

Artículo doctrinal

**LA FUNCIÓN DE COMPLIANCE EN
BLOCKCHAIN, CRIPTOACTIVOS Y
LA NUEVA ECONOMÍA DIGITAL.**

UNA APROXIMACIÓN AL IMPACTO DE LA TECNOLOGÍA
BLOCKCHAIN EN LA PROFESIÓN DE CUMPLIMIENTO
NORMATIVO

ALMUDENA DE LA MATA MUÑOZ

PROFESORA DRA. UNIVERSITARIA,
MANAGING PARTNER BLOCKCHAIN INTELLIGENCE Y
PRESIDENTA DEL BLOCKCHAIN INTELLIGENCE LAW INSTITUTE

ENERO 2023

La función de compliance en blockchain, criptoactivos y la nueva economía digital.

Una aproximación al impacto de la tecnología blockchain en la profesión de cumplimiento normativo.



Dra. Almudena de la Mata Muñoz
CEO de Blockchain Intelligence y Blockchain Intelligence Law Institute.
Académica correspondiente de la Real Academia de Jurisprudencia y Legislación.
Directora de las Certificaciones Experto/a Legal y Compliance en Blockchain, Criptoactivos y Metaversos

Table of Contents

1. Blockchain en compliance hoy.....	2
1.1. El doble impacto de Blockchain sobre la función de compliance.....	2
1.2. La nueva operativa digital sobre Blockchain, objeto de control por las unidades de cumplimiento normativo.....	2
1.3. El apoyo institucional al uso de tecnología Blockchain para el impulse de la economía y la mejora de la sociedad.....	4
2. La evolución del marco normativo específico en blockchain, DLTs y criptoactivos y su impacto en la función de cumplimiento.....	6
3. La relación de las unidades de compliance con los supervisores y los registros específicos relativos a la operativa blockchain / cripto.....	9
4. Riesgos, prácticas y procesos de cumplimiento derivados del uso de blockchain y cripto.....	10
5. Lucha por el talento compliance-blockchain-cripto y las nuevas herramientas digitales para la función de cumplimiento.....	11
6. Las habilidades requeridas en los puestos de compliance digital.....	13

1. Blockchain en compliance hoy

1.1. El doble impacto de Blockchain sobre la función de compliance

La función de compliance se está viendo fuertemente afectada por la tecnología Blockchain. Este impacto se manifiesta en dos vertientes muy diferentes. Por un lado, Blockchain ha creado una nueva operativa económica y social, así como la generación de nuevos activos digitales (criptoactivos, criptomonedas, NFTS...) y nuevos espacios de contratación como los metaversos, que deben cumplir con la normativa aplicable y ser objeto de control por las unidades de compliance.

Por otra parte, Blockchain ofrece herramientas muy valiosas para el ejercicio de la propia función de compliance. Se trata de una tecnología óptima para la gestión fiable de registros y bases de datos, así como para mejorar la trazabilidad y auditabilidad de acciones y procesos que ayudan a la identificación de incumplimientos y definición de responsabilidades. Blockchain también habilita el desarrollo de procesos multiparte, sobre la base de confianza descentralizada y la automatización de procesos vía Smart contracts y tokenización. De esta forma se favorece la implicación de diversas unidades de negocio en los procesos de cumplimiento.

Además, esta tecnología permite la creación de incentivos para favorecer internamente el cumplimiento tanto de normativa como de políticas internas o canales de denuncia (whistle blowing) a través de sistemas de tokenización.

1.2. La nueva operativa digital sobre Blockchain, objeto de control por las unidades de cumplimiento normativo.

Desde la fundación del Blockchain Intelligence Law & Compliance Institute hace más de 5 años, hemos sido testigos de una creciente demanda de personal especializado y de conocimiento de Blockchain en el ámbito del cumplimiento normativo.

Sin duda un sector importante de actividad tiene lugar en el entorno financiero, tanto de entidades tradicionales como tecnológicas y fintechs además de empresas relacionadas con la actividad cripto como exchanges, fondos de inversión o plataformas de NFTs o productos de inversión DEFI (finanzas descentralizadas). A medida que ha aumentado la operativa en este campo, también ha crecido la preocupación por la posible utilización de estos productos y operativas financieras para el desarrollo de actividades delictivas o crimen financiero.

