en el mundo de las criptomonedas?

Yandira Sapa Oruro*

Universidad Nacional de San Agustín

1. Introducción

Desde la creación del *Bitcoin* en 2009, las *criptomonedas* han revolucionado el sistema financiero global. Este nuevo panorama ha crecido exponencialmente, generando oportunidades sin precedentes en términos de inversión, inclusión financiera y descentralización de la economía. La promesa de un sistema sin intermediarios, donde las transacciones se realizan de manera rápida y con costos reducidos, ha atraído a millones de usuarios en todo el mundo. Sin embargo, esta misma estructura, que favorece la autonomía y la privacidad, también ha abierto la puerta a actividades ilícitas de gran escala, entre ellas el **lavado de activos.**

El Grupo de Acción Financiera Internacional (en adelante GAFI), organismo encargado de establecer estándares para la lucha contra el lavado de dinero y el financiamiento del terrorismo, ha señalado que las criptomonedas representan un desafío crítico para los sistemas de prevención y fiscalización de delitos financieros. Su capacidad de movilizar grandes sumas de dinero sin una supervisión efectiva, el uso de monederos anónimos y descentralizados, así como la facilidad para trasladar fondos a través de múltiples jurisdicciones, han convertido a estos activos en una herramienta atractiva para organizaciones criminales, cárteles de droga y redes de corrupción.

En América Latina, el uso de criptomonedas en esquemas de lavado de dinero ha crecido exponencialmente, con casos documentados de redes de narcotráfico, corrupción política y fraudes financieros utilizando Bitcoin, Tether y otras criptodivisas para ocultar fondos ilícitos.

Cabe precisar que las criptomonedas son activos digitales basados en tecnología blockchain, el cual es un registro descentralizado que almacena datos en bloques encadenados de forma segura, transparente e inmutable, permitiendo transacciones sin intermediarios y con alta trazabilidad. Hay que enfatizar que la mayoría de transacciones son anónimas. Bitcoin es la primera y más conocida criptomoneda, utilizada tanto como reserva de valor como medio de intercambio. Tether, por otro lado, es una stablecoin (criptomoneda estable) vinculada al valor del dólar estadounidense, diseñada para reducir la volatilidad de precios característica de otras criptomonedas. El término criptodivisas engloba a todas estas monedas digitales, que pueden ser utilizadas de manera legítima, pero también pueden facilitar

** Yandira Sapa Oruro, abogada por la Universidad Nacional de San Agustín (UNSA), egresada de la maestría en Ciencias Penales por la UNMSM. Ha sido asistente judicial en la Corte Superior Nacional y abogada de la Procuraduría del Poder Judicial; actualmente abogada del Estudio Jurídico Loza Ávalos.*

actividades ilícitas debido a la dificultad de rastrear sus transacciones. En países con regulaciones frágiles o con sistemas de fiscalización ineficientes, estas operaciones ocurren con facilidad y casi total impunidad.

Perú no es ajeno a esta problemática. A pesar del crecimiento del mercado cripto en el país y el aumento de operaciones financieras a través de activos digitales, la respuesta del sistema de justicia peruano sigue siendo deficiente y lenta. Actualmente, no existen mecanismos adecuados de rastreo y control, como sí se ha implementado últimamente en la Unión Europea a través del Reglamento sobre Mercados de Criptoactivos[1] (en adelante Reglamento MiCA) que establece que los agentes económicos deban obtener licencia para comercializar y donde se regula un proceso de verificación de la propiedad de monederos digitales con criptoactivos que superan los 1000 euros, por ejemplo.

Además, las leyes contra el lavado de dinero a nivel internacional como la Anti Money Laundering o Ley contra el lavado de dinero (en adelante AML) proponen directrices contables y de transparencia sobre criptoactivos ejecutadas por organismos reguladores como los supervisores de las Virtual Asset Service Provider o Proveedor de Servicios de Activos Virtuales (VASP)[2] Estas políticas son consecuencia de una progresiva codificación de las recomendaciones de la GAFI.

