

Hacia una Regulación Blockchain Funcional y Basada en Riesgos en América Latina: El Caso de Ecuador y Modelos Comparados

Escrito por: Abogado Edwin Gabriel Mejía Rodríguez. Especializado en Derecho Digital, Inteligencia Artificial y Blockchain.

Introducción

El auge de las tecnologías blockchain y los criptoactivos en América Latina ha llevado a una proliferación de propuestas legislativas “maximalistas” que buscan regular este fenómeno de forma integral. Sin embargo, regular todo lo relacionado con blockchain mediante leyes generales puede resultar contraproducente si se carece de sustento técnico e institucional. Un ejemplo ilustrativo es el proyecto de Ley Orgánica sobre Uso y Regulación de Tecnologías Blockchain en Ecuador, cuyo fracaso legislativo evidenció los riesgos de un entusiasmo regulatorio descontextualizado. Este artículo ofrece una crítica jurídica profunda a dichas propuestas maximalistas, abogando por una regulación funcional, sectorial, escalonada y basada en riesgos, alineada con estándares internacionales (GAFI/FATF, MiCA, GENIUS Act, entre otros) y adaptada a las realidades locales. A través de un enfoque comparado, se analizan modelos regulatorios recientes en la región – Brasil, Chile, Argentina, así como los avances en Paraguay, Colombia, Perú y Bolivia – para extraer lecciones que orienten una hoja de ruta regulatoria más sólida para Ecuador. Se abordan de manera sistemática: **(i)** las razones del fracaso legislativo en Ecuador; **(ii)** los principios de una regulación funcional y por riesgos; **(iii)** los riesgos específicos del ecosistema cripto latinoamericano (lavado de activos, minería ilegal, flujos ilícitos); **(iv)** elementos clave de una regulación regional técnicamente viable; **(v)** desafíos en protección de datos y privacidad; y **(vi)** conclusiones enfocadas en una gobernanza digital legítima, con seguridad jurídica y responsabilidad institucional. La intención es generar una reflexión que evite afirmaciones infundadas, destacando la importancia de no importar modelos legales sin la debida contextualización.

I. El fracaso del proyecto de Ley Blockchain en Ecuador: causas y lecciones

El proyecto de Ley Orgánica de Blockchain en Ecuador, finalmente archivado por la Asamblea Nacional en octubre de 2025, ejemplifica cómo una iniciativa legislativa bien intencionada puede naufragar por falta de armonía con el ordenamiento vigente y ausencia de sustento técnico. El Pleno de la Asamblea decidió archivar el proyecto tras concluir que *“no guarda armonía con el ordenamiento legal vigente ni garantiza los principios de seguridad jurídica, protección de datos personales y sostenibilidad financiera”*. La presidenta de la comisión legislativa respectiva, Cecilia Baltazar, advirtió que regular una tecnología en rápida evolución podía *“limitar su desarrollo y generar conflictos con las competencias del Banco Central y los organismos de control financiero”*. En efecto, el proyecto ecuatoriano pretendía crear un marco normativo integral para blockchain, imponiendo principios de innovación, neutralidad tecnológica, transparencia, trazabilidad y protección de datos, así como una nueva Comisión Nacional de Blockchain bajo el Ministerio de Telecomunicaciones. No obstante, esta ambiciosa propuesta resultó *“incoherente con la normativa nacional”* y evidenció *“un entusiasmo mal gestionado, sin respaldo técnico”*.

Entre las razones del fracaso legislativo se pueden identificar: **(a) Conflictos constitucionales y monetarios:** Ecuador es una economía dolarizada, y cualquier normativa sobre activos digitales debía cuidarse de no vulnerar el régimen monetario vigente. Expertos del Banco Central alertaron que una ley apresurada podría incluso *“vulnerar el régimen de dolarización vigente”* si permitía la circulación de criptoactivos como dinero alternativo sin el debido control. **(b) Superposición normativa y vacíos de competencia:** El proyecto invadía ámbitos ya regulados por otras leyes y entidades. Por ejemplo, pretendía regular tokens de

valor (que podrían caer bajo normativa de mercado de valores) y aspectos de medios de pago digitales (competencia natural del Banco Central), creando redundancias y posibles choques de competencias. **(c) Falta de preparación técnica e institucional:** Tras varias comparecencias, organismos como la Superintendencia de Bancos y la de Compañías coincidieron en que el país aún carecía de la *“madurez técnica y jurídica necesaria”* para legislar sobre una tecnología tan compleja. Esto refleja un vacío de gobernanza: no se contaba con una autoridad experta ni con estudios de impacto suficientes. Regular sin comprender profundamente el fenómeno, ya sea por parte del ecosistema local o del propio Estado es, como se ha señalado, *“imprudente y potencialmente contraproducente”*. **(d) Promesas tecnológicas sin sustento:** El discurso que acompañaba al proyecto sugería que la adopción de blockchain, per se, traería transparencia y prevención de ilícitos. Sin embargo, el informe técnico recalcó que las herramientas basadas en blockchain *“no garantizan por sí solas la prevención del lavado de activos”* y que su implementación exige una infraestructura institucional fuerte. En otras palabras, se intentó legislar presumiendo beneficios automáticos de la tecnología, cuando en realidad su efectividad depende de las condiciones de aplicación.

En suma, el fallido proyecto ecuatoriano deja lecciones claras: la regulación de las tecnologías emergentes no debe acelerarse sin un diagnóstico riguroso; debe respetar la arquitectura legal existente (en lugar de contradecirla) y requerirá construir capacidad institucional antes que crear entes nuevos sin experiencia, evidenciando la necesidad de enfoques más graduales y técnicos, en contraposición al maximalismo legislativo.