Esta preocupación ha sido objeto de atención de reguladores y supervisors en las distintas jurisdicciones dotando ya de un cierto marco legal a la actividad de prevención por las unidades de compliance. Así, parte importante de esta operativa se enmarca en el establecimiento de procesos de KYC y prevención del blanqueo de capitales y financiación del terrorismo (AML/CFT) así como el cumplimiento de sanciones financieras. En definitiva, se establecen estructuras de control basadas en riesgo (risk-based approach) y en colaboración constante con los supervisores.

Llama la atención la alta proporción de proyectos basados en Blockchain que han sido admitidos en las distintas ediciones del sandbox financiero español, siendo esto indicativo del uso real y creciente de esta tecnología en la industria Española así como del interés de las instituciones públicas por comprender su operativa y favorecer el desarrollo de la innovación de forma controlada y sostenible.



Además, han sido en muchas ocasiones las unidades de cumplimiento, las encargadas de gestionar la relación con los respectivos supervisores (Banco de España, CNMV o Dirección General de Seguros (DGS)).

Pero estas no son las únicas unidades de compliance que se están especializando en Blockchain. También las empresas tradicionales de los más variados sectores están formando a su personal en esta tecnología para la gestión de los riesgos vinculados y la implantación de nuevos sistemas adaptados a sus procesos digitales. Desde el lanzamiento de la Certificación Experto Legal y Compliance en Blockchain y Criptoactivos de Blockchain Intelligence con el Consejo General de la Abogacía, han pasado por nuestras aulas representantes de las unidades de compliance de empresas con actividad en el ámbito asegurador, retail, construcción, inmobiliario, energía, gestión, consultoría, industria automovilística, producción agrícola, galerías de arte, clubs de fútbol, etc. Las necesidades de control de compliance en

estos casos son muy variadas. Algunas empresas operan con criptoactivos o han invertido en NFTs. Otras utilizan sistemas de identidad digital sobre Blockchain en sus procesos de KYC. Algunas han optado por buscar financiación a través de STOs o utilizan redes Blockchain para la mejor gestión de algunos de sus procesos multiparte. Varias de ellas están empleando sistemas blockchain para hacer posible la participación y toma de decisiones a distancia en los órganos

de gobierno de las empresas. También se han desarrollado procesos internos multiparte sobre bases de datos distribuidas por ejemplo para la gestión de tesorería o procesos en los que están involucradas diversas empresas y cuyos datos se gestionan en Blockchains o DLT que facilitan la trazabilidad y control del proceso. Toda esta actividad basada en tecnología Blockchain requiere del control y gestión de cumplimiento. Aún incipiente, pero de importancia clave, es el desarrollo de metaversos basados en Blockchain en los que se desarrolla una importante actividad contractual digital y al que la Unión Europea está dedicando un importante esfuerzo para determinar y mitigar los posibles riesgos vinculados.

Además, en el ámbito de la administración pública se han desarrollado proyectos Blockchain para dotar de mayor transparencia y eficiencia a sus servicios. El uso de Blockchain en el Desarrollo de soluciones de administración pública digital ha hecho necesaria la participación de la intervención y alguna unidad interna de compliance de organismos públicos. Un ejemplo interesante es el Desarrollo de sistemas de contratación digital sobre Blockchain, como es el caso de la implantada en la Comunidad Autónoma de Aragón. Por otra parte existen numerosos ejemplos de colaboración público privada sobre la base de aplicaciones Blockchain como es el caso del proyecto del puerto de Cartagena.