No obstante, en nuestro país, además de que no hay una legislación específica para la regulación o supervisión de criptoactivos, se puede desprender que esto se debe al desconocimiento en estos tópicos. Es de esta manera que las autoridades enfrentan serias limitaciones en términos de capacitación, tecnología y regulación. Así que es inevitable que surjan las siguientes preguntas:

- **¿Cuenta el Estado, a través del Ministerio Público, con herramientas efectivas para rastrear transacciones en blockchain?**

- **¿Tenemos jueces y fiscales especializados y el conocimiento necesario para diferenciar entre un operador legítimo de criptomonedas y un esquema de lavado de dinero?**

La realidad es que Perú no está preparado para enfrentar los casos de lavado de activos a través de criptoactivos, esto en el entendido de que las criptomonedas son el mecanismo o instrumento para la conversión, colocación o integración del dinero ilícito. A diferencia de otras jurisdicciones (países como Argentina y España), donde se han implementado regulaciones

[1] Este reglamento entró en vigor desde el 30 de diciembre de 2024 en la UE; se caracteriza por poseer un marco regulatorio de transparencia, así como determina las obligaciones que deben cumplir los proveedores y oferentes de criptoactivos. En "Reglamento europeo sobre los criptoactivos (MiCA)", EUR-Lex, con acceso el 25 de setiembre del 2024, https://eur-lex.europa.eu/ES/legal-content/summary/european-crypto-assets-regulation-mica.html.

[2] FATF. Financial Action Task Force - Annual Report 2019-2020, FATF/OECD. Paris, 2019. En este informe se recomienda que se incluya dentro de la regulación de criptoactivos a los supervisores de VASP, quienes obtienen información sobre los oferentes y beneficiarios intervinientes en las transferencias de criptoactivos.

claras y unidades especializadas en la investigación de delitos financieros digitales. Nuestro país sigue operando con métodos tradicionales que resultan ineficaces ante un fenómeno de esta magnitud.

2. Criptomonedas y su rol en el delito de lavado de activos

Las criptomonedas han emergido como una alternativa financiera innovadora, funcionando como activos digitales que permiten transferencias de valor sin intermediarios a través de la tecnología blockchain. Este sistema descentralizado garantiza seguridad, transparencia e inmutabilidad en las transacciones; pero también introduce serios desafíos regulatorios, especialmente en la prevención del lavado de dinero y el financiamiento del crimen organizado. A diferencia de los sistemas bancarios tradicionales, donde los movimientos de capital están sujetos a estrictos controles, las criptomonedas pueden circular a nivel global con mínima supervisión, lo que facilita su uso en actividades ilícitas.

Existen dos formas principales de adquisición y comercialización de criptomonedas: centralizada y descentralizada. En la modalidad centralizada, intervienen terceros que facilitan las transacciones tales como las plataformas de exchanges centralizados (CEX) como Binance y Kraken que, aunque permiten la compra y venta de activos digitales, actúan como intermediarios para que bien apliquen ciertas regulaciones o bien ellos mismos exigen los procesos de verificación de identidad (KYC – Know Your Customer); no obstante, no siempre cumplen con los estándares internacionales de prevención de lavado de activos. En contraste, bajo el esquema descentralizado, los usuarios operan directamente entre sí sin intermediarios, por ejemplo, dentro de los mercados P2P (peer to peer) que permiten transacciones directas entre los mismos usuarios, sin intermediación bancaria ni verificación obligatoria, lo que convierte a esta modalidad en un punto crítico para la circulación de fondos ilícitos. Ello permite la posibilidad de operar bajo seudónimos y direcciones alfanuméricas, sin que los participantes conozcan el verdadero origen de los fondos, es decir, un factor de alto riesgo en la lucha contra el lavado de dinero.

La delincuencia organizada transnacional ha fortalecido su capacidad para explotar las vulnerabilidades del sistema financiero mediante el uso de mixers y tumblers. Estos servicios están diseñados para fragmentar y mezclar criptomonedas de diferentes usuarios, con el objetivo de ocultar el origen y destino de los fondos, dificultando así su rastreo. Al combinar múltiples transacciones, los mixers aumentan la privacidad de las operaciones, pero también pueden ser utilizados para actividades ilícitas, como el lavado de dinero.

Un caso emblemático es el de Silk Road[3], un mercado negro en línea que operó en la red Tor entre 2011 y 2013. En este sitio, se facilitaban transacciones anónimas de bienes y servicios ilegales, utilizando Bitcoin como medio de pago. En noviembre de 2021, las autoridades incautaron más de 50,676 Bitcoins, valorados en aproximadamente 3,360 millones de dólares, que habían sido

[3] El fundador de una plataforma que funcionaba en la web oscura para fines del tráfico de sustancias ilícitas fue condenado en junio del 2015.

robados de Silk Road en 2012 por James Zhong, quien empleó técnicas para ocultar el origen de los fondos, complicando su rastreo durante años. Además, la utilización de "mulas financieras", individuos reclutados para recibir y transferir dinero sin conocer su origen ilícito, es una estrategia común en delitos de fraude y estafas digitales. Estas personas, a menudo inconscientes de su participación en actividades ilegales, facilitan el movimiento de fondos obtenidos de manera fraudulenta, complicando la detección y prevención del lavado de dinero.