II. Principios para una regulación funcional, escalonada y basada en riesgos

A la luz de estas lecciones, resulta imperativo definir los principios rectores de una regulación sobre blockchain y criptoactivos que sea eficaz y sostenible. Varios estándares internacionales brindan guía en este sentido, privilegiando un enfoque funcional y basado en riesgos en lugar de normas omnipresentes dictadas por la moda tecnológica.

Neutralidad tecnológica y enfoque funcional: Un primer principio es que la ley debe centrarse en las funciones económicas o actividades que se desarrollan (p. ej., toma de depósitos, intermediación financiera, custodia de activos, emisión de valores) y no en la tecnología por sí misma. Esto evita tanto lagunas como duplicidades. Por ejemplo, si un “token” se utiliza como valor mobiliario (security token), debería encuadrarse bajo la regulación de mercado de valores existente, con las adaptaciones necesarias, en lugar de crear una categoría jurídica completamente aislada. Este fue el enfoque de países como Chile y México, que incluyeron a los activos virtuales dentro de sus marcos fintech generales, sin dictar una “ley blockchain” específica. La Ley Fintech chilena (Ley N°21.521, 2022) promueve la innovación financiera y mantiene la neutralidad tecnológica, extendiendo el perímetro regulatorio de la Comisión para el Mercado Financiero (CMF) a nuevos servicios como plataformas de transacción de criptomonedas, custodia de criptoactivos, asesoría en inversión automatizada, etc. En lugar de regular en abstracto “la blockchain”, se regula la intermediación financiera basada en tecnología, equiparando obligaciones (transparencia, gestión de riesgos, reporte de operaciones sospechosas) para quienes ofrezcan servicios con criptoactivos de forma análoga a otros actores financieros. Este paradigma funcional garantiza piso parejo y evita tanto vacíos regulatorios como la sobre-regulación tecnológica.

Gradualidad y regulación escalonada: Dada la veloz evolución del ecosistema cripto, los reguladores recomiendan adoptar esquemas escalonados o sandboxes regulatorios antes de promulgar normas rígidas. Un sandbox permite pruebas controladas de proyectos con criptoactivos bajo supervisión, lo que *“fomenta la innovación dentro de un marco controlado”*. Colombia ha sido pionera regional al implementar en 2021–2022 la Arenera, un sandbox donde exchanges de criptomonedas operaron temporalmente en alianza con bancos para

ensayar medidas de seguridad y trazabilidad. Esta experiencia piloto brindó insumos valiosos para delinear regulaciones permanentes, a la vez que mitigó riesgos durante la experimentación. La adopción de proyectos piloto y fases graduales de implementación también caracteriza el enfoque prudencial de países como Bolivia, que, tras años de prohibición absoluta, en 2025 pasó a una “*apertura regulada*” mediante programas experimentales y decretos progresivos antes de cualquier ley integral. La gradualidad permite corregir rumbo conforme se aprende, en contraste con la rigidez de una ley maximalista promulgada de una vez.

Enfoque basado en riesgos (Risk-based approach): Inspirada en estándares de GAFI/FATF, la regulación debe asignar recursos y exigencias en proporción al riesgo de cada actividad o entidad. Esto implica diferenciación por tipo de actor y tamaño (“proporcionalidad”) y por tipo de criptoactivo. Por ejemplo, la Unión Europea con MiCA (Markets in Crypto-Assets Regulation) distingue entre categorías de tokens: las stablecoins significativas (e-money tokens o asset-referenced tokens de gran volumen) estarán sujetas a requisitos mucho más estrictos, incluyendo autorización previa, auditorías, reservas de respaldo y supervisión de la Autoridad Bancaria Europea, mientras que para tokens no referenciados se prevén requisitos más ligeros. Asimismo, MiCA estableció umbrales para identificar emisores “significativos” cuyas monedas estables pasan a supervisión especial si alcanzan cierto volumen de usuarios, capitalización o transacciones. Esta es una forma de regulación escalonada por nivel de riesgo: *“si un emisor de stablecoin alcanza la condición de significativo, pasa bajo supervisión más estricta”*. Por otro lado, se exime del perímetro regulatorio a actividades verdaderamente descentralizadas o puramente P2P sin intermediarios identificables, dado que MiCA no aplica plenamente a negociaciones totalmente descentralizadas ni a criptoactivos sin emisor identificable (e.g. Bitcoin), reconociendo los límites prácticos de la supervisión pública en esos casos. Este enfoque de graduar la intensidad regulatoria según el riesgo busca eficacia (foco en lo que realmente puede generar perjuicio sistémico o al usuario) y eficiencia (no ahogar la innovación de bajo riesgo con cargas innecesarias).

Alineación con estándares internacionales: Un principio transversal es asegurar la compatibilidad internacional de la regulación. Dado el carácter global de las redes blockchain, cualquier regulación aislada que se aparte drásticamente de las recomendaciones reconocidas puede generar arbitraje regulatorio o aislamiento financiero. Por ello, la normativa debe incorporar las recomendaciones del Grupo de Acción Financiera Internacional (GAFI) en materia de activos virtuales (Recomendación 15 y 16), las cuales exigen que los Proveedores de Servicios de Activos Virtuales (VASPs/PSAV) estén sujetos a obligaciones de prevención de lavado equivalentes a las de instituciones financieras tradicionales. Varios países latinoamericanos ya han ajustado sus marcos ALD/CFT en ese sentido: por ejemplo, Paraguay mediante la Resolución SEPRELAD 314/2021 incluyó a toda persona o empresa que realice actividades con activos virtuales (intercambio, transferencia, custodia, minería, etc.) como sujeto obligado bajo la Ley 1015/1997 de lavado de activos, imponiendo KYC, monitoreo de transacciones y reporte de operaciones sospechosas en línea con los estándares GAFI. Argentina, por su parte, en marzo de 2024 reformó su ley antilavado (Ley 27.739) para crear la categoría legal de VASPs y asignar a la Comisión Nacional de Valores (CNV) la tarea de establecer un marco regulatorio integral para la industria cripto, enfatizando la protección al usuario, seguridad informática, protección de datos personales, transparencia y buenas prácticas de gobierno corporativo en el sector. Esta reforma argentina obliga a los proveedores cripto a registrarse ante la CNV y cumplir medidas ALD/FT, y surgió precisamente para alinear al país con las exigencias internacionales luego de una larga ausencia de marco legal. Del mismo modo, una regulación ecuatoriana sensata deberá insertarse en ese consenso global: asegurar que los exchanges locales apliquen la “regla de viaje” (travel rule) para compartir información de origen/destino en transferencias cripto, exigir

debida diligencia intensificada en productos de mayor riesgo (como servicios de mixing o stablecoins algorítmicas), etc., tal como recomiendan GAFI y las nuevas regulaciones europeas.

Institucionalidad clara y coordinación sectorial: Un principio adicional es definir con claridad qué entidad reguladora se encarga de cada ámbito, aprovechando las competencias sectoriales existentes en vez de crear organismos ad hoc sin experiencia. La legislación y práctica comparada sugiere que una arquitectura institucional híbrida puede funcionar: en Brasil, la Ley 14.478/2022 (Marco Legal de Activos Virtuales) estableció lineamientos generales y el Poder Ejecutivo designó al Banco Central de Brasil (BCB) como autoridad encargada de licenciar y supervisar a los prestadores de servicios de activos virtuales (VASP). En desarrollo de ello, Brasil emitió el Decreto 11.563/2023 que formalizó la competencia del BCB, y este Banco Central ya ha avanzado en regulaciones secundarias (por ejemplo, consultas públicas sobre requisitos de capital, gobernanza y la implementación de la regla de viaje para exchanges). Paralelamente, la autoridad de mercados (CVM) conserva atribuciones si un criptoactivo califica como valor. Este reparto deja los pagos y cambios de criptomonedas bajo el ala del regulador bancario, asegurando supervisión prudencial, mientras que los tokens con características de valores o instrumentos financieros quedan sujetos a la normativa de valores – un enfoque sectorial coherente. Siguiendo esa lógica, en Ecuador podría aprovecharse el andamiaje de la Superintendencia de Bancos, la de Compañías y el Banco Central, coordinados mediante un comité interinstitucional, en lugar de concentrar todo en una nueva “Comisión de Blockchain” sin recorrido (como proponía el fallido proyecto). La coordinación interinstitucional es crucial también para abordar los criptoactivos de forma integral: Chile, por ejemplo, con la Ley Fintech involucró tanto a su Banco Central (en temas de sistemas de pago, moneda digital y stablecoins) como a la CMF (en ámbitos de valores, intermediación y open finance), reconociendo que distintos reguladores tienen mandatos concurrentes en este ecosistema y necesitan un enfoque concertado.

En síntesis, una regulación “inteligente” sobre blockchain debe ser *tecnológicamente neutral*, centrada en las funciones económicas subyacentes; gradual y adaptable, mediante pilotos o implementación escalonada; proporcional al riesgo, distinguiendo actores sistémicos de actores menores, y distintos tipos de criptoactivos según su uso; armonizada internacionalmente en materias clave (especialmente ALD/CFT); y sustentada en una institucionalidad clara, aprovechando y coordinando a los reguladores existentes. Estos principios sientan las bases para normativas eficaces, evitando tanto lagunas legales como excesos bienintencionados que pudieran sofocar la innovación o contravenir otros marcos.

III. Riesgos específicos del ecosistema cripto en América Latina: lavado, minería ilegal y flujos ilícitos

Cualquier esquema regulatorio funcional debe responder a los riesgos reales que presentan los criptoactivos en el contexto latinoamericano. Entre los más acuciantes se encuentran: **(1) el lavado de activos** y financiamiento ilícito mediante cripto; **(2) la minería ilegal** (explotación ilícita de recursos naturales facilitada por cripto); y **(3) los flujos ilícitos transfronterizos**, que incluyen evasión de controles cambiarios, fuga de capitales y movimientos ligados a actividades criminales. Analizamos cada uno brevemente y cómo la regulación puede mitigar estos riesgos.

Lavado de activos y financiamiento del terrorismo (LA/FT): La posibilidad de mover valor fuera del sistema financiero tradicional mediante criptomonedas ha atraído a organizaciones criminales que buscan ocultar el origen de fondos ilícitos. América Latina, con economías fuertemente afectadas por el narcotráfico, la corrupción y otros delitos rentables, enfrenta el

peligro de que redes criminales usen exchanges locales o servicios P2P para blanquear dinero. De hecho, Argentina, uno de los países con mayor adopción cripto debido a la depreciación del peso, reconoció que hasta 2024 “*carecía de un marco legal para cripto*” y que la CNV mantenía un enfoque laxo, lo que generaba un vacío en materia de prevención de lavado. La reacción vino con la mencionada Ley 27.739/2024, cuyo propósito central fue incorporar a los VASPs al régimen ALD/CFT y obligarlos a monitorear y reportar operaciones sospechosas. Del mismo modo, Perú actualizó su normativa en 2023 mediante el Decreto Supremo 006-2023-JUS, incluyendo expresamente a los “Proveedores de Servicios de Activos Virtuales (PSAV)” domiciliados en Perú como sujetos obligados a implementar un sistema de prevención de lavado de activos (SPLAFT) conforme a la Ley de la UIF. La regulación peruana define PSAV alineada a la definición GAFI (abarcando intercambio fiat/cripto, cripto/cripto, transferencias, custodia y servicios financieros relacionados), y exige a estos proveedores aplicar diligencia debida del cliente, monitoreo de operaciones y reporte de sospechas a la UIF. Incluso países de menor desarrollo normativo, como Paraguay, han emitido reglamentaciones administrativas para traer a los actores cripto al radar antilavado: la Resolución 314/2021 de SEPRELAD obliga a toda persona que realice actividades con activos virtuales a registrarse y cumplir la Ley ALD, aunque el país aún no cuente con una ley integral. En Bolivia, donde el marco general estaba rezagado, en 2025 la Unidad de Investigaciones Financieras (UIF) emitió la Resolución Administrativa UIF/19/2025 incorporando formalmente a exchanges, custodios y plataformas cripto como sujetos obligados, con registro obligatorio, KYC/AML, monitoreo y reporte de operaciones sospechosas, y políticas de diligencia basadas en riesgo. Estas respuestas evidencian que el riesgo de lavado es tomado muy en serio a nivel regional, y cualquier propuesta legislativa en Ecuador debe, como mínimo, contemplar la obligatoriedad de registros de VASPs y un régimen robusto de AML/KYC, so pena de quedar desalineada del estándar internacional y facilitar la penetración de capitales ilícitos.