1.3. El apoyo institucional al uso de tecnología Blockchain para el impulso de la economía y la mejora de la sociedad.

Este incremento de actividad sobre tecnología Blockchain tanto en el ámbito privado como el público se ve auspiciado por la actividad de las instituciones europeas. Desde el 2017, la Unión Europea ha implementado una hoja de ruta con el objeto de impulsar el desarrollo y uso de esta tecnología como elemento clave para el mantenimiento de la competitividad europea a nivel internacional. Esta actividad institucional se estructura en tres grandes líneas de trabajo:

- Desarrollo de regulación específica y criterios de interpretación jurídica que desarrollamos en el epígrafe siguiente;
- Desarrollo de infraestructura Blockchain europea sentando las bases tecnológicas y regulatorias para el desarrollo de una plena

sociedad digital segura. En este sentido se ha avanzado en: a) el desarrollo de la red europea Blockchain (EBSI), b) la creación de un medio de pago digital de emisión por el Banco Central Europeo (euro digital / criptoeuro / CBDC) y c) el avance en los modelos de identidad digital y la creación del EU ID Wallet o monedero de identidad digital europea.

- Apoyo al desarrollo de aplicaciones blockchain en el sector privado a través de mecanismos de financiación de proyectos.

Ya en octubre de 2017, el Consejo de Europa solicitó a la Comisión Europea adoptar medidas relativas a blockchain con intención de lograr un mejor posicionamiento geopolítico y económico de la UE a nivel mundial. Con este mandato, en febrero de 2018 la Comisión puso en marcha el Observatorio y Foro Europeo de Blockchain¹ con objeto de identificar a los actores relevantes, las barreras técnicas, jurídicas y de mercado e impulsar el desarrollo de blockchain en el entorno europeo². En abril de 2018, 22 países europeos, incluyendo a España, firmaron una Declaración de Cooperación estableciendo la European Blockchain Partnership cuyo objetivo es crear una infraestructura europea de servicios basados en blockchain (European Blockchain Services Infrastructure –EBSI) para facilitar el intercambio transfronterizo. En la actualidad el número de países firmantes de esa declaración asciende a 30 (todos los países de la UE más Noruega y Liechtenstein). Desde entonces se han dado importantes pasos en la creación de esta infraestructura EBSI, sobre la que se están implementando relevantes casos de uso como los proyectos encaminados a lograr una identidad digital autogestionada común, facilitar la emisión de títulos universitarios en blockchain o el desarrollo de un número de seguridad social común, la gestión del reconocimiento del derecho de asilo a efectos transfronterizos y vinculado también con el sistema de identidad digital o la generación de un sistema de financiación de PYMEs.

Pero las instituciones europeas apoyan también con decisión las iniciativas privadas en Blockchain a través de la inversión realizada a través de programas de financiación y el trabajo dedicado a desarrollar un marco jurídico-regulatorio claro que permita el desarrollo de redes blockchain así como de productos y servicios basados en ellas.

¹ EU Blockchain Observatory and Forum <https://www.eublockchainforum.eu/>

² Montaña Merchán y Angel Martín, The European Blockchain Service Infrastructure y el Desarrollo blockchain en el marco institucional europeo. Casos de uso [<https://blockchainintelligence.es/the-european-blockchain-service-infrastructure-ebsi-y-el-desarrollo-de-blockchain-en-el-marco-institucional-europeo-casos-de-uso/>].

2. La evolución del marco normativo específico en blockchain, DLTs y criptoactivos y su impacto en la función de cumplimiento.

Reguladores y supervisores han trabajado en los últimos años de forma incesante tanto para crear un corpus regulatorio específico como para desarrollar una actividad supervisora adecuada a la nueva realidad. Frente a la indefinición jurídica de los primeros tiempos en relación con el fenómeno blockchain/ cripto, actualmente disponemos ya de mayor claridad regulatoria y obligaciones claras de cumplimiento y registro en unidades habilitadas ad hoc.

La velocidad del abordaje regulatorio en materia Blockchain/ DLT ha sido vertiginosa. Solo en nuestra jurisdicción europea se han desarrollado importantes normas en materia de criptoactivos, blanqueo de capitales y financiación del terrorismo, normativa de valores y tokenización de instrumentos financieros, regulación y desarrollo de la identidad digital y normativa fiscal. En este sentido, cabe destacar que contamos ya con un cuerpo regulatorio específico que ayuda a definir conceptos y taxonomía y a entender la voluntad del legislador en cuanto a la protección de los mercados y la operativa social vinculada con el fenómeno cripto y Blockchain.

Así disponemos ya de normativa explícita entre la que destacamos: a) el Reglamento de Mercados de Criptoactivos (MiCA) (no en vigor), b) el Reglamento UE 2022/858 sobre un régimen piloto de infraestructuras del mercado basadas en tecnología de registro descentralizado (Régimen Piloto) y su impacto en el proyecto de Ley del Mercado de Valores y de los Servicios de Inversión, (aprobada por unanimidad en el Congreso de los Diputados el pasado diciembre), c) Reglamento sobre resiliencia operativa digital (Reglamento DORA), d) la 5ª directiva 2018/843 de prevención de blanqueo de capitales y su trasposición en la Ley 10/2010 de prevención de blanqueo de capitales y financiación del terrorismo (LPBC) a través del Real Decreto Ley 7/2021 o e) la regulación fiscal de criptoactivos acompañada de las respuestas de la Agencia Tributaria a las consultas. Mención especial merece también la publicación del Reglamento eIDAS2 y el paquete de medidas tecnológicas con el que la UE pretende dotar a ciudadanos y entidades de herramientas de identidad digital como la EU ID Wallet.

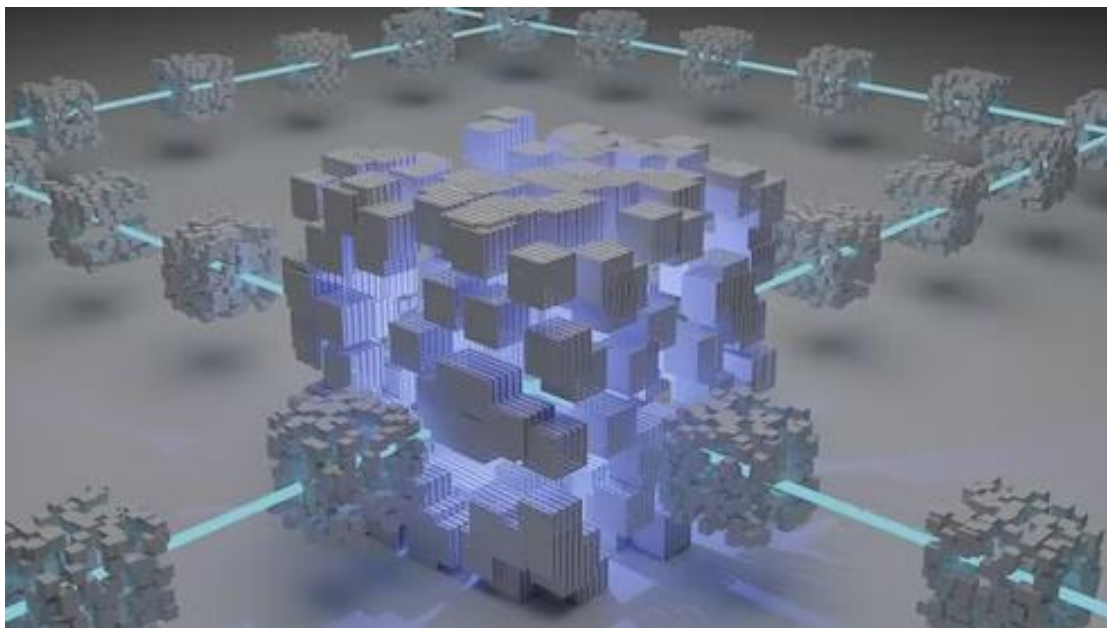
También disponemos de orientaciones, criterios y alertas de reguladores y supervisores como CNMV, la European Securities Markets Agency (ESMA), Banco de España, la European Banking Agency (EBA), EIOPA o la Agencia de protección de datos y continúa la creación de estándares nacionales e internacionales relacionados con las redes y las aplicaciones Blockchain. En este sentido, cabe destacar las guías que desde hace años vienen realizando las autoridades regulatorias

europas sobre la adaptación de la regulación y supervisión de determinados fenómenos, productos o mercados que han surgido como consecuencia del uso de Blockchain. Por ejemplo, la European Securities and Markets Authority – ESMA - publicó [un documento](#) en el que trata la aplicación a los criptoactivos de la normativa relativas a mercado de valores.

Por su parte, la European Banking Authority – EBA - en [su informe](#) de 9 de enero de 2019 () abordó también el tema de los criptoactivos desde la perspectiva de la aplicación de la normativa financiera como la relativa al dinero electrónico, servicios de pago, prevención del blanqueo de capitales y otras normativas aplicables a instituciones de crédito).

Por otra parte, determinados grupos de trabajo están reflexionando sobre la adecuada aplicación de normativa europea a este nuevo fenómeno. Un ejemplo es el esfuerzo que varios grupos realizan sobre la aplicación del Reglamento General de Protección de Datos a la realidad Blockchain. Este es el caso del art. 29 Working Party, Opinion 04/2014 on Anonymisation Techniques, 0829/14/EN, 20 llegó a la conclusión de que los datos transaccionales encriptados con procesos de hashing podrían considerarse datos personales de acuerdo con el Reglamento de Protección de Datos (GDPR).

A nivel internacional también se trabaja colectivamente para desarrollar visiones comunes y una actividad coordinada de control de riesgos derivados del uso de criptoactivos. Así, existe una importante actividad en el seno de estructuras como el G20, FSB, el BIS. Por su impacto especial en la función de cumplimiento, cabe destacar el papel del Grupo de Acción Financiera Internacional GAFI (FATF), organismo intergubernamental que establece estándares internacionales con el objetivo de prevenir el lavado de dinero global y el financiamiento del terrorismo. GAFI ha trabajado desde el 2014 sobre el fenómeno de los activos virtuales (VA) emitiendo distintas recomendaciones y guías. El 28 de octubre de 2021 publicó una Guía actualizada para fomentar la aplicación de un enfoque basado en el riesgo (risk-based) en el tratamiento de los VAs y los proveedores de servicios de activos virtuales (VASP). En ella se hace hincapié en la necesidad de que los países, los VASP y otras entidades que participan en las actividades de activos virtuales (AV) comprendan los riesgos de lavado de dinero y financiamiento del terrorismo derivados de tales actividades y tomen las medidas de mitigación adecuadas para gestionar esos riesgos. La Guía analiza además cómo las actividades de AV y los VASP entran



dentro del alcance de las Normas del GAFI. Se describen los tipos de actividades incluidas en la definición de VASP y proporciona ejemplos de tales actividades que caerían dentro de esa definición, así como aquellas que potencialmente serían excluidas. Además, la Guía destaca los elementos necesarios para calificar como VASP, que son (a) actuar como un negocio para o en nombre de otra persona y (b) proporcionar o facilitar activamente actividades relacionadas con activos virtuales.

Se proporciona, así, a los sectores público y privado orientaciones centradas en seis áreas clave: (1) aclarar las definiciones de VA y VASP para dejar claro que estas definiciones son expansivas y no debería haber un caso en el que un activo financiero relevante no esté cubierto por las Normas del GAFI (ya sea como un VA o como otro activo financiero), (2) proporcionar orientación sobre cómo se aplican las Normas del GAFI a las stablecoins y aclarar que una serie de entidades involucradas en acuerdos de stablecoin podrían calificar como VASPs bajo las Normas del GAFI, (3) proporcionar orientación adicional sobre los riesgos y las herramientas de que disponen los países para hacer frente a los riesgos de BC/FT en las transacciones entre pares, que son transacciones en las que no participa ninguna entidad obligada, (4) proporcionar orientación actualizada sobre la concesión de licencias y el registro de proveedores de servicios de pago automatizado, (5) proporcionar orientación adicional a los sectores público y privado sobre la aplicación de la "travel rule", e (6) incluir principios de intercambio de información y cooperación entre supervisores de proveedores de servicios de pago automatizado. Se trata de un documento clave para la definición de estructuras de control interno pero también para el desarrollo de la actividad supervisora.

En definitiva, tanto a nivel internacional como europeo y nacional se ha ido configurando un corpus regulatorio y una taxonomía que facilita y

justifica la labor de los compliance officers en relación con las infraestructuras DLT, la actividad con criptoactivos, el uso de Smart contracts y tokenización y el establecimiento de los prestadores de servicios de criptoactivos.

3. La relación de las unidades de compliance con los supervisores y los registros específicos relativos a la operativa blockchain / cripto.



La operativa relacionada con los activos cripto (activos digitales o activos virtuales) es relativamente reciente y está en constante evolución. Por ello, la prevención de riesgos vinculados a esta operativa requiere de la colaboración de los

agentes implicados con los organismos supervisores.

En el marco de la normativa aplicable se han establecido ya obligaciones de cumplimiento y registro como la inscripción en el Registro de proveedores de servicios de cambio de moneda virtual por moneda fiduciaria y de custodia de monederos electrónicos del Banco de España, de acuerdo con lo establecido en la Disposición Adicional Segunda de la Ley 10/2010 de prevención de blanqueo de capitales y financiación del terrorismo (LPBC). La inscripción en este registro está condicionada (i) a la existencia de procedimientos y órganos adecuados de prevención de blanqueo de capitales y de financiación del terrorismo, y (ii) al cumplimiento de los requisitos de honorabilidad comercial y profesional.

Hasta ahora, han sido generalmente las unidades de compliance las encargadas de asegurar el cumplimiento de las obligaciones y gestionar el acceso a este registro. El establecimiento de los procedimientos así como la definición de órganos y estructuras de decisión en relación con los objetivos de prevención de blanqueo han sido objeto de responsabilidad de los profesionales de cumplimiento que ha venido desarrollando su tarea en colaboración con el negocio y las unidades tecnológicas internas por un lado y por otro con los órganos de supervisión.

4. Riesgos, prácticas y procesos de cumplimiento derivados del uso de blockchain y cripto.

Como hemos visto, la actividad sobre redes Blockchain es muy variada. Cada aplicación tendrá sus propias exigencias de cumplimiento y generará riesgos específicos que serán objeto de atención de la función de compliance.

En términos de riesgos regulatorios, es necesario hacer una interpretación de la naturaleza jurídica de la aplicación en cuestión para identificar adecuadamente los riesgos vinculados y la normativa aplicable en su caso. En este sentido es conveniente alertar de la posible evolución de dicha naturaleza jurídica de los activos o negocios jurídicos digitales, en cuyo caso, les serán de aplicación normas distintas a lo largo del tiempo. Así lo especifica la EBA en su orientación de 2019. Esto implica que la función de compliance debe permanecer activa durante la vida del negocio jurídico o aplicación tecnológica y ser garante del cumplimiento más allá de la gestión inicial.

A la gestión de los riesgos vinculados con la normativa aplicable se suman los de naturaleza reputacional, siendo necesario desarrollar procedimientos que permitan identificar y mitigar este tipo de riesgos. La naturaleza descentralizada de la operativa Blockchain dificulta en muchas ocasiones la actividad de los compliance officer.

Un primer nivel de riesgos está vinculado con el tipo de red Blockchain o DLT en la que se desarrolla la aplicación. Hay importantes diferencias entre redes públicas, privadas o públicopermisionadas con implicaciones fundamentales en cuestiones como: a) sostenibilidad, b) definición de la jurisdicción aplicable, c) responsabilidades de las partes, d) la identificación de los nodos que componen la red y e) mantenimiento de la operatividad de la red y riesgos vinculados con el posible fin de la red.

Un segundo nivel de riesgos tiene que ver con el negocio jurídico desarrollado en Blockchain y sus elementos constitutivos (identidad, acuerdo de las partes, contratación electrónica y cumplimiento de obligaciones con empleo de tokenización o criptomonedas/criptoactivos).

Especialmente instituciones financieras, las fintechs y las empresas cripto han desarrollado una práctica de control de cumplimiento y mitigación de riesgos específica para la actividad con criptoactivos. Los riesgos más inminentes en este entorno tienen que ver con el uso de criptomonedas o criptoactivos para actividades delictivas, blanqueo de capitales o financiación del terrorismo así como la evasión del cumplimiento de sanciones o interacción con PEPs. También recientemente el uso de criptomonedas o criptoactivos en el ámbito de

los conflictos internacionales como la guerra de Ucrania ha abierto un nuevo ámbito de riesgos geopolíticos y ciberseguridad.

Para evitar el uso delictivo o el incumplimiento de la normativa aplicable, las unidades de compliance han ido introduciendo modificaciones en sus sistemas de control de blanqueo, financiación del terrorismo y sanciones. Han ampliado los requisitos de control en sus operativas KYC y han introducido herramientas digitales de control de las transacciones cripto.

Una de las mayores dificultades para las unidades de cumplimiento en el control de criptoactivos es la definición de la jurisdicción aplicable. Otro reto es la dotación de conocimiento tecnológico suficiente para poder identificar transacciones relacionadas con activos digitales que impliquen riesgo para la institución. Por ello, se suele externalizar la monitorización a empresas externas especializadas.

5. Lucha por el talento compliance-blockchain-cripto y las nuevas herramientas digitales para la función de cumplimiento.



Los riesgos vinculados con la nueva operativa digital requieren de talento específicamente formado en las tecnologías de uso real en el ámbito empresarial. El creciente empleo de activos digitales y las aplicaciones basadas en Blockchain, lejos de ser un espacio de alta especialización o un

boom puntual del mercado, están evolucionando en una operativa creciente, estandarizada y transversal. Como hemos visto, prácticamente todos los sectores de la economía se ven afectados por las nuevas herramientas digitales. El futuro de la economía es eminentemente digital y es precisamente Blockchain la tecnología que hace posible la creación de mercados sin ninguna intermediación analógica en los que las partes no solo se encuentran y negocian sino que logran la perfección del negocio jurídico y su ejecución automática y digital. Las previsiones apuntan por tanto a Blockchain, web 3.0 y metaversos como los nuevos entornos de contratación. Con este crecimiento en la operativa digital, aumentan también los riesgos de fraude, de incumplimiento regulatorio y reputacionales, siendo el papel

de compliance digital absolutamente clave en el desarrollo sostenible de esta nueva economía.

En el caso de que el negocio esté desarrollando una aplicación Blockchain (por ej. emisión de una criptomoneda, desarrollo de un metaverso o plataforma de gestión de comercio internacional, creación y venta de un NFT...), la unidad de cumplimiento deberá estar integrada en el equipo de desarrollo para lograr un resultado “compliant by design”. En otras ocasiones, las organizaciones compran o usan soluciones Blockchain del mercado para una mejor gestión del negocio o bien utilizan o invierte en activos basados en Blockchain (criptoactivos). En este caso también existen riesgos que la función de compliance debe identificar y que servirán al negocio para tomar la decisión sobre el producto o negociar con los proveedores posibles adaptaciones (técnicas o contractuales que mitiguen o eliminen los posibles riesgos).

Además, las unidades de compliance emplean cada vez más herramientas digitales basadas en Blockchain para mejorar su propia operativa del departamento. Se trata entre otros de:

- Mantenimiento de bases de datos en redes blockchain/DLT con el fin de garantizar transparencia y trazabilidad así como poder compartir datos en procesos multiparte. Este es el caso de herramientas de almacenamiento de actas de reuniones o toma de decisiones con el fin de tener claridad sobre la responsabilidad (accountability) de las partes implicadas.
- Uso de herramientas digitales de participación digital en órganos de decisión.
- Creación de incentivos vía token para el fomento de cumplimiento de las políticas internas.
- Herramientas específicas para el cumplimiento de obligaciones regulatorias como el establecimiento de canales de alerta o whistle blowing.

Estamos en un momento de feroz búsqueda de talento compliance digital. Nuestra bolsa de trabajo y función de Head Hunting recibe continuas peticiones de compliance officers y abogados con conocimientos en criptomonedas, privacidad y blanqueo de capitales en el entorno cripto y transformación digital de unidades de cumplimiento. Estos profesionales trabajan directamente con el negocio en el diseño de soluciones y también son clave en la elección de aplicaciones de terceros que contienen elementos Blockchain de contratación automática, mantenimiento de bases de datos enfocados a la supervisión y la auditoría.

6. Las habilidades requeridas en los puestos de compliance digital.



Los profesionales de cumplimiento deben conocer tanto el funcionamiento de la tecnología Blockchain como sus usos y aplicaciones para poder identificar la normativa aplicable, cumplir con las exigencias normativas, elaborar un mapa de riesgos y mitigadores relacionados así como utilizar las herramientas digitales para una mejora de la eficiencia de la unidad.

Tanto en el caso de desarrollo de aplicaciones Blockchain como en el de la elección de soluciones Blockchain del mercado, es necesario en primer lugar una comprensión de los distintos tipos de redes y su funcionamiento (especialmente los mecanismos de consenso y gobernanza de las redes) Ello tendrá importantes implicaciones en cuanto a la responsabilidad de las partes, viabilidad del proyecto y posibles requerimientos contractuales, riesgos operativos y reputacionales de negocio.

También será necesario entender las posibles aplicaciones que corren sobre esas redes (criptomonedas o criptoactivos, tokenización, smart contracts o identidad digital) y la operativa de negocio específica vinculada (custodia, cambio de moneda, finanzas descentralizadas - DEFI, uso de tokenización en metaversos, etc.).

Los compliance officers “de nueva generación” deberán estar familiarizados con la operativa Blockchain y por supuesto conocer no solo la normativa aplicable a esta realidad sino también los criterios de reguladores y supervisores. A veces es necesario adelantar soluciones para evitar que el mercado digital, veloz y audaz, genere riesgos sociales indeseados (risk-based-approach). En este sentido, las unidades de compliance son excelentes aliados para la supervisión y son pieza clave para el desarrollo sostenible y sólido del negocio.

Más allá del marco normativo es fundamental que los compliance officers hayan utilizado las herramientas digitales que son objeto de su control. Por eso, la certificación de Blockchain Intelligence acompaña todos los módulos de aprendizaje de laboratorios prácticos en los que los oficiales de cumplimiento y abogados utilizan las redes y aplicaciones Blockchain que van a controlar. De hecho, utilizan wallets, reciben criptoactivos, emplean wallets de identidad digital y analizan

las cuestiones vinculadas de privacidad, programan un Smart contract, mintean un NFT. También hemos desarrollado el primer espacio en el metaverso, donde los alumnos interactúan y utilizan sus avatares, NFTS y wallets. Recordemos que el futuro de la contratación y las relaciones humanas sucederá principalmente en metaversos y por tanto serán espacios necesitados de identificación y control de riesgos. Por último, los alumnos sellan su certificado en Blockchain y obtienen el token que demuestra su asistencia (POAP). De esta manera, conseguimos una total inmersión y comprensión de la tecnología y podemos identificar cómo desarrollar una estrategia y procedimientos de compliance así como utilizar las herramientas digitales que facilitan la propia actividad.

El futuro de la contratación digital estará definitivamente vinculad a la tecnología Blockchain y por ello consideramos que se trata un elemento clave para el desarrollo de la profesión.

CURSOS CERTIFICADOS BLOCKCHAIN



CURSO
EXPERTO LEGAL Y COMPLIANCE
EN BLOCKCHAIN

[VER CURSO](#)



CURSO
CRIPTOACTIVOS Y CUSTODIA:
REGULACIÓN Y NEGOCIO

[VER CURSO](#)



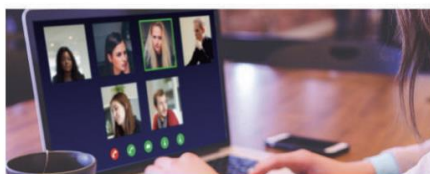
CURSO
EXPERTO COMPLIANCE
EN BLOCKCHAIN

[VER CURSO](#)



CURSO
EXPERTO LEGAL
EN BLOCKCHAIN

[VER CURSO](#)



CURSO
BLOCKCHAIN
Y POSIBILIDADES DE USO

[VER CURSO](#)



CURSOS Y
WORKSHOPS
INHOUSE

[MÁS INFO.](#)

www.blockchainintelligence.es

info@blockchainintelligence.es