La combinación de mixers, tumblers y mulas financieras representa un desafío significativo para las autoridades en la lucha contra el lavado de dinero y otros delitos financieros, especialmente en países donde la regulación y supervisión de las criptomonedas aún están en desarrollo.

Otro ejemplo notable es el esquema Ponzi conocido como **PlusToken**[4], que operó principalmente en China y Corea del Sur desde abril de 2018. PlusToken prometía altos rendimientos a los inversores a través de su billetera de criptomonedas y su token asociado. Se estima que los operadores de PlusToken defraudaron entre 2,000 y 2,900 millones de dólares en criptomonedas. En 2019, varios sospechosos fueron arrestados, y en 2020, las autoridades chinas detuvieron a 109 personas relacionadas con el esquema, incluyendo a sus líderes principales.

A nivel internacional, organismos como la GAFI han instado a los gobiernos a regular las criptomonedas bajo estándares más estrictos, exigiendo la identificación de usuarios en exchanges y el reporte de transacciones sospechosas a las Unidades de Inteligencia Financiera (en adelante UIF). En la Unión Europea, el Reglamento MiCA establece normativas para la supervisión de activos digitales, mientras que en Estados Unidos, tribunales han dictado sentencias ejemplares contra plataformas que facilitan el blanqueo de capitales, como en el caso U.S. v. **Harmon**[5], donde un operador de un servicio de mezcla de Bitcoin fue condenado por violar regulaciones AML.

En contraste, Perú carece de un marco legal robusto y mecanismos tecnológicos para rastrear transacciones con criptomonedas en operaciones delictivas. Actualmente, el país enfrenta una brecha en la regulación financiera digital, dejando al sistema judicial sin herramientas efectivas para investigar y sancionar el lavado de dinero mediante activos digitales. La falta de capacitación en análisis forense de blockchain, junto con la ausencia de unidades especializadas en criptodelitos, pone en

[4] "Las autoridades chinas han incautado 4,2 millones de dólares a los directores del Plus Token". Bitcoin.es, acceso el 27 de noviembre de 2020, https://bitcoin.es/noticias/las-autoridades-chinas-han-incautado-42-millones-de-dolares-a-los-directore s-del-plus-token/.

[5] De fecha 29 de febrero de 2024; en esta sentencia la Corte argumenta que su decisión se fundamenta convenientemente en informes de expertos sobre el análisis de los blockchain. Detalla que se basa en la información brindada por las principales bolsas de divisas virtuales y otras financieras, las cuales utilizan herramientas de software de análisis de cadenas de bloques como parte de sus programas contra el blanqueo de dinero para cumplir con sus obligaciones regulatorias y monitorear las transacciones en busca de actividades sospechosas, así como también confían en la precisión del software Chainalysis la cual posee alta credibilidad dentro del ecosistema de criptoactivos.

riesgo la integridad del sistema financiero y expone al país a convertirse en un punto ciego en la lucha contra el crimen financiero digital. Para cerrar esta brecha, es fundamental que el Estado implemente reformas legislativas, coopere con organismos internacionales y capacite a fiscales y jueces en tecnologías de rastreo financiero, evitando así que Perú se convierta en un refugio para el lavado de activos digitales.

3. El caso peruano: Falencias y Desafíos en la Investigación del Lavado de Activos con Criptomonedas

El sistema de justicia peruano enfrenta graves deficiencias en la fiscalización y regulación del lavado de activos a través de criptomonedas, debido a la falta de un marco normativo claro y herramientas tecnológicas adecuadas para la supervisión de transacciones digitales. A diferencia de países como Estados Unidos y la Unión Europea, donde se han implementado normativas AML específicas para activos digitales, Perú carece de leyes precisas que regulen la operatividad de las criptomonedas y su uso en actividades ilícitas. De acuerdo con Zohar y Meiklejohn[6], la ausencia de una legislación clara no solo dificulta la detección de operaciones sospechosas, sino que genera un vacío legal que permite a los criminales mover fondos sin restricciones bancarias ni supervisión estatal. Este problema se agrava si no hay una colaboración más reforzada, sobre todo en capacitación, entre los organismos reguladores nacionales, como la UIF y el Ministerio Público, lo que deja a las autoridades sin acceso a herramientas avanzadas para rastrear flujos ilícitos en la blockchain.

Uno de los principales desafíos en la lucha contra el lavado de activos con criptomonedas en Perú es la dificultad para rastrear fondos ilícitos debido a la falta de herramientas tecnológicas especializadas y la escasez de personal capacitado en análisis forense de blockchain. La naturaleza descentralizada y pseudónima de muchas criptomonedas permite que los delincuentes oculten el origen y destino de los fondos, dificultando su identificación por parte de las autoridades.

En jurisdicciones como Alemania y Canadá, los organismos de justicia han desarrollado unidades especializadas en el rastreo de transacciones en blockchain, utilizando herramientas avanzadas como Chainalysis, Elliptic y CipherTrace. Estas plataformas son esenciales para la detección y análisis de actividades sospechosas en el ecosistema de criptoactivos:

- Chainalysis es una empresa de análisis de blockchain que proporciona herramientas de inteligencia financiera para rastrear transacciones en criptomonedas. Sus soluciones permiten a gobiernos y empresas detectar patrones de lavado de dinero, identificar actores ilícitos y desmantelar redes criminales que utilizan activos digitales. Es utilizada por agencias como el FBI y la Europol.

- Elliptic ofrece soluciones de monitoreo y cumplimiento normativo para instituciones financieras y gubernamentales, ayudándolas a identificar transacciones vinculadas con el financiamiento del terrorismo, narcotráfico y otros delitos. Su tecnología

[6] Zohar y Meiklejohn. Cryptocurrency and Financial Crime. 2019.

utiliza inteligencia artificial y análisis de datos en blockchain para asignar niveles de riesgo a direcciones y billeteras sospechosas.

- CipherTrace, ahora propiedad de Mastercard, se especializa en la identificación de transacciones fraudulentas y el rastreo de criptomonedas utilizadas en actividades ilícitas. Su plataforma permite a reguladores y bancos evaluar el riesgo de criptoactivos y garantizar el cumplimiento de normativas contra el lavado de dinero.

En contraste, Perú no cuenta con plataformas tecnológicas especializadas ni con unidades de análisis forense de blockchain, lo que impide a fiscales, jueces y organismos reguladores rastrear el origen y destino de los criptoactivos. Esta brecha tecnológica y operativa limita significativamente la capacidad del Estado para procesar casos de lavado de dinero en el entorno digital, permitiendo que las redes criminales continúen operando con relativa impunidad.

El sistema judicial peruano y los organismos de control financiero presentan serias limitaciones frente al auge de los activos digitales, lo que ha permitido que redes criminales exploten estas vulnerabilidades para blanquear capitales sin ser detectadas. En Estados Unidos, en el antes referido caso United States v. Harmon se demostró la eficacia del uso de pruebas forenses de blockchain en la condena de un operador de un servicio de mezclado de Bitcoin utilizado para lavar más de $300 millones en criptomonedas. En contraste, en Perú no existen precedentes judiciales donde se haya procesado exitosamente un caso de lavado de activos con criptoactivos, debido a la falta de protocolos de investigación adecuados y unidades especializadas en delitos financieros digitales.

4. Recomendaciones y Medidas Urgentes

Para enfrentar eficazmente el lavado de activos a través de criptomonedas, es imperativo que el sistema de justicia peruano implemente un programa integral de capacitación en tecnología blockchain dirigido a fiscales, jueces y cuerpos policiales. En países como Estados Unidos y Alemania, se han establecido unidades de cibercrimen financiero especializadas en el rastreo de transacciones en la blockchain, utilizando herramientas avanzadas como Chainalysis y Elliptic para identificar operaciones ilícitas. Zohar y Meiklejohn [7]la falta de conocimiento técnico entre los operadores judiciales es uno de los mayores obstáculos en la persecución del lavado de activos digitales. Además, Perú debe armonizar su legislación con los estándares internacionales establecidos por el GAFI (Grupo de Acción Financiera Internacional), adoptando regulaciones similares al Reglamento MiCA de la Unión Europea, que exige la identificación obligatoria de usuarios en exchanges y la notificación de transacciones sospechosas a las UIF. Asimismo, es crucial la creación de unidades especializadas en delitos financieros digitales dentro del Ministerio Público y la Policía Nacional, con acceso a tecnología de

[7] Zohar y Meiklejohn. Cryptocurrency and Financial Crime. 2019

rastreo y análisis de criptoactivos. En Estados Unidos, el caso United States v. Bitcoin Fog[8] se evidenció cómo la cooperación entre agencias especializadas y el uso de pruebas forenses de blockchain permitió desmantelar una red que lavó más de $335 millones en criptomonedas. Siguiendo este modelo, Perú debe fortalecer la colaboración con exchanges regulados y plataformas de criptomonedas, exigiendo que cumplan con normativas AML y compartan información sobre transacciones de alto riesgo. Los periodistas Vigna y Casey[9] enfatizan que la cooperación internacional entre jurisdicciones es fundamental para evitar que los activos digitales se utilicen como refugio para el crimen organizado. Sin estas reformas urgentes, **Perú seguirá rezagado en la lucha contra el lavado de dinero digital, permitiendo que su sistema financiero sea explotado por redes criminales transnacionales.**

5. Conclusiones

Primero, Perú no está preparado para investigar el delito de lavado de activos con criptomonedas, lo que convierte a estas investigaciones en un ejercicio especulativo y arbitrario. La falta de regulación específica, herramientas tecnológicas adecuadas y personal capacitado impide que las autoridades puedan seguir el rastro de los criptoactivos con precisión. A diferencia de países como Estados Unidos y bloques económicos como la Unión Europea, donde se han desarrollado unidades especializadas en análisis de blockchain, en Perú no existen protocolos efectivos para detectar, rastrear y sancionar operaciones ilícitas con criptomonedas. Investigar sin contar con conocimientos técnicos adecuados no solo es ineficaz, sino que también abre la puerta a errores judiciales y acusaciones infundadas.

Por lo tanto, el Estado peruano está llevando a cabo investigaciones "a ciegas", lo que genera un grave riesgo de vulneración de derechos fundamentales. Según los principios del **debido proceso y legalidad penal,** una investigación debe basarse en pruebas sólidas y metodologías verificables con un sistema de justicia eficaz. Sin embargo, en el caso de los criptoactivos, ni la Fiscalía ni la Policía cuentan con las herramientas necesarias para analizar transacciones en blockchain con rigor técnico, lo que viola el derecho a la defensa y genera procesos viciados de nulidad. En otros países como Alemania y Canadá, la persecución de estos delitos se realiza con pericias especializadas y el uso de inteligencia artificial para el rastreo de fondos, elementos que Perú no posee en su arsenal investigativo, puesto que muchas veces solo se limita a las pericias contables.

Sin una legislación clara y alineada con estándares internacionales, nuestro país está criminalizando operaciones legítimas sin distinguir entre el comercio legal de criptomonedas y el lavado de activos. En la Unión Europea, el Reglamento MiCA (2023) ha establecido lineamientos claros sobre la trazabilidad de los criptoactivos, mientras que en Perú las autoridades aún no han definido criterios específicos para diferenciar entre actividades legítimas y operaciones ilícitas. Esta falta de regulación adecuada

[8] De fecha 29 de febrero de 2024.
[9] Michael Casey y Paul Vigna. The Truth Machine: The Blockchain and the Future of Everything. (St. Martin's Press, 2018).

condena a personas inocentes a procesos penales injustificados, basados en interpretaciones erróneas y sin fundamentos técnicos sólidos. La ausencia de especialización convierte a las investigaciones en juicios de intenciones y no en análisis forenses verificables.

Por ello, la falta de capacitación en tecnología blockchain y la falta de cooperación internacional efectiva, tornan a las investigaciones en carentes de validez técnica y jurídica. En nuestro país, no existe un equipo especializado ni se faculta el acceso a softwares forenses de criptoanálisis, lo que impide determinar con certeza el origen de los fondos y su destino. Investigar delitos financieros digitales sin los recursos adecuados es equivalente a procesar a alguien sin pruebas, basándose en suposiciones en lugar de hechos verificables, lo que representa una violación flagrante del derecho a la defensa y al principio de presunción de inocencia de todo ser humano en un Estado de derecho.

6. Referencias

Casey, Michael y Vigna, Paul. The Truth Machine: The Blockchain and the Future of Everything. St. Martin's Press, 2018.

Zheng, Zibin y et al. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. 6th International Congress on Big Data, 2017.

Zohar y Meiklejohn. Cryptocurrency and Financial Crime. 2019.