Minería ilegal y delitos medioambientales asociados: Bajo este rubro tenemos, la explotación ilegal de oro y otros recursos minerales cuyos beneficios son blanqueados o movilizadas vía criptomonedas. América Latina sufre una “fiebre del oro” ilegal, especialmente en la Amazonía (zonas de Perú, Colombia, Venezuela y Bolivia), donde el crimen organizado obtiene ingentes ganancias de la extracción ilícita. Reportes periodísticos han indicado que estos fondos ilícitos encuentran cauces de lavado en mercados internacionales, *incluyendo criptomonedas* como mecanismo para transferir valor sin recurrir al sistema bancario tradicional. Aunque la magnitud exacta es difícil de cuantificar, la creciente adopción cripto en países vecinos sugiere que organizaciones criminales vinculadas a minería ilegal podrían estar usando exchanges locales o stablecoins para mover su riqueza, escapando a los controles financieros convencionales. En cuanto a la minería ilegal de recursos naturales financiada con cripto, la clave estará en el trabajo conjunto de autoridades ambientales, aduaneras y financieras para rastrear flujos sospechosos: requiriendo que los VASPs fortalezcan el perfilamiento de clientes (e.g. alertar si un pequeño comercio comienza a recibir grandes montos en cripto sin explicación económica) y facilitando la colaboración internacional para seguir la pista a activos digitales vinculados a redes criminales transnacionales.

Flujos financieros ilícitos y riesgos macroeconómicos: Un rasgo común en la región es la presencia de controles cambiarios, alta informalidad y economías ilícitas que buscan arbitrar entre monedas. Las criptomonedas y stablecoins han brindado una nueva vía para la evasión de controles de capital, la fuga de divisas y la transferencia transfronteriza de ganancias ilícitas (ej. del narcotráfico). Países como Argentina y Venezuela, con estrictos controles de cambio, han visto surgir mercados paralelos de criptoactivos donde individuos y empresas adquieren stablecoins (USDT, USDC) como *dólar digital* para protegerse de la

devaluación o sacar ahorros del país. Sin una regulación adecuada, estos flujos pueden debilitar las políticas monetarias y fiscales. En Ecuador, aunque no hay moneda nacional que proteger (por la dolarización), existe el riesgo de que el ecosistema cripto sea usado para canalizar fondos de origen ilícito hacia el exterior, o para traer recursos de procedencia dudosa, aprovechando vacíos normativos. Además, sin normas, los consumidores quedan expuestos a fraudes, esquemas piramidales y quiebras de plataformas: la región ha sufrido múltiples estafas (desde “*zonas de minería cloud*” ficticias hasta *exchanges* locales que desaparecen con los depósitos), lo cual constituye también un flujo ilícito (depredación financiera de la población). La regulación debe por tanto atender también el frente de protección al inversor/usuario, imponiendo estándares de solvencia, custodia segregada y divulgación transparente a los proveedores cripto. Algunos países han empezado a tomar cartas en este sentido: las reglamentaciones generales No. 994 y No. 1058 que la CNV argentina emitió (tras la Ley 27.739) tiene entre sus ejes la protección del ahorro del público y la solvencia de los proveedores, y el GENIUS Act en Estados Unidos incorpora salvaguardias para usuarios de stablecoins, p. ej., prioridad para los tenedores en caso de bancarrota del emisor y obliga a reservas 100% líquidas precisamente para evitar colapsos que perjudiquen a los tenedores. Estas experiencias resaltan que los riesgos ilícitos no son únicamente penales o macroeconómicos, sino también riesgos para los derechos de los usuarios; todos ellos deben calibrarse en un régimen de regulación por riesgos. En la práctica, esto significa exigir mayores requisitos (capital, reportes, auditorías) a las actividades de mayor impacto potencial (p. ej. custodios de gran escala, emisores de stablecoins de amplio uso) y controles más simples o excepciones para usos de menor riesgo (por ejemplo, *startups* en fase de sandbox o proyectos pequeños limitados en volumen).

IV. Elementos clave de una regulación regional técnicamente viable

A partir del análisis comparado, emergen varios elementos comunes en los marcos regulatorios más exitosos o prometedores de la región. Estos elementos deberían ser considerados al trazar una hoja de ruta regulatoria para Ecuador, adaptándolos a su realidad institucional. En particular, destacan:

1. Definiciones legales claras y clasificación de activos: Muchos fracasos regulatorios comienzan por definiciones imprecisas o demasiado abarcadoras. Una buena ley debe definir qué es un “activo virtual”, “token” o “criptoactivo” para fines legales, distinguiendo sus subtipos principales. La Ley brasileña 14.478/2022, por ejemplo, introduce la categoría legal de “activo virtual” y sienta principios generales para su regulación, evitando sin embargo entrar en tecnicismos cambiantes. Bolivia, en sus recientes decretos, reconoció la necesidad de diferenciar figuras: actualmente carece de definiciones jurídicas completas entre *criptoactivos*, *tokens de valor*, *tokens utilitarios*, etc., lo que genera criterios dispares entre autoridades. Corregir esto es parte de su agenda pendiente. Ecuador debería aprovechar estas lecciones y establecer en su normativa qué tipos de tokens existen y bajo qué marco se ubica cada uno: por ejemplo, delimitar qué constituye “*token de pago*” (similar a moneda electrónica), “*token de valor*” (similar a valor negociable), “*utility token*” (con uso en plataforma) y dejar claro qué leyes aplican en cada caso (monetarias, del mercado de valores, de consumidores, etc.). Esto brinda certeza jurídica y evita vacíos de arbitraje. Asimismo, conviene excluir expresamente lo que no se regula (por ejemplo, si las transacciones estrictamente personales o entre particulares quedan fuera del perímetro, o si la minería individual no estará sujeta a licencias mientras no se conecte al sistema eléctrico público, etc.), para no desalentar actividades legítimas por ambigüedad.

2. Registro y licenciamiento de proveedores de servicios (VASPs): Un registro obligatorio de VASPs es ya un estándar en formación. Argentina instauró en 2024 un registro en la CNV

donde deben inscribirse quienes brinden servicios cripto al público, definiendo criterios de territorialidad (dominio “.ar”, operaciones dirigidas a residentes, porcentaje de ingresos local) para evitar la elusión del registro. Perú también exige que los PSAV nacionales se inscriban ante la UIF y adopten un sistema de prevención de lavado. Paraguay y Bolivia, sin leyes específicas, han utilizado sus órganos antilavado para demandar registro de operadores cripto (ante SEPRELAD y UIF respectivamente). En un paso más allá, Brasil prevé un régimen de licenciamiento supervisado por su Banco Central: los exchanges y otras empresas cripto deberán obtener autorización de funcionamiento, similar a como se exige a instituciones de pago, con periodos de transición para adecuarse a las disposiciones de la ley. En la misma línea, Bolivia aprobó en 2025 el Decreto Supremo 5384, que establece el marco general para la constitución, operación y supervisión de Empresas de Tecnología Financiera (fintech) en Bolivia, incluyendo explícitamente modelos basados en blockchain, tokenización y activos virtuales. Este marco boliviano fija pilares de gobernanza corporativa, ciberseguridad/protección de datos y requisitos de capital y gestión de riesgos para las fintech que operen en el país. Aunque deberá ser reglamentado en detalle por el regulador (ASFI), representa un intento de crear un régimen licencial fintech/VASP acorde a estándares prudenciales. Para Ecuador, resultará esencial definir qué organismo otorgará licencias o habilitaciones a los VASPs (sea una Superintendencia existente u otra agencia especializada) y los requisitos para ello: capital mínimo, idoneidad de directivos, planes de ciberseguridad, segregación de fondos de clientes, etc. Un régimen escalonado podría contemplar licencias diferenciadas (por ejemplo: exchange, custodio, emisor de activos digitales, proveedor OTC) con exigencias según la naturaleza del servicio. También se debe prever la cooperación internacional: muchos VASPs operan a nivel regional, por lo que memorandos de entendimiento entre supervisores o exigencias de reciprocidad serán útiles para que un exchange no evada controles simplemente mudándose a otra jurisdicción.

3. Capa AML robusta e integración con el sistema financiero: Como ya se argumentó, la piedra angular para mitigar los riesgos es la capa ALD/CFT. Los marcos comparados han incorporado diversas medidas: reportes obligatorios de operaciones sospechosas por parte de VASPs (en Chile, la Ley Fintech impone a todos los entes regulados reportar transacciones sospechosas a la Unidad de Análisis Financiero, integrando de lleno a los nuevos actores); umbrales de identificación de clientes (en Perú, los PSAV deben aplicar debida diligencia del cliente en operaciones desde USD 1000 o en cualquier monto si involucra dinero en efectivo, siguiendo lineamientos UIF); y prohibiciones de operar con jurisdicciones de alto riesgo (Argentina, por reglamento CNV 994/2024, denegó el registro a personas o entidades radicadas en jurisdicciones no cooperantes o de alto riesgo GAFI, cerrando la puerta a operadores de paraísos fiscales). Un elemento clave es exigir la “Travel Rule”: que los VASPs ecuatorianos transmitan información del remitente y destinatario en transferencias de activos virtuales sobre cierto umbral, al igual que lo hacen los bancos con las transferencias electrónicas tradicionales. Esto alinea con la Recomendación 16 de GAFI y dificulta el movimiento anónimo de fondos ilícitos. Adicionalmente, sería recomendable integrar el ecosistema cripto con el sistema bancario formal a través de protocolos de debida diligencia reforzada: es decir, los bancos que ofrezcan servicios a exchanges o plataformas cripto deben exigirles cumplimiento regulatorio y reportar posibles incongruencias (varios escándalos globales han involucrado bancos que facilitan rampas fiat-cripto sin controles). Una normativa clara puede facultar a la Superintendencia de Bancos a emitir directrices para la banca respecto a clientes del sector cripto, evitando arbitrariedades (como cierres unilaterales de cuentas a fintech legítimas) pero asegurando una puerta de enlace vigilada entre finanzas tradicionales y cripto.

4. Protección al consumidor e integridad del mercado: Un elemento a veces subestimado es la tutela de los usuarios de criptoactivos y la integridad de los mercados digitales. La Unión

Europea, mediante MiCA, abordó este punto exigiendo que las plataformas centralizadas de intercambio establezcan sistemas para prevenir abuso de mercado (manipulación de precios, insider trading) tal como se exige en mercados de valores. Igualmente, MiCA prohíbe expresamente el uso de información privilegiada en cripto y obliga a la transparencia en las reglas de trading y tarifas de las plataformas. En el plano de protección al inversionista minorista, es importante requerir divulgación adecuada de riesgos: que las plataformas informen sobre la volatilidad, la no garantía estatal, la irreversibilidad de transacciones, etc. Países de la región ya han emitido alertas sobre estos riesgos; por ejemplo, la Superintendencia de Mercado de Valores peruana advirtió públicamente que las empresas que ofrecen o promocionan cripto no están reguladas ni garantizadas, y que las criptos “*suelen estar vinculadas a actividades ilícitas*”, enfatizando el *caveat emptor*. Sin embargo, más allá de alertas, la regulación puede establecer mecanismos concretos: requerir contratos claros, políticas de reclamación por hackeos o fallas, segregación de activos de clientes (para evitar que una insolvencia del exchange consuma los fondos de sus usuarios), seguros de depósito en exchanges (al menos para cubrir ataques cibernéticos, similar a cómo ciertos países exigen seguros a custodios de valores), y lineamientos contables específicos para empresas cripto. Asimismo, se deben contemplar sanciones por prácticas abusivas: la normativa ecuatoriana deberá prever infracciones y multas para quienes operen sin registro/licencia, para exchanges que no cumplan con reportes, o para esquemas fraudulentos. Brasil en su ley tipificó el delito de estelionato con activos virtuales, por ejemplo, para perseguir estafas cripto. Estas herramientas legales disuaden la proliferación de fraudes que lamentablemente han encontrado terreno fértil en la ausencia de regulación.

5. Régimen para stablecoins y monedas digitales: Dado el crecimiento explosivo de las stablecoins (criptoactivos vinculados a monedas fiat, p.ej. USDT), cualquier marco moderno debe contemplar reglas específicas para ellas. Las stablecoins tienen un potencial sistémico mayor (por su uso como sustituto monetario) y presentan retos de reserva y paridad. El GENIUS Act estadounidense (2025) ofrece un referente: establece que los emisores de stablecoins de pago en USD deben mantener reservas 1:1 en activos de altísima liquidez y reportarlas mensualmente, prohíbe que estas reservas se reinviertan o devenguen interés y otorga a los tenedores derecho preferencial en caso de quiebra del emisor. Además, el GENIUS Act clarifica la naturaleza jurídica de las stablecoins (*no* son valores ni commodities, sino un nuevo tipo de instrumento de pagos) y define un esquema de licenciamiento dual: tanto bancos como entidades no bancarias pueden emitir stablecoins, pero bajo supervisión de las autoridades financieras (federales o estatales) según el tipo de entidad. En la Unión Europea, MiCA igualmente exige a los emisores de tokens referenciados a activos cumplir requisitos de solvencia, liquidez, gobierno corporativo y les impone límites si llegan a ser “significativos” para la estabilidad financiera. En América Latina, pocas jurisdicciones han abordado aún el tema de stablecoins; México permitió en su Ley Fintech 2018 que las instituciones de tecnología financiera operen con *activos virtuales autorizados por el Banco de México*, lo cual ha sido interpretado como stablecoins principalmente, pero la regulación secundaria es restrictiva y no ha habilitado del todo su uso. Bolivia, en 2025, curiosamente habilitó operaciones limitadas con stablecoins en su sistema bancario como medida para paliar la falta de dólares físicos: bancos como BISA y BCP introdujeron servicios de compraventa y custodia de USDT para sus clientes, dentro de un marco piloto supervisado. Esta apertura controlada boliviana busca satisfacer la demanda de divisas digitales sin comprometer la moneda nacional, yendo “*por un camino prudente de adopción regulada*” en contraste con el experimento radical de El Salvador de adoptar Bitcoin como moneda de curso legal. Para Ecuador, la reflexión sobre stablecoins es crucial dado su esquema dolarizado: el uso masivo de stablecoins USD podría apoyar la digitalización de la economía dolarizada, pero también conlleva riesgos si circulan tokens no supervisados que la gente pudiera

confundir con depósitos bancarios. Una posibilidad sería autorizar stablecoins específicas (respaldadas 100% por USD) emitidas localmente bajo licencia del Banco Central o entidades autorizadas, para que coexistan con el dólar físico bajo regulación (un enfoque análogo a regular la emisión de dinero electrónico, como ya existió en Ecuador hace unos años con el fallido proyecto de dinero electrónico estatal). Cualquier emisión o uso de stablecoins en pagos debería coordinarse con el Banco Central para no generar una *paralegalidad monetaria*. En paralelo, se debe desincentivar el uso de stablecoins opacas o no auditadas mediante requisitos de registro y divulgación a emisores extranjeros que operen en el país.

6. Gobernanza institucional y cooperación regional: Finalmente, un elemento clave es la creación de instancias de coordinación y asesoramiento técnico permanentes. No se sugiere crear organismos nuevos sin capacidad (como la “Comisión Blockchain” propuesta en Ecuador, que carecía de expertos y chocaba con entes existentes), pero sí podría constituirse un comité interinstitucional de activos digitales con representantes del Ministerio de Finanzas, Banco Central, Superintendencias financiera y de valores, Unidad de Análisis Financiero, e incluso académicos o sector privado, para monitorear continuamente el avance tecnológico y ajustar las políticas. Brasil, por ejemplo, instaló grupos de trabajo dentro del BCB para la temática cripto y su integración con PIX (sistema de pagos). Asimismo, es deseable fomentar la cooperación regional: las similitudes de retos hacen viable compartir mejores prácticas, o incluso pensar en reconocimiento mutuo de licencias en el futuro (quizá remoto, pero la UE sirve de inspiración con su pasaporte MiCA para proveedores cripto autorizados en un país miembro). Organismos como la Asociación de Supervisores Bancarios de las Américas (ASBA) o el propio GAFILAT pueden servir de plataforma para alinear entendimientos y tal vez desarrollar estándares regionales mínimos. Una regulación técnicamente viable debe prever mecanismos para adaptarse sobre la marcha (cláusulas de revisión periódica, potestades reglamentarias flexibles a las agencias) dado que los riesgos y el mercado cripto de 2025 podrían lucir muy diferentes en 2030.

V. Desafíos regulatorios en protección de datos y privacidad

Uno de los ámbitos en que convergen la tecnología blockchain y el derecho es el de la protección de datos personales y la privacidad, planteando desafíos singulares. Cualquier normativa blockchain debe conciliarse con las leyes de protección de datos vigentes (en Ecuador, la Ley Orgánica de Protección de Datos Personales de 2021) para evitar contradicciones y vacíos de tutela. El fallido proyecto ecuatoriano de Ley Blockchain, de hecho, fue objetado en parte porque “*no garantizaba... la protección de datos personales*”, una deficiencia grave dado que blockchain puede implicar tratamiento masivo de información.

Existen dos grandes dimensiones a considerar: (1) **Privacidad del usuario frente al Estado y terceros** en sus transacciones con criptoactivos, y (2) **Cumplimiento de las normas de datos personales por las implementaciones en blockchain** (especialmente las basadas en registros inmutables y públicos). En el primer aspecto, se debe lograr un equilibrio entre la necesaria trazabilidad para combatir delitos y el derecho a la privacidad de las personas en sus intercambios legítimos. La regulación basada en riesgos aporta aquí: por ejemplo, exigir identificación y reporte en transacciones de valor significativo (p.ej. superiores a USD 1000, siguiendo umbrales ALD), pero no imponer vigilancia intrusiva en micro transacciones o actividades personales de bajo monto. Asimismo, las autoridades deben manejar con estricta confidencialidad los datos recolectados bajo la Travel Rule u otros mecanismos; una preocupación válida es evitar que surja un panóptico financiero donde cada pago del ciudadano sea rastreado. La normativa podría incorporar principios de minimización de datos y proporcionalidad: los VASPs recabarán solo los datos necesarios para cumplir con la ley, y los informes a la UIF u otras agencias deben limitarse a lo pertinente para investigación de

ilícitos, con debidas salvaguardas. Por otro lado, el anonimato y seudonimato en las redes descentralizadas plantea dilemas: si bien Bitcoin y similares permiten transacciones seudónimas, la regulación puede desincentivar el uso de mecanismos de ocultamiento extremos (como mezcladores o ciertas monedas de privacidad) sin criminalizar la simple búsqueda de privacidad. El desafío es no equiparar privacidad con ilegalidad: usuarios honestos valoran su privacidad y la ley debe respetarlo, persiguiendo más bien el abuso de dichas herramientas con fines delictivos específicos.

Respecto a la segunda dimensión, la compatibilidad de blockchain con las leyes de datos personales, hay notorias tensiones. Las blockchains públicas son inmutables por diseño: una vez que un dato es registrado, no puede alterarse ni borrarse fácilmente. Esto choca con principios como el derecho al olvido o supresión consagrados en normas como el GDPR europeo y equivalentes latinoamericanos. Si, por ejemplo, una implementación blockchain estatal almacenara datos personales (piénsese en un registro de identidad, de tierras o de historiales académicos en blockchain), ¿cómo se rectificarían o eliminarían datos incorrectos o una vez expirado su propósito? La regulación deberá imponer criterios de privacidad desde el diseño (“privacy by design”) en cualquier solución blockchain pública o privada que maneje datos personales. Una opción técnica es usar datos off-chain con referencias hash on-chain: es decir, no grabar el dato personal en la cadena, sino un código indescifrable que lo represente, de modo que el dato original pueda borrarse o modificarse en la base de datos tradicional sin que la blockchain viole esa eliminación. Asimismo, puede contemplarse el uso de blockchains permisadas (no totalmente públicas) para casos que involucren información personal sensible, de forma que solo entidades autorizadas tengan acceso, y siempre bajo reglas de tratamiento de datos.

Otro aspecto es la portabilidad de la identidad digital. Algunos proponentes de blockchain impulsan conceptos de *identidad auto-soberana*, donde los usuarios controlan sus credenciales a través de la cadena. Esto podría empoderar a los individuos respecto a sus datos, pero también requerirá un marco legal que reconozca dichas identidades y asegure que cumplen los estándares de veracidad y seguridad. Ecuador podría experimentar, en un sandbox regulatorio, proyectos de identidad digital blockchain compatibles con su Ley de Datos Personales, evaluando cómo otorgar validez legal a credenciales on-chain sin sacrificar la privacidad.

Finalmente, cabe resaltar la importancia de la ciberseguridad y protección de datos en las plataformas cripto. Los exchanges centralizados manejan información personal (documentos de identidad, comprobantes de domicilio, etc.) de cientos de miles de usuarios por sus programas KYC. La regulación debe exigirles medidas robustas para resguardar esos datos contra brechas de seguridad. Por analogía, Bolivia en su Decreto 5384 incorporó la ciberseguridad y protección de datos como uno de los tres pilares obligatorios para empresas fintech/blockchain, requiriendo protocolos, auditorías externas y reportes periódicos en la materia. Asimismo, la Ley Fintech de Chile, al establecer el sistema de Open Finance, impuso que el intercambio de datos entre entidades financieras se realice “*según estándares estrictos de protección de datos personales y bajo requisitos de seguridad definidos por la CMF*”, garantizando que la apertura e innovación no vengán a costa de la privacidad del usuario. Ecuador deberá asegurarse de que cualquier normativa que facilite el intercambio de información (sea entre empresas o hacia el Estado) incorpore equivalentes salvaguardas, más aún, considerando la reciente vigencia de su ley de datos personales que crea altas obligaciones de seguridad a los responsables de datos. En síntesis, privacidad y blockchain no son objetivos antagónicos si se legisla con fineza: se puede permitir la trazabilidad necesaria para controlar delitos, a la par de proteger los derechos de los ciudadanos mediante

limitaciones al alcance de la vigilancia y promoviendo soluciones tecnológicas que anonimizan o encriptan datos sensibles en las cadenas de bloques.

VI. Conclusiones: hacia una gobernanza digital legítima, con seguridad jurídica y responsabilidad institucional

La exploración realizada conduce a una conclusión central: la regulación de blockchain y criptoactivos en América Latina debe alejarse del maximalismo legislativo y acercarse a una gobernanza digital por capas, legítima y técnicamente informada. Para el caso de Ecuador – y extensivo a sus vecinos– esto implica forjar un marco normativo legítimo, es decir, respaldado en un amplio consenso social e institucional. La legitimidad proviene de procesos inclusivos (consultando a expertos, industria, academia, ciudadanía) y de la adecuación constitucional: por ejemplo, cualquier norma ecuatoriana ha de respetar la arquitectura del Estado (competencias del Banco Central sobre moneda, derechos fundamentales como la privacidad, y principios de proporcionalidad). El fracaso de la Ley Blockchain archivada mostró las consecuencias de intentar imponer un modelo importado sin ese anclaje local. Por tanto, la hoja de ruta regulatoria deberá ser construida con diálogo intersectorial y paulatina, ganando legitimidad a cada paso.

En términos de seguridad jurídica, la futura regulación debe aportar claridad, certeza y no contradicción con el resto del ordenamiento. Esto supone definir con precisión conceptos (qué está permitido, qué prohibido, quién regula qué), eliminando zonas grises que hoy abundan. La seguridad jurídica se reflejará en que los emprendedores tecnológicos sepan a qué atenerse –qué licencias requieren, qué impuestos pagan, qué responsabilidades tienen– y que los usuarios tengan certeza sobre la legalidad de usar cripto en determinadas condiciones. Un marco claro también atraerá inversión seria en el sector, al reducir la incertidumbre normativa. La comparativa muestra que países como Brasil y Argentina, al promulgar sus leyes recientes, dieron un mensaje de estabilidad normativa que ha sido bien recibido por mercados y proyectos, al proveer reglas de juego, aunque falten detalles por reglamentar. Ecuador deberá aspirar a lo mismo: una ley o conjunto de leyes coherentes, que se inserten lógicamente en el sistema legal (financiero, societario, penal, etc.) y no generen dobles interpretaciones. También implica evitar la “inflación legislativa”: mejor una norma marco bien estructurada, complementada con regulación técnica flexible, que múltiples leyes aisladas y potencialmente inconsistentes.

Finalmente, la responsabilidad institucional es un pilar sin el cual las normas quedarían en el papel. Esto requiere fortalecer las capacidades de las entidades encargadas de supervisar e implementar la regulación. No basta con asignar al Banco Central o a una Superintendencia nuevas facultades sobre cripto; dichas entidades deben contar con unidades especializadas, personal capacitado en tecnología blockchain, herramientas de monitoreo (por ejemplo, softwares de análisis de cadenas para seguimiento de transacciones sospechosas) y protocolos de coordinación. La experiencia ecuatoriana demostró que intentar adelantarse sin la capacidad instalada conlleva retrocesos. En contraste, modelos como el chileno o el brasileño muestran agencias preparándose para la tarea: Chile, antes de implementar la Ley Fintech, planificó 18 meses de elaboración de más de 70 normas técnicas con amplia participación pública, entendiendo que la capacidad regulatoria se construye progresivamente. Bolivia, al virar de la prohibición a la regulación, asignó nuevas facultades a su UIF y encargó a su regulador financiero (ASFI) diseñar procedimientos de autorización para fintech y PSAV, con lo cual reconoce que sin órgano responsable activo la apertura sería caótica. En esa línea, Ecuador necesita definir claramente quién será responsable de la “gobernanza cripto”: posiblemente una mesa entre el Ministerio de Economía y el Banco Central para la estrategia, y en la ejecución la Superintendencia de Bancos para exchanges

que tocan dinero fiat, la de Compañías para asuntos de valores tokenizados, etc., apoyados todos por la UAFE (Unidad de Análisis Financiero) en la vigilancia ALD. Y estas instituciones deberán asumir la responsabilidad de actualizar la normativa conforme evolucione la tecnología – la rigidez es enemiga en un campo tan dinámico.

En conclusión, el futuro de la regulación blockchain en Ecuador y América Latina no debe ser ni de entusiasmo desbordado sin sustento, ni de inmovilismo ante lo desconocido, sino de una gobernanza digital equilibrada. Esta se basará en *legitimidad* (normas discutidas, justificadas y coherentes con los valores jurídicos locales), en *seguridad jurídica* (reglas claras, estables y armonizadas internacionalmente) y en *responsabilidad institucional* (autoridades que asumen su rol con recursos y conocimiento). Solo así podrá brindarse un entorno donde la innovación financiera descentralizada florezca de manera segura, sin reproducir modelos descontextualizados ni poner en riesgo la estabilidad económica o los derechos de los ciudadanos. Ecuador tiene ante sí la oportunidad de aprender de las experiencias reseñadas –tanto aciertos como tropiezos– para construir un marco regulatorio de nueva generación, funcional y basado en riesgos, que sirva de referencia en la región y verdaderamente potencie los beneficios de la tecnología blockchain al servicio del desarrollo, dentro de un Estado de derecho.