Influencia en el blanqueo de capitales de la convergencia entre tecnologías

FACULTAD DE CIENCIAS HUMANAS Y SOCIALES

Autora: María Porras Santisteban

Director: José María Blanco Navarro

Madrid

2021/2022

Resumen

En el presente proyecto se lleva a cabo un estudio acerca del impacto que tiene la convergencia entre las tecnologías de blockchain e inteligencia artificial en el ámbito financiero enfocado al delito de blanqueo de capitales. Desde un punto de vista histórico como jurídico, ahondamos en la acción tipificada observando su evolución basada en la influencia de estas dos tecnologías punteras. Asimismo, recogemos las ventajas y contingencias que presenta la convergencia y evaluamos, en función, al estudio bibliográfico, las conclusiones.

Abstract

In this project, a study is carried out on the impact of the convergence between blockchain technologies and artificial intelligence in the financial field focused on the crime of money laundering. From a historical and legal point of view, we delve into the typified action observing its evolution based on the influence of these two cutting-edge technologies. Likewise, we collect the advantages and contingencies that the convergence presents, and also, we evaluate, based on the bibliographic study, the conclusions.

ÍNDICE

I.INTRODUCCION ----------3
PROPOSITO----------3
OBJETIVO GENERAL ----------4
METODOLOGÍA----------5
II.REVISION BIBLIOGRAFICA ----------7
ANALISIS DEL DELITO DE BLANQUEO DE CAPITALES----------7
ANALISIS DE LA TECNOLOGIA DE LA INTELIGENCIA ARTIFICIAL ---- 23
CONVERGENCIA Y SU PROYECCION ---------- 24
III.ANALISIS CRITICO ---------- 26
VENTAJAS---------- 26
RIESGOS ---------- 27
IV.APLICACIÓN A LA CIBERSEGURIDAD DE LA CONVERGENCIA------- 29
TÉNCNICAS APLICADAS Y MODUS OPERANDI ---------- 29
V. POLÍTICA CRIMINAL E INVESTIGACION INCONVENIENTES ---------- 33
1. RETOS NORMATIVOS Y POLICIALES ---------- 33
2. IDONEIDAD DEL BLOCKCHAIN CON CRIPTOMONEDAS PARA EL BLANQUEO ---------- 34
3. BLOQUEO, INCAUTACION Y DECOMISO DE CRIPTODIVISAS --------- 36
VI.CONCLUSIONES ---------- 37
VII.BIBLIOGRAFIA---------- 39

I. INTRODUCCION

1. PROPOSITO

De todas las acciones tipificadas en el Código Penal español, la autoría de "guante blanco" es de las menos etiquetadas socialmente con una connotación peyorativa. El blanqueo de capitales surge en Estados Unidos en los años 20, conocido entonces como "money laundering", debido a que el mafioso Al Capone, con el fin de esconder la procedencia de su dinero ilícito, creó una red de lavanderías para integrar el dinero sucio en el flujo legal monetario.

A raíz de ese momento, las formas y tamaños del blanqueo de capitales en todo el mundo han sido, ante todo, de lo más creativo. Desde empresarios de alto prestigio, políticos, personas de a pie, hasta terroristas y narcotraficantes. Todos ellos se han ido adaptando a las investigaciones de las Fuerzas y Cuerpos de Seguridad del Estado, a los nuevos métodos de investigación y, evidentemente, a las nuevas tecnologías.

Las nuevas tecnologías suponen un gran avance tanto social como económico, las personas ya no tienen que presenciarse en un banco, ya no tiene por qué salir su nombre en los telediarios por la gran capacidad de dichas tecnologías de mantener el anonimato.

Este trabajo de investigación quiere profundizar, no en el pasado, si no en el futuro. La proyección de este delito en el marco del progreso. La tecnología blockchain, actualmente muy utilizada.

No podemos imaginarnos con exactitud cómo será, como tendremos que adaptarnos desde la corriente de control formal e informal, ni cómo los delincuentes se ingeniarán una vía para seguir blanqueando.

La innovación empresarial, la protección de datos, las redes sociales, nuestra jerga no deja de estar cada día más llena de un lenguaje tecnológico al que no debemos dar la espalda. A medida que el progreso avanza, nosotros debemos avanzar con él.

Este tema siempre ha sido de gran interés para mi. Desde aquellas lavanderías, pasando por paraísos fiscales -el chocolate suizo- y los territorios offshore, hasta quien sabe. ¿LA RED? Una cadena de bloques todavía desconocida para una sociedad tecnológicamente novata, pero que seguro que será muy famosa para todos en poco tiempo. Una inteligencia artificial que no dependa de nadie, que ahora para robarla no hay que entrar a un banco con pistola, solo sentarse en una silla y hackear.

Internet ha desarrollado una mentalidad comercial innovadora, los procesos comerciales utilizando plataformas digitales permite una mayor agilidad en la vida cotidiana, ahorrándonos tiempo en ir presencialmente a cualquier sitio. Ahora únicamente se moviliza nuestro dinero. El internet de las cosas (IoT), la tecnología Blockchain (BL) y la Inteligencia Artificial (IA), además de otras, son herramientas del progreso para facilitar la oferta y la demanda, incluso el ahorro o la inversión. La tecnología Blockchain aumenta la confianza y la seguridad de los usuarios o clientes y es capaz de almacenar cualquier documentación digital. El internet de las cosas impulsa la automatización de las industrias y facilita adaptando el uso de los procesos comerciales. Y por último, la inteligencia artificial mejora los procedimientos detectando parones y optimiza los resultados.

El presente trabajo se estructura en 3 bloques:

En primer lugar, el acercamiento a la acción tipificada desde términos legales. En segunda posición, la irrupción de la tecnología blockchain y las criptomonedas en el mercado económico tradicional, analizando operaciones. Y los nuevos avances tecnológicos con la inteligencia artificial. Finalmente, la sinergia de tecnologías y sus consecuencias respecto a la prevención del delito de blanqueo de capitales.

2. OBJETIVO GENERAL

Analizar los impactos actuales y futuros de la convergencia entre inteligencia artificial y blockchain en el blanqueo de capitales en España.

2.1 Objetivos específicos:

- Identificar las debilidades de dichas tecnologías que se puedan aprovechar para delinquir.
- Detallar las ventajas de la convergencia de tecnologías respecto a la acción tipificada.
- Fomentar la inclusión de estas tecnologías como forma de combate para el blanqueo de capitales.
- Operacionalizar los métodos de investigación y criticar la incoherente regulación.
- Facilitar la comprensión de estos conceptos tecnológicos a la ciudadanía.

3. METODOLOGÍA

La metodología empleada en este proyecto es de naturaleza cualitativa, basada en el método inductivo. En primer lugar, se realiza un análisis bibliográfico sobre el delito de blanqueo de capitales, desde sus orígenes documentados hasta la proyección futura con la influencia de las tecnologías. Al igual que ocurre con la acción tipificada, el estudio del funcionamiento del blockchain y de la inteligencia artificial, ha sido recabado desde distintos recursos bibliográficos.

La información documental ha sido extraída de diferentes fuentes primarias digitales como: Blog de Registradores de España, Centro Criptológico Nacional, Europol, GAFI, Google Schoolar, SEPBLAC y otras más fuentes con artículos académicos. Esta búsqueda nos permite estudiar y analizar los conceptos protagonistas del proyecto y dar cabida a conclusiones propias.

Para acotar la búsqueda, mayoritariamente, se utilizaron los términos "blanqueo de capitales", "cryptocurrencies", "blockchain", "inteligencia artificial" y "prevención del blanqueo de capitales".

Asimismo, hemos tenido en cuenta el marco legislativo para poder enmarcar nuestro trabajo, la actual legislación española que sentencia este delito es el Código Penal español y la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo. Además, el marco europeo e internacional también están reflejados en nuestro texto desde dictámenes emitidos por las instituciones mas destacadas.

En segundo lugar, tenemos en cuenta fuentes secundarias como noticias de prensa y artículos digitales para aportar esa visión cronológica de hechos significativos, tanto en materia de regulación como en avances científicos. Incluso, sumergirnos en blogs tecnológicos para ahondar información sobre aquello que más desconocemos, el futuro.

Por otro lado, y acompañando la revisión bibliográfica y el estudio documental, contamos con observación participante dentro de la institución de la Guardia Civil, donde se tuvo la oportunidad de acudir a conferencias nacionales e internacionales sobre los temas relevantes que se exponen en nuestro texto. Se realizaron estudios internos sobre la trazabilidad de las criptomonedas, sobre nuevos modus operandi, la Deep web, técnicas

OSINT y otros estudios que por confidencialidad no se podrán anexar en el presente trabajo.

Tras el estudio documental realizado para situar nuestro proyecto, continuamos con un análisis crítico y fundamentado a partir de la etapa anterior del trabajo. Y después de ambas partes cubiertas, expondremos de forma explicita nuestras conclusiones.

II. REVISION BIBLIOGRAFICA

La clasificación del contenido académico, objeto de estudio, va a ser desde cuatro subapartados:

a) Análisis del delito de Blanqueo de Capitales, desde su naturaleza, su legislación nacional y de componente internacional y, modus operandi.

b) Análisis de la tecnología blockchain y su aplicación en las criptomonedas. Relación de este delito con la tecnología: cómo se han empleado históricamente los avances tecnológicos para cometer el acto criminal, naturaleza, elementos relevantes y regulación.

c) Análisis de la tecnología -inteligencia artificial-.

d) Convergencia y proyección de la influencia recíproca entre tecnologías.

1. ANALISIS DEL DELITO DE BLANQUEO DE CAPITALES

A nivel internacional no existe una definición exacta del delito de blanqueo de capitales, aunque en la Unión Europea se establece, bajo la Directiva 2018/1673 del Parlamento y Consejo Europeo contra el blanqueo de capitales en materia de derecho penal, el 23 de octubre de 2018. En ella se establece, en su artículo tercero, una definición consensuada entre los Estados Miembro:

> "a) la conversión o la transmisión de bienes, a sabiendas de que dichos bienes provienen de una actividad delictiva, con el propósito de ocultar o encubrir el origen ilícito de los bienes o de ayudar a personas que estén implicadas en dicha actividad a eludir las consecuencias legales de su acto;
>
> b) la ocultación o el encubrimiento de la verdadera naturaleza, origen, ubicación, disposición, movimiento o derechos sobre los bienes o la propiedad de los mismos, a sabiendas de que dichos bienes provienen de una actividad delictiva;
>
> c) la adquisición, posesión o utilización de bienes, a sabiendas, en el momento de la recepción, de que dichos bienes provienen de una actividad delictiva.".

> Los Estados Miembros, según la Directiva, deben seguir las Recomendaciones del GAFI para la prevención del blanqueo de capitales y la financiación del terrorismo.

Podemos observar que, entre todas las definiciones sobre este hecho delictivo, coinciden tres elementos. El primer elemento se centra en el proceso, esto quiere decir que es una acción continuada en el tiempo. Es cierto que puede existir un hecho puntual de blanqueo de capitales, pero normalmente se tiene en cuenta su preparación, premeditación y su recorrido prolongado en el tiempo. El segundo elemento coincidente es el encubrimiento. La ocultación de la procedencia delictiva de los bienes es fundamental en el tipo. Por último, otorgar apariencia de legitimidad al dinero sucio. Este elemento brinda comodidad al operar con el dinero.

Debemos tener en cuenta que este hecho delictivo supone un impacto negativo en el orden socio económico global, afectando a la integridad y reputación de las instituciones financieras y mercados, perdiendo ingresos fiscales y, por consiguiente, suele derivar en corrupción.

El blanqueo de capitales se refiere como una acción tipificada en el código penal contra el orden socio económico y el patrimonio entre los artículos 298 a 304 del Capítulo XIV -De la receptación y el blanqueo de capitales-, Título XIII. Se considera un fenómeno delictivo transfronterizo, y cada día más en un mundo tecnológico y globalizado. Se remonta a muchos años atrás. Tiene como objetivo incorporar bienes de ilícita procedencia o de procedencia licita, pero no declarado en el tráfico económico legal. Su regulación se encuentra en los artículos 298 a 304 de Código Penal. La apariencia licita de los bienes de procedencia ilícita al mercado económico legal permite su uso y disfrute y pretende eliminar el rastro de ese origen ilegal.

Este tipo delictivo viene importado de las herramientas que utiliza el crimen organizado; aunque en la actualidad, se emplea en muchas otras ocasiones. Los bienes jurídicos que se pretenden proteger de este delito son: el funcionamiento legal del sistema financiero y económico del país y, el interés del Estado español en perseguir y castigarlo.

El tipo básico de blanqueo de capitales no consiste únicamente en el lavado de la procedencia del dinero o de su disfrute, sino que pretende abarcar todo el proceso desde la adquisición, la posesión, la utilización, la conversión o la transmisión de esos bienes

con la finalidad de encubrir su origen. Tampoco se excluirían aquellas personas que hayan facilitado la elusión de las consecuencias legales detonadas del delito.

Existen agravantes del tipo básico del blanqueo de capitales cuando la procedencia de esos bienes resulta de:

- Delitos contra la ordenación del territorio y el urbanismo.
- Cohecho.
- Tráfico de influencias.
- Malversación.
- Fraudes y exacciones ilegales.
- Negociaciones y actividades prohibidas a los funcionarios.
- Tráfico de drogas.
- Terrorismo.

1.1 CONCEPTO DOCTRINAL

Para comprender, realmente, el delito al que etsá sujeto este trabajo, debemos saber apreciar la distinción entre dos conceptos: “dinero negro” y “dinero sucio”.

El primer concepto, “dinero negro” se refiere a aquel que tiene origen lícito, pero no está declarado o no lo está adecuadamente en el país al que le debe su amparo fiscal. Dinero sucio: de origen ilícito. En contraposición, tenemos “dinero sucio”, es aquel al que aludimos cuando hablamos de dinero cuyo origen es ilícito.

El blanqueo solo es acción tipificada cuando los bienes proceden de actividades delictivas; en el caso de que se introduzca o se intente introducir dinero negro en el mercado legal no conllevará un proceso penal, si no un proceso administrativo.

La STS 156/2011, de 21 de marzo está anexada a las Cuarenta Recomendaciones del GAFI, asumiendo la doctrina y jurisprudencia de la misma, en relación a las fases del blanqueo de capitales. El GAFI, en sus recomendaciones para la prevención del blanqueo de capitales y financiación del terrorismo, establece la Recomendación 15 para Nuevas Tecnologías. Dentro de esta recomendación a los países se establecen pautas de

identificación, análisis y actuación contra este delito. Los países deberían considerar a los activos virtuales como "bienes, fondos o productos de valor equivalente", para poder así, aplicar las medidas pertinentes tanto a esos activos como a los proveedores de los mismos. A estos últimos los vamos a denominar Proveedores de Servicios de Activos Virtuales (PSAV). Los países deben exigir la identificación, evaluación y aplicación de medidas eficaces con el fin de reducir el riesgo desde los PSAV, al igual que requerir licencias o registros, por lo menos en los países donde se creen; independientemente de que sea persona jurídica o física. El fin es evitar que los criminales posean o sean beneficiarios finales de estas entidades virtuales. En el caso de que no se tenga licencia se tendrán que imponer sanciones efectivas y disuasorias. Además, se hará una supervisión y monitoreo por las autoridades competentes, incluyendo la cooperación internacional. Asimismo, en la recomendación diez se marca un umbral de 1000 euros en transacciones ocasionales, por las que el PSAV debe dar aviso si se superan, y, por otro lado, como cualquier otra institución financiera, se deben recopilar y registrar los usuarios para que por previa petición las autoridades hagan seguimiento y congelación.

El blanqueo de capitales puede llegar a ser, desde un proceso sencillo y rápido, hasta uno complejo y duradero en el tiempo. La doctrina general acepta y clasifica tres etapas principales en el proceso.

La primera de ellas es la fase de adquisición/colocación. En esta etapa se produce la aprehensión física del dinero de procedencia ilícita con el fin de ocultarlo. En esta etapa confluyen grandes cantidades de dinero lo que resulta complicado esconderlo. Esta etapa está considerada por la ONU en el E/CN.15/1992/4Add.5, Money Laundering and associates issues: the meed for international cooperation, del ECOSOC, 23 de marzo de 1992, pp. 7-8, núm 23, como la de más alto riesgo para los criminales, debido a que mientras se busca como depositar el dinero o activos en el curso legal o transporte transfronterizo. El reclutamiento de mulas o intermediarios es de vital importancia; por supuesto a cambio de una prima por el servicio o en otros casos, a través de extorsión o coacción.

La siguiente etapa es la metamorfosis o etapa de transformación. Se traduce en la ocultación a través de operaciones financieras y mercantiles del dinero en efectivo – como ha sido siempre -, pero ahora también se refleja en grandes billeteras de criptomonedas. Ingeniería financiera.

Finalmente, la última fase es la de integración, en esta los activos pasan a entrar en el tráfico legal financiero. Por lo que quedaría a total disposición de uso a pesar de su procedencia.

1.2 MODUS OPERANDI Y SU PROYECCION

Encontramos en el periódico El Diario, 2016, se publica un estudio de los principales métodos utilizados para el blanqueo de capitales según Juan Carlos Galindo de la Asociación de Sujetos Obligados en Prevención del Blanqueo Capital y lucha Contra la Corrupción (ASEBLAC). Consta de nueve modus operandi y vamos a desarrollar cada uno de ellos.

a. Efectivo

Se considera efectivo, según la Agencia Tributaria, lo establecido en el artículo 34.2 de la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y financiación del terrorismo. Incluyendo así los siguientes medios de pago: en primer lugar, "el papel moneda y la moneda metálica, nacionales o extranjeros"; en segundo lugar, "los cheques bancarios al portador denominados en cualquier moneda" y, en tercer lugar, "cualquier otro medio físico, incluidos los electrónicos, concebido para ser utilizado como medio de pago al portador".

De los más métodos empleados para el blanqueo de capitales encontramos. En primer lugar, **e**mpresa**s** con uso intensivo de efectivo: haciendo referencia a negocios que manejan mucho dinero físico como pueden ser tiendas, bares, restaurantes, autolavados, estancos y otros muchos. En estos negocios es muy complicado poder diferencias desde autoría o investigación la diferenciación de los fondos y su origen.

En segundo lugar, a través del contrabando de efectivo. En España existe una limitación de pagos en efectivo con el fin de prevenir posibles blanqueos en determinadas operaciones, dispuesto en el artículo 7 de la Ley 7/2012, de 29 de octubre.

- Las limitaciones impuestas por la Agencia Tributaria son: la primera, cuando alguna de las partes involucradas actúe en calidad de empresario o profesional, se limitarán los pagos a 2.500 euros en efectivo o su contravalor en monedas extranjera. En

segundo lugar, la cantidad asciende a 15.000 euros o su contravalor en moneda extranjera cuando el pagador sea una persona física y pueda justificar no tener domicilio fiscal y no actúe como empresario o profesional en España.

- Otras formas de contrabando de efectivo pueden ser a través del canjeo de premios de lotería, de casinos y casas de cambio o incluso, compra de arte.

b. Por métodos financieros:

- Fondos de inversiones.

  Este método es más útil en la tercera fase, la fase de integración. Estos fondos manejan grandes cantidades dinero, suele moverse a través de terceros COMO empresas fantasmas o bancos en paraísos fiscales.

- Hawala o transferencias informales/sistemas bancarios paralelos o subterráneos y empresas de servicios monetarios.

  El hawala es inherentemente étnico. No está sujeto a regulación de ningún tipo. Las transacciones son mayoritariamente en efectivo lo que inhibe la trazabilidad del dinero y sus poseedores.

  Y las empresas de servicios monetarios permiten enviar pequeñas cantidades de dinero al extranjero, con un anonimato muy arraigado hasta hace poco que han regulado las transacciones por medio de identificación de remitentes y destinatarios.

- Crowfunding y ONGs. El método del crowfunding hace referencia a un sistema abierto con el fin de recaudar activos para un proyecto. Se realiza a través de plataformas web poniendo en contacto a ambas partes, recaudadores y personas que desean contribuir. Este método es interesante por os movimientos de genera y la operacionalización que permite en grandes y pequeñas transacciones.

c. Por métodos no financieros basados en productos:

- Fideicomisos y sociedades en paraísos fiscales y uso de testaferros.

Las organizaciones criminales crean estructuras complejas, normalmente, transnacionales y con ventajas fiscales o vacíos legales de índole fiscal. Los testaferros dentro de estas estructuras jerárquicas realizan un papel muy importante, escondiendo la verdadera identidad del titular real de la empresa y máximo beneficiario. Es un sistema opaco y, comúnmente, cuenta con profesionales de los ámbitos vitales para lograr el proceso desde el origen hasta la integración del dinero en el mercado legal.

- Sobrefacturación y subfacturación.

Desde el GAFI, el blanqueo de capitales por medio del comercio se basa en «[...] el proceso de disimular el producto de los delitos [...] a través del falseamiento del precio, la cantidad o la calidad de las importaciones o exportaciones».

- A través de adquisición de activos inmobiliarios.

Este método permite a las organizaciones criminales comprar activos inmobiliarios por debajo de su precio e introducir una gran parte de dinero ilícito como dinero negro, sin declarar en las compras.

d. ICO (Initial Coin Offering)

Es el equivalente a la Oferta Pública Inicial (IPO). Se refiere a cuando una sociedad busca recaudar dinero para crear una nueva moneda, aplicación o servicio; en este caso, se lanza una ICO como una forma de recaudar fondos. Inversores lanzan sus ofertas y con ello reciben un token de criptomoneda nueva emitido por la entidad. Este token puede utilizarse a modo interno; es decir, canjeable dentro de la misma sociedad por productos y servicios que ofertan o representar una participación en la misma.

e. Mulas económicas

Por encargo del delincuente, transportan, ocultan, envían o transfieren dinero de procedencia ilícita. Se dan casos de mulas "profesionales", pero en muchas ocasiones las mulas son captadas mediante engaño, promesa de ingresos fáciles, etc. Es frecuente

incluso la captación a través de ofertas de empleo, entre personas con necesidades económicas, problemas de drogadicción, etc, que a veces no llegan a ser del todo conscientes del origen ilícito del dinero. Finalmente, y aunque no es tan habitual, los delincuentes llegan a emplear mediante engaño o diferentes técnicas que buscan no declarar la procedencia de los fondos a personas o empresas especializadas en la intermediación y envío de dinero.

2. ANALISIS DEL BLOCKCHAIN Y SU APLICACIÓN DESDE LAS CRIPTOMONEDAS PARA EL BLANQUEO DE CAPITALES

2.1 Naturaleza del blockchain

Con relación a establecer una única definición, podemos concretar que la mayoría de las ideas coinciden en que la tecnología Blockchain "es una forma de tecnología de contabilidad distribuida (DLT, por sus siglas en inglés), que registra bloques de información en la red de la cadena, respaldada por los nodos que la conforman", (Berryhill, Bourgery, y Hanson, 2018).

El origen de la tecnología blockchain precede al auge y a los inicios del Bitcoin. La idea de esta tecnología surge en 1991 de la mano del Doctor Stuart Haber y el Doctor Scott Stornetta, cuyos estudios describieron una cadena de bloques que estuviese criptográficamente protegida para que fuese inmutable, con el fin de congregar más documentos digitales y mejorar la eficiencia de la computación. Ambos investigadores mejoraron la propia tecnología a través de la introducción de los árboles de Merkle, que permitían agrupar en un solo bloque más documentos.

Por otro lado, los ahora conocidos "Smart contracts" o contratos inteligentes surgieron a manos de un informático, jurista y criptógrafo, Nick Szabo en 1996. Según él "Smart contract" es un conjunto de promesas, especificadas en forma digital, incluidos los protocolos dentro de los cuales las partes cumplen estas promesas". A pesar de lo que conocemos hoy de la tecnología que utilizan este tipo de contratos, la idea origina no se complementaba con el Blockchain. El fin de estos era imposibilitar o dificultar el incumplimiento de los contratos.

La relevancia de esta tecnológica fue impulsada, en 2008, por la aparición de la criptomoneda Bitcoin. Surgió desde el pseudónimo de Satoshi Nakamoto. El blockchain supuso una innovación al pretender descentralizar transacciones y hacerlas de un modo directo. Fue la innovación de un nuevo sistema de seguridad, transparencia y privacidad, prácticamente impenetrable, del concepto de una versión digital de dinero en efectivo, basado en la tecnología de Haber y Stornetta. Con el objetivo de garantizar la inmutabilidad del registro de manera descentralizada e indirecta, añadiendo el término de minería para crear incentivos financieros para la participación en la verificación de las transacciones de los bloques. Este procedimiento de minería, en Bitcoin, se refiere a "proof of work, PoW" o prueba de trabajo.". La base del Blockchain es pública, lo que permite guardar registro de cada transacción y distribuirla entre todos los miembros. Se considera una tecnología transaccional. Por lo tanto, se establece que el computo de las técnicas de minería, hash y criptografía, surgieron las criptomonedas.

La criptografía, haciendo mención al matemático inglés Alan Turing, como creador de la esta materia a partir de la máquina "Enigma", descifrando lenguaje encriptado en la

Segunda Guerra Mundial. Por ello, la criptografía es la encargada de producir y, como la raíz de la palabra indica, cifrar o descifrar las claves oportunas para que el usuario pueda acceder de forma privada a las criptomonedas y, de forma pública, ofrecer esa clave utilizada y necesita en la transacción. Desde la criptografía obtenemos también, la firma digital, confirmando así al propietario del mensaje que se envía.

Por otro lado, la función hash permite verificar el mensaje.

Y finalmente, la potencia de cálculo y minería. Funciona de forma que el usuario remitente realiza una transferencia, esta llega al minero quien, en función de la cantidad que el remitente derive a pagar las tasas de ese movimiento, se posicionará con preferencia a que la transacción se realice con anterioridad a otras.

Podemos decir que han sido tres vertientes las que han concluido en su implantación y creación social. La primera es la idea y puesta en marcha de las criptomonedas, con Bitcoin, desde un registro público. La segunda son las redes distribuidas. Y, por último, el consenso social y la teoría de juegos.

I. Satoshi Nakamoto y Bitcoin

El 15 de septiembre de 2008, Lehman Brothers, la entidad financiera estadounidense se declara en quiebra. Este acontecimiento tuvo una repercusión expansiva hasta tal punto de iniciar una gran crisis económica mundial. Este efecto dominó algunos teóricos del campo lo asociaron con la Teoría del Efecto Mariposa, la cual afirma que, si una pequeña mariposa bate sus alas en un lugar remoto del mundo, este aleteo provocará un gran tornado al otro lado del mundo. No podemos conjeturar que el único elemento del desastre fue Lehman Brothers, es más, muchas entidades financieras fueron las que desestabilizaron el curso económico mundial.

Contextualizando la gran crisis económica, pocos meses después surge una idea revolucionaria e innovadora, el Bitcoin. Bajo el seudónimo de Satoshi Nakamoto, se publica un documento que pretende introducir una forma descentralizada de mediar y gestionar transacciones monetarias. La idea central rondaba en esa forma directa de realizar pagos entre usuarios, lo denominado Peer-to-Peer. De esta forme surgió una nueva moneda.

La intrusión de Bitcoin al mercado tuvo que guiarse por una serie de restricciones del consenso de estados y entidades financieras reacias a su aparición. Para lograr el objetivo, Bitcoin tuvo que asemejarse en características al efectivo, un bajo coste de uso, fiabilidad de que las transacciones se realicen e intentar lidiar con el *problema del doble gasto;* el cual consiste en que un solo token digital puede ser gastado dos veces. Esta duplicidad no se da en el dinero físico -monedas y billetes-, estos archivos electrónicos pueden duplicarse y no dejar evidencias en el cambio de titularidad de los mismos. La solución a esta problemática se tiene la posibilidad de paliarse a través de la tecnología Blockchain que incluye algoritmos criptográficos de todas las transacciones.

Esto conllevó a que dicha tecnología incentivase el interés de las personas dentro y fuera del sector financiero, en ella.

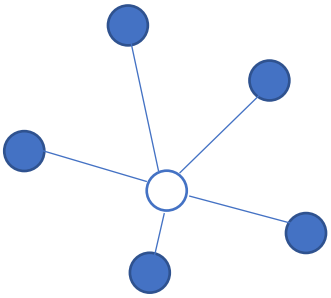
II. Redes distribuidas

Diferencia entre descentralizado, distribuido y centralizado. Explicamos la diferencia a continuación.

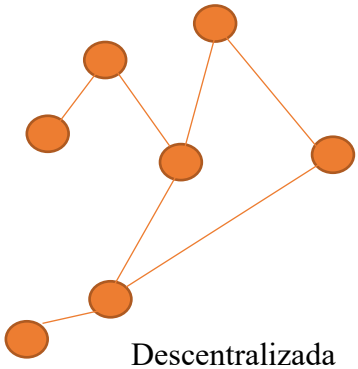
Centralizada: nodos periféricos conectados a una unidad central.

Descentralizada: conjunto de sistemas/ordenadores que trabajan para mejorar y controlar la red.

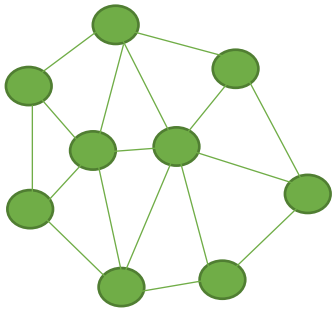
Distribuida: no poseen un centro individual o colectivo. Los nodos se entrelazan unos con otros sin filtro para coartar la información que ofrecen los otros.



Centralizada



Descentralizada



Distribuida

III. Consenso social y teoría de juegos

El R3 es un consorcio de entidades financieras que tienen como fin desarrollar productos desde la tecnología Blockchain para el sector Fintech y banca en general. La era de la digitalización está obligando a las empresas y a las personas a convertirse en usuarios. El ecosistema R3 permite actualizarse a las entidades colaboradoras y no caer en la obsolescencia.

En el comienzo de esta tecnología, la cadena de bloques se basaba en una red pública, donde para todos los usuarios era posible ver las transacciones de Bitcoin. A raíz de ese momento, han surgido dos modelos más de redes: la privada y la híbrida. Aunque las criptomonedas siguen empleando una red pública.

Comenzamos explicando la primogénita. La red pública hace referencia a la accesibilidad y a la apertura; es decir, los usuarios desde la tecnología IoT -Internet de las Cosas- pueden entrar en las plataformas de blockchain y su visibilidad es divulgada. Los datos

están abiertos al público, el software y su desarrollo. Cualquier consumidor o persona interesada puede revisar, auditar y desarrollar sus datos. Tiene medidas de seguridad para que no se altere la base de datos. Su carácter es descentralizado, lo que supuso una gran innovación para los flujos monetarios fiduciarios centralizados.

En segundo lugar, definimos la red privada de blockchain. En contraposición a la red pública, esta tiene un carácter centralizado. La accesibilidad no es abierta si no que cuenta con un acceso restringido a usuarios. No suelen contar las criptomonedas ni se realizan acciones de minería.

Finalmente, la última red es la híbrida. Se caracteriza por mezclar las características de la sinergia entre las dos anteriores. Su accesibilidad es de naturaleza privada, aunque su libro de contabilidad tiene personalidad pública. Es empleado, mayoritariamente, por gobiernos o empresas para compartir entre los mismos organismos sus datos seguros. Está basada en la transparencia y la confianza para sus usuarios o clientes. Y destacamos que es una red parcialmente descentralizada.

ELEMENTOS DEL BLOCKCHAIN Y POSIBLES AMENAZAS

A continuación, vamos a exponer los tres elementos principales de la tecnología blockchain. En primer lugar, contamos con los participantes, todas aquellas personas físicas y jurídicas que colaboran en la solución digital que ofrece la cadena de bloques. Desde usuarios, entidades financieras, autoridades, auditores y más.

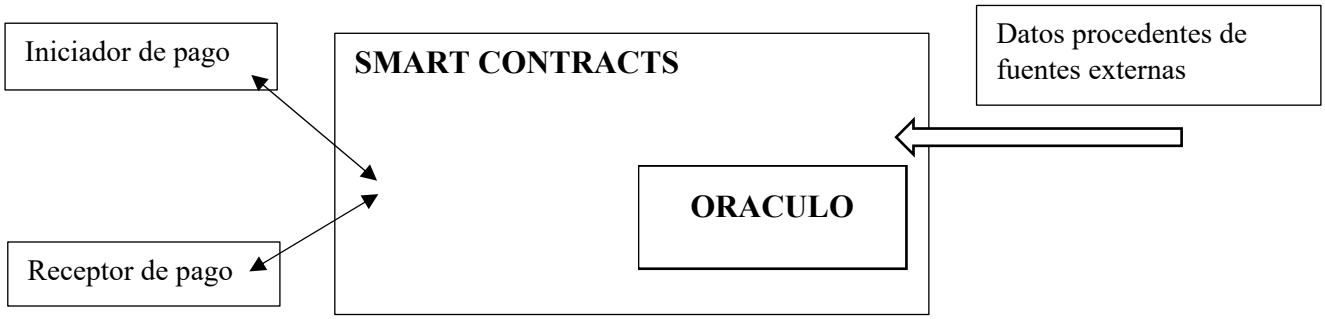
En segundo lugar, encontramos los activos. Elementos digitales de intercambio, almacenaje o protección. Y, finalmente, las transacciones, modificaciones y operaciones registradas en la cadena de bloques.

SMART CONTRACTS

Un contrato inteligente es un código informático que facilita verificar y asegurar el cumplimiento de un acuerdo digital de forma automática. Es ejecutado de manera descentralizada. Sus características principales son la inmutabilidad y la transparencia. Validez independiente de autoridades, es público e invariable al ser desplegado. Pueden seguirse, localizarse y verificarse por las entidades participantes. Los códigos pueden ser

ejecutados por nodos de minería de la cadena de bloques, siendo así un código autoejecutable que puede verificar el cumplimento de términos y condiciones predefinidos.

El código funciona (si pasa X, entonces Y) + condiciones de información externa. Como cualquier programa puede tener fallos de diseño o de desarrollo.



2.2 Naturaleza de las criptomonedas

"Criptomoneda se define por el Grupo de Acción Financiera Internacional (GAFI), "*como una representación digital de valor no emitida ni garantizada por un banco central ni por una autoridad, no necesariamente asociada a una moneda de curso legal, que no tiene la consideración de moneda o divisa, pero es aceptada por personas físicas o jurídicas como medio de pago y que puede transferirse, almacenarse o negociarse por medios electrónicos"*. Esta definición es además empleada en el artículo 1 de la Directiva de modificación de la Directiva (UE) 2015/849 relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo.".

En este proyecto trabajamos sobre el blanqueo de capitales utilizando las criptomonedas y tratando las más relevantes como ejemplos. Procedemos a definirlas con el fin de contextualizar su naturaleza. Por otro lado, denominamos altcoin a aquellas criptomonedas más pequeñas que funcionan como una alternativa frente a las diez principales criptomonedas.

Monedas Digitales. Son un tipo de monedas utilizadas y conocidas socialmente para realizar intercambios tanto de bienes como de servicios. Cada mercado decide el valor de las mismas.

Criptodivisas o Criptomonedas. En la clasificación enmarcaríamos ambos conceptos dentro de una subcategoría de monedas digitales. Teniendo en cuenta el matiz de que estas son emitidas y controladas desde la descentralización. Estas carecen de soporte físico que las respalde.

Criptoactivos. Denominados también criptomonedas o criptodivisas. Hacen referencia a la representación digital de un valor no garantizado por un banco central ni autoridad financiera o pública. No tienen porqué respaldar a una moneda de curso legal. Están socialmente aceptados para transferirse, almacenarse y negociarse a través de medios electrónicos.

Monedas Virtuales. Según el Banco Central Europeo, en el año 2012, las monedas virtuales se clasifican como un ejemplar de monedas digitales no reguladas. Son emitidas y empleadas por las personas que las desarrollan y es aceptada por una comunidad para ser utilizada por la misma.

Dinero fiduciario. Se denomina dinero fiduciario a aquel que no está respaldado por la confianza social de las personas sobre aquellas entidades que lo emiten, no posee un respaldo material.

Moneda estable. Es aquella moneda fiduciaria digitalizada y basada en la tecnología blockchain. Es una moneda diseñada para minimizar la variabilidad del precio, puede estar vinculada a una criptomoneda. No están reguladas lo que conlleva inseguridad por parte de sus usuarios. Se usan sistemas de contabilidad basados en monedas fiduciarias.

WALLETS Y EXCHANGES

Se considera “wallet” aun software o programa informático que almacena tanto claves públicas y privadas. Estas claves permiten operar con criptomonedas, enviando como recibiendo transacciones. Ejemplificando de modo comparativo con un uso más divulgado socialmente, decimos que las claves públicas podrían compararse con el número de la cuenta bancaria que puede ser accesible a todo el mundo; sin embargo, las

claves privadas son las claves que te dan acceso a tu cuenta bancaria, el pin de la tarjeta, por ejemplo.

Existen distintos tipos de billeteras donde almacenar los criptoactivos de los usuarios, los clasificamos en:

Paper wallet: se encuentra siempre offline. Se refiere a un documento impreso donde se contiene una dirección publica a la que se pueden enviar criptomonedas y una clave privada. Podría ser un código QR, el cual te facilita e inmuniza contra ataques, las transacciones, ya que solo hay que escanearlos. La mayor ventaja es que no está almacenada en ninguna red.

Wallet móvil: este formato permite una operabilidad más accesible, ya que puedes llevar contigo en el teléfono móvil la billerta virtual. Se ejecutan las transacciones a través de una aplicación, realizando los pagos desde el smartphone. Hay algunas aplicaciones que te permiten, incluso, realizarlas por contacless. Sin embargo, una desventaja respecto a otro tipo de wallet es que este está sujeto a una mayor vulnerabilidad ante ataques informáticos.

Wallet online: este formato almacena las claves privadas a través de los servidores de la empresa que facilita este servicio. Permite que los usuarios tengan acceso a las billeteras desde cualquier parte.

Wallet físico/hardware: como medida de seguridad, estos dispositivos de almacenamiento en frío disponen de un chip de seguridad que permite que tus claves privadas no ingresen en el ordenador. A la hora de operar con las criptomonedas del wallet, solo habrá que introducir dicho pin. Este formato ofrece la posibilidad en caso de pérdida del dispositivo, de recuperar mediante la “semilla” o clave que se recibe cuando se encarga, las criptomonedas.

Wallet de escritorio: están instalados en los ordenadores personales de los usuarios; por lo tanto, las claves privadas se almacenan en el disco duro de los mismos. Estos ordenadores puedes ser vulnerables una vez están conectados a la red.

REGULACION DE LAS CRIPTOMONEDAS

La naturaleza jurídica de las criptomonedas carece de un enfoque consensuado globalmente, lo que deriva en una carencia de índole regulatoria al no enmarcarse en un sistema financiero regular. Las estrategias que se ha planteado e incluso, en casos,

adoptado en algunos países es la extrapolación de la normativa existente para valores e instrumentos financieros. La aplicabilidad de estas normativas es reprochable debido, como hemos dicho, a que las criptomonedas no están sujetas a una naturaleza bien definida, que se consideraría el punto de partida.

Desde Europa, teniendo en cuenta que países europeos han adoptado esa primera estrategia como válida. Las directivas que preocupan y se relacionan más con este tema son: (l) la segunda directiva de entidades de dinero electrónico, (ll) la segunda directiva de servicios de pago y (lll) el MIFID ll.

La Segunda Directiva de Dinero Electrónico, la Directiva 2009/110 CE del Parlamento Europeo y del Consejo, de 16 de septiembre de 2009, establece como posible que las criptomonedas se encuadren o, mejor dicho, se regulen, a través de esta directiva, comparándolas al dinero electrónico. Aunque como ya hemos explicado anteriormente, las criptomonedas no tienen un respaldo físico.

Para comprender la carencia normativa, tenemos que comparar el dinero físico y el electrónico comparten una base legal y un respaldo en oro de los Bancos Centrales de cada país. Sin embargo, las criptomonedas no comparten ninguna de esas características. De aquí su problemática.

Por otro lado, se debe contemplar que las divisas virtuales puede que no se puedan enmarcar dentro de ninguna normativa vigente hasta el momento; por lo que, se debería valorar la implementación y creación de una norma completamente nueva.

Finalmente, como método coercitivo, se podrían prohibir a nivel internacional este tipo de activos, aunque esta no se reflexiona más que por las vertientes más negacionistas. Al fin y al cabo, las sociedades y sus reglas deben adaptarse a los cambios y a sus progresos.

Como ejemplo de esta adaptación tenemos el “dólar de arena”. Esta criptomoneda se ha implementado en Bahamas, así como el yuan digital en algunas ciudades chinas. Esta moneda digital es la primera a nivel emitida por un Banco Central, en este caso el de Bahamas. La finalidad del gobierno respecto a este proyecto innovador es descentralizar un dinero nacional para sus habitantes. Los ciudadanos dispondrán de una billetera móvil eliminando la intermediación de instituciones bancarias y financieras evitando los gastos de los movimientos del dinero.

3. ANALISIS DE LA TECNOLOGIA DE LA INTELIGENCIA ARTIFICIAL

Definición de Marvin Minsky, uno de los pioneros de la Inteligencia Artificial: "ciencia de construir máquinas para que hagan cosas que, si las hicieran los humanos, requerirían inteligencia", desde una perspectiva científica podemos hablar de la base de la informática moderna. La confluencia de teorías es la semilla de esta innovación: Teoría de la Computación, Cibernética, Teoría de la Información, Procesamiento Simbólico.

Una definición más precisa podría ser la de Nebendah (1998), "campo de estudio que se enfoca en la explicación y emulación de la conducta inteligente en función de procesos computacionales basados en la experiencia y el conocimiento continuo del ambiente.".

El término inteligencia artificial ha ganado especial renombre en muchos ámbitos durante esta última década. Aunque esta tecnología data estudios de la década de los años 50, su crecimiento, dentro del sector financiero y económico en el que se basa este proyecto, se debe, fundamentalmente, a tres factores. El primero de ellos es la mejora de los algoritmos que conforman esta tecnología, adaptándola a la actualidad y a sus necesidades. El segundo se centra en un aumento exponencial de datos que procesar y almacenar. Y, por último, el bajo coste que permite realizar las funciones anteriores. Las funciones cognitivas en las máquinas, derivadas de la inteligencia artificial pueden cometer errores debido a la naturaleza centralizada de esta tecnología, dando lugar a la manipulación de los datos. Esto no garantiza, por lo tanto, la autenticidad de los mismos ni las fuentes. Sus decisiones se pueden volver peligrosas, irreflexivas y erróneas.

Debemos comprender que esta tecnología trabaja con los datos procedentes de las aplicaciones web, de las redes sociales y de los dispositivos IOT entre otros, esto suma una gran cantidad de información que procesar. Por ello, para asegurar y proteger esos elementos de una manera descentralizada, y eso solo se consigue a partir de la sinergia entre blockchain e inteligencia artificial.

En 2021, el Gobierno de España se propuso impulsar un marco referencial sobre una regulación de esta tecnología a través de la creación de un organismo de supervisión cuyo objetivo se centrará en minimizar y controlar los riesgos existentes o posibles de su implementación en nuestra realidad, no solo económica. En la Disposición adicional centésima trigésima de la Ley 22/2021, de 28 de diciembre, de Presupuestos Generales del Estado (PGE) ya publicada en el BOE. Se denominará como "Agencia Española de Supervisión de la Inteligencia Artificial".

Esta incorporación es consecuencia de la creciente utilización por parte de organismo tanto públicos como privados de los algoritmos de la IA. La auditoría a estas aplicaciones será responsabilidad de la futura agencia.

Se estableció, a nivel nacional, una estrategia desde la España Digital sobre la inteligencia artificial en 2020 con miras al 2025. En ella se podían encontrar siete objetivos:

i. "Potenciar la excelencia científica y la innovación en IA;
ii. Liderar el desarrollo de herramientas, tecnologías y aplicaciones para la proyección y uso de la lengua española en la IA;
iii. Promover la creación de empleo cualificado, impulsando la formación y educación, estimulando el talento español y atrayendo el talento global;
iv. Incorporar la IA como factor de mejora de la productividad, de la eficacia en la Administración Pública y motor del crecimiento económico sostenible e inclusivo;
v. Generar un entorno de confianza de la IA, tanto en el plano tecnológico, como en el regulatorio y en el de su impacto social;
vi. Impulsar el debate a nivel global sobre el desarrollo tecnológico de valores humanistas (*Human-Centered AI*), centrado en velar por el bienestar de la sociedad, creando y participando en foros y actividades divulgativas para el desarrollo de un marco ético que garantice los derechos individuales y colectivos de la ciudadanía;
vii. Potenciar la IA inclusiva y sostenible, como vector transversal para afrontar los grandes desafíos de nuestra sociedad, específicamente para reducir la brecha de género, la brecha digital y apoyar la transición ecológica y la vertebración territorial.". (Pina, 2022).

4. CONVERGENCIA Y SU PROYECCION

Debemos tener en cuenta que ambas tecnologías, tanto blockchain como la IA, presentan deficiencias en su uso; sin embargo, una sinergia entre ambas puede abordar esos errores eficazmente. Los algoritmos de la inteligencia artificial están basados en datos que permiten aprender, inferir y tomar decisiones. Estos mismos algoritmos de

aprendizaje automático van funcionan de manera notable cuando se recopilan de forma segura en una plataforma. A esta plataforma la ponemos el nombre de blockchain o cadena de bloques, donde se almacenan los datos y las transacciones firmadas criptográficamente, siendo así validadas por los nodos, lo que permite la inalterabilidad. Esta unión forja un resultado confiable e indiscutible. En definitiva, la IA y BL forman un sistema seguro, inmutable y descentralizado para contenido sensible ya que siembra un entorno seguro.

Todo el conjunto de fases desde el procesado de los datos, análisis y la toma de decisiones sería compartido públicamente, confiable, firmados digitalmente e inmutables, almacenándose así en las cadenas de bloques. Sin necesidad de intermediarios.

A continuación, vamos a exponer la proyección a corto medio plazo de esta convergencia.

Últimamente, tanto la tecnología blockchain como la inteligencia artificial están cogiendo renombre dentro de la sociedad, no solo especializada en el ámbito tecnológico digital. La convergencia de ambas suena a futuro, pero ya existen experimentos y pruebas empíricas sobre la misma. No podemos centrarnos únicamente en estas dos tecnologías debido a que, como ya hemos mencionado, promueven un espacio amplio, seguro e inmutable a la hora de almacenar, procesar y verificar datos digitales. No obstante, cuando pensamos en el fututo debemos enmarcar en él también a otras tecnologías como IoT y Big Data. Todas ellas juntas aportan, no solo mayor seguridad en cualesquiera transacciones si no que elaboras dentro de cadenas de bloques seguros un espacio inmutable donde registrar cualquier documento digital o transacción.

III. ANALISIS CRITICO

1. VENTAJAS

Dentro de la buena praxis, podemos referir que la introducción de las cadenas de bloques donde se encuentran las criptomonedas y la revolucionaria inteligencia artificial aportan a los usuarios y al futuro una serie de características positivas. De entre todasa ellas vamos a destacar las más relevantes para nuestra investigación:

- Descentralización y autorregulación: Estas cualidades fueron el motor que impulsó la creación de las criptomonedas, basándose en la tecnología blockchain. La oportunidad de que los usuarios escojan la dirección del mercado, ajena a autoridades superiores. Además, la inteligencia artificial colabora encontrando patrones; es decir, su procesamiento permite informar de propias especulaciones más tangibles y precisas que las que pueden dar usuarios en la inflación del valor de mercado.
- Seguridad: La tecnología de las cadenas de bloques permite el almacenamiento de los datos y sus transacciones de forma encriptada, lo que conlleva una mayor confianza de los usuarios. La inteligencia artificial tiene como reto estimar o conjeturar sobre patrones; en el caso de la seguridad, es una gran ayuda a las cadenas de bloques ante la detección de ciberataques.
- Smart Contracts: La continua innovación tecnológica junto con el fuerte apoyo de convergencia entre nuestras tecnologías de estudio, este tipo de contratos podrán desarrollar su máximo potencial dentro de aplicaciones. La garantía de que los derechos y obligaciones de los usuarios, dentro de un marco legal, se cumplirán desde la base de confianza bidireccional con el apoyo de la inteligencia artificial y su capacidad de corregir errores. Se busca la eficiencia en negocios multiusuario.
- Ciberseguridad: Es un campo en auge debido a la alta digitalización de servicios y bienes, lo que conlleva a que a una inteligencia descentralizada con toma de decisión sobre la incorporación de los agentes involucrados permitirá un mayor control formal ante amenazas.
- Almacenamiento: La capacidad inmensa del blockchain junto con la habilidad de ordenar de la inteligencia artificial, ahorra espacio además de esfuerzo personal. Reduce costes. Teniendo en cuenta también las posibilidades que ofrece la inteligencia artificial automatizando los procesos operativos y aumentando la

capacidad de análisis. Esto forja que el futuro del sistema financiero y la economía en general se beneficien de esta unión.

2. RIESGOS

Desde la perspectiva más alejada al control formal de esta convergencia de tecnologías disruptivas, podemos establecer las posibles contingencias también ligadas a ella. Podemos pensar que algunas de las principales características tanto del blockchain como de la IA, se pueden volver en contra de lo que para en algún momento fueron creadas. Estos instrumentos poseen cualidades que a menudo pueden suscitar incertidumbre sobre su implementación.

El Banco de España en conjunto con la CNMV instruyeron en 2018 sobre los riesgos de las criptomonedas; volatilidad, falta de transparencia y complejidad, esos fueron los tres atributos que emplearon para describir a los criptoactivos. De las contingencias extraídas del documento, vamos a escoger las que, en relación con nuestro tema, los que vemos más reseñables y añadiremos otros, de manera autónoma, tras el estudio bibliográfico.

1. Ámbito regulatorio débil o inexistente. Desde España, la regulación como ya hemos analizado anteriormente es precaria. A nivel europeo no existe, como tal, un marco que acoja con exactitud los límites de los criptoactivos. Por otro lado, desde la IA están aconteciendo movimientos legislativos más visibles y aplicables, pero sin la suficiente fuerza real como para evitar amenazas tangibles.
2. Inversiones de alto riesgo. Según la Comisión Nacional del Mercado de Valores se estima que existen aproximadamente 7.000 -dato recogido en 2021- criptomonedas muy similares al Bitcoin. Esto provoca inseguridad por el alto componente especulativo que conlleva la inversión.
3. Anonimato. Es un riesgo conjunto de ambas tecnologías. La privacidad por defecto y por diseño es una cualidad explotada y requerida por separado. Al unirse, provoca un anonimato peligroso para el usuario. El sistema de doble encriptación explicado mantiene las transacciones realizadas por los usuarios accesibles solamente a quien posea la clave de acceso a la cuenta privada junto con la opacidad de análisis de datos.

4. Interpretabilidad. La capacidad de la inteligencia artificial de procesar datos es abrumadora, pero en su uso cabe la estancia de personas físicas que sean capaces de interpretar esos datos.

5. Formación de precios. La manipulación a la que están sometidas las criptomonedas es vertiginosa. Al no estar sujetas de mecanismos eficaces regulatorios, la información sobre su valor puede ser inexacta o poco fiable.
6. Fronteras. Como ya sabemos la regulación nacional e internacional es precaria. En las transacciones puede existir una diferencia transfronteriza entre los actores implicados; e incluso, es posible que por medio herramientas como VPN (redes privadas virtuales) que desvinculen la posición real, los intercambios sufran imprevistos y malas praxis.
7. Robo, estafa o pérdida. La tecnología que se emplea para emitir las criptomonedas no está supervisada; por lo que se enfrenta a riesgos específicos como la perdida o robo de las claves privadas de los wallet. Esto desemboca en la gran contingencia de los usuarios de no poder recuperar sus criptoactivos.

IV. APLICACIÓN A LA CIBERSEGURIDAD DE LA CONVERGENCIA

1. TÉNCNICAS APLICADAS Y MODUS OPERANDI

a. Mixers, / mezcladores

Una de las principales características y mayores deseos de la comunidad de las criptomonedas es la mejora de la anonimización y la privacidad de sus usuarios. Este elemento dificulta y entorpece a las instituciones financieras en la investigación y prevención del blanqueo de capitales.

Con esta idea surge la técnica mixer, cuyo funcionamiento es sencillo. El usuario envía criptomonedas a estos servicios, los mixers, y estos devuelven otras criptomonedas del mismo valor, depositadas por otras personas a la dirección inicial. Si ponemos un ejemplo más tangible, podríamos decir que un grupo de personas introducen dentro de una caja monedas, un mixer agita la caja, y posteriormente, devuelve a cada usuario la cantidad de monedas que introdujo, pero estas son distintas a las iniciales manteniendo el mismo valor.

b. Deep web/ Darknet

La Deep web o darknet no es un instrumento con única finalidad delictiva, aunque esta red de internet fue creada para comercializar eludiendo la fiscalidad de los países y ahorrar costes de distintos servicios. Actualmente es conocida, por dar rienda suelta a la delincuencia a través del anonimato. Dentro del blanqueo de capitales, las criptomonedas son la principal fuente de movimiento de dinero negro en este mercado. Las criptomonedas y su anonimato, además en conjunto con el de la darknet permiten a los delincuentes ser invisibles o prácticamente invisibles a las autoridades.

Podemos encontrar desde robo de tarjetas de crédito y débito como compra y venta de criptomonedas, además de otros servicios de blanqueo.

La ruta de la seda fue uno de los primeros y principales servicios de esta red, comprando y vendiendo droga por internet. Ahora con la ayuda de las criptomonedas su rastreo se ha convertido en un reto para las autoridades.

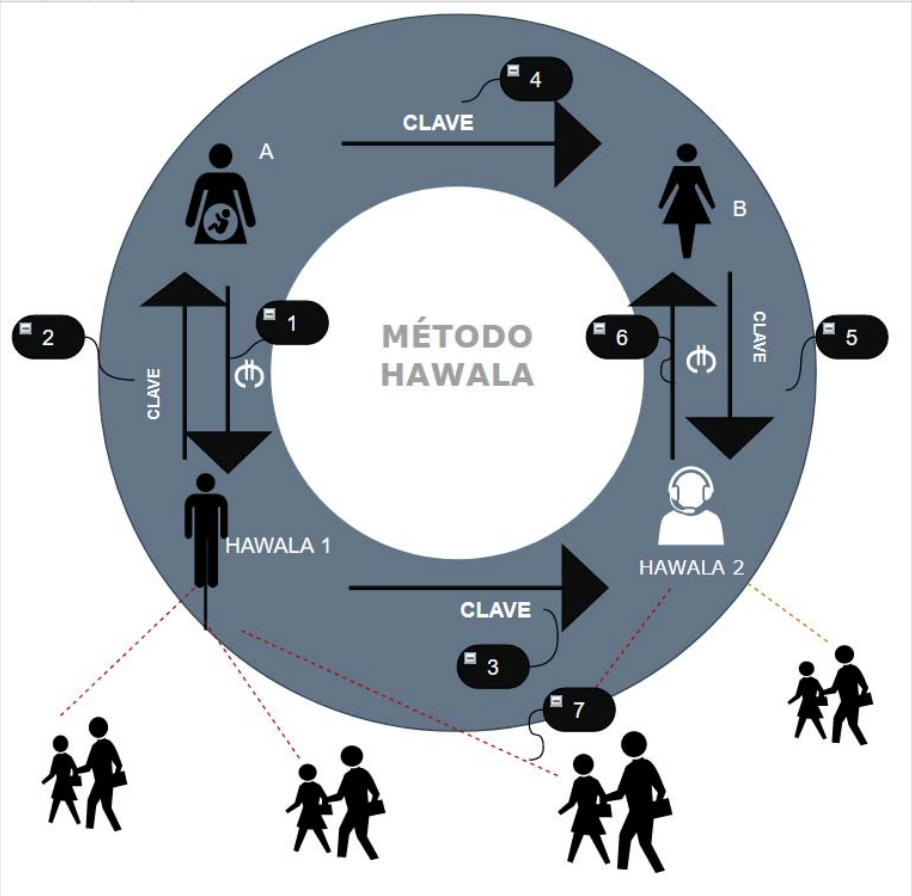
(Porras, M. 2021. Imagen propia. "Venta de criptocuentas robadas").

a. Dispositivos físicos de almacenamiento de criptomonedas.

La técnica de blanqueo de capitales en el que se emplean estos dispositivos consiste en almacenar tus monedas en un aparato físico con una clave privada. Pasan desapercibidos por su forma, son completamente legales en España y alrededores y son capaces de transportarse a través de cualquier frontera. Dentro de ellos se llevan las criptomonedas, muchas veces se relaciona o se complemente con el método de colaboración o hawala.

Uno de sus mayores inconvenientes a la hora de abordar estos dispositivos en una investigación es que en el momento de incautarlo, no hace falta estar presente con el dispositivo para operar con él. Debido a su tecnología permite operar a través de la clave de manera remota; por lo tanto, aunque estes en presencia del aparato, sus criptomonedas puedes enviarse en cualquier momento si se tiene la clave privada.

e. Hawala



https://app.diagrams.net/

b. Bots

Se entienden como una simulación y/o especulación de operaciones con el objetivo de que los criptoactivos aumenten o reduzcan su valor de mercado según el interés del especulador. Esto sire como modus operandi porque al especular sobre el valor de las criptomonedas, las organizaciones pueden comprar o vender las mismas según sus intereses para introducir o sacar el dinero sucio.

c. NFT (NOT FUNGIBLE TOKEN) o token no fungible.

Se refiere a un token criptográfico no intercambiable, es único e irrepetible. Se basa en un registro coleccionable verificable a través de la tecnología blockchain catalogándolo, así como original. Este modus operandi de blanqueo de capitales lo compararíamos con

el blanqueo por medio de arte físico, explicado con anterioridad. Los archivos digitales se venden por sumas de criptomonedas muy elevadas, con el fin de blanquea dinero con ellas.

"*Jack Dorsey, uno de los creadores de la popular red social Twitter, vendió su primer "tweet" por un valor superior a los US$ 2.9 millones"*

https://parentesis.com/noticias/culturageek/El_jefe_de_Twitter_Jack_Dorsey_vendio_su_primer_tweet_como_NFT_por_29

d. Criptomulas:

Uno de los delitos más comunes digitalmente en estos tiempos, son las estafas a través de la red. Estas estafas permiten manejar dinero ajeno e incluyendo las facilidades delictivas de la Deep web al igual que las ventajas que ofrecen las criptomonedas, las estafas, dentro de los delitos contra el patrimonio se ha convertido en uno de los predilectos para las organizaciones criminales. Conviene destacar que la mayoría de los fondos a blanquear de esta forma digital provienen de tráfico o terrorismo.

Las criptomulas son un elemento de la pirámide de las organizaciones criminales fundamental, debido a que este eslabón permite la movilización de los activos y facilita el despiste a las investigaciones. Las criptomulas son captadas, mayoritariamente, con conocimientos en el sector digital y las tecnológicas de la comunicación e información (TIC), para que oculten tanto el origen como el destino de los fondos de procedencia ilícita.

V. POLÍTICA CRIMINAL E INVESTIGACION INCONVENIENTES
1. RETOS NORMATIVOS Y POLICIALES

Dentro del campo de la tecnología blockchain de las criptomonedas podemos decir que los retos normativos están basados en la carencia de una jurisprudencia emanada por las autoridades legislativas y judiciales de cada país. De esta manera, cada nación tendría su propia actuación delimitada a la hora de investigar y sancionar actos delictivos por medio de esta tecnología.

El Grupo de Acción Financiera Internacional en sus normas de no obligado cumplimiento, publica a través de las investigaciones que la misma organización realiza junto con la participación e innovaciones de los países y sus jurisprudencias, recomendaciones o "soft law" para impulsar el control formal de este progreso tecnológico con uso delictivo.

La creciente preocupación dimanada por los entrañables riesgos que plantea la creciente demanda de adquisición y empleo de criptoactivos, se refleja en una acción incipiente y no en una regulación armonizada y global.

El Proyecto europeo "TITANIUM" (Tools for the Investigation of Transactions in Underground Markets), creado en mayo de 2017 y finalizado en abril de 2020, tenía el objetivo de investigar en colaboración y ayuda de las agencias e instituciones dedicadas a mitigar el terrorismo y el crimen organizado involucrando monedas virtuales y transacciones clandestinas. Interpol fue uno de los quince participantes del equipo multidisciplinar. Durante esos tres años, se establecieron soluciones técnicas a través de datos obtenidos por herramientas e instrumentos forenses desde la privacidad y hermetismo del entorno en el que se movían. Algunas de sus funciones eran:

- "El monitoreo de tendencias en ecosistemas de mercado de moneda virtual y darknet.
- El Análisis de transacciones en diferentes libros de contabilidad de moneda virtual.
- Generar informes de pruebas a prueba de tribunales basados en procedimientos analíticos reproducibles y legalmente compatibles.". (Interpol, 2022).

Desde la perspectiva más policial, podemos observar imitaciones en sus investigaciones por falta de presupuesto para equipos, personal, formación y actuación.

2. IDONEIDAD DEL BLOCKCHAIN CON CRIPTOMONEDAS PARA EL BLANQUEO

En este apartado vamos a exponer algunos de las principales ventajas que atraen a los delincuentes a emplear criptomonedas para el blanqueo de capitales.

EVASION EN EL ANALISIS DE TRAZABILIDAD

Con el fin de evitar la trazabilidad de las operaciones, se pueden distinguir dos estrategias principales, de protocolo y de blockchain.

En primer lugar, estrategias de protocolo. En el caso de que se quiera ocultar la trazabilidad, se evitará consultar el saldo desde tu dirección de manera online, así no aparece en blockchain.com. Si no se ingresa con las claves del wallet, se oculta la dirección. También, se puede distraer la trazabilidad a través de los mixers con múltiples direcciones. Se debe observar recurrentemente el estado del wallet para prevenir comportamientos involuntarios o desconocidos. Finalmente, no usar direcciones jerárquicas que pueden recuperarse.

Por otro lado, disimular la trazabilidad según estrategias de blockchain a partir de; por un lado, proveedores en darknet, algunos usan precios muy específicos (suelen incluir muchos decimales). Quieren calcular un tipo de cambio para un monto en moneda fiduciaria. Se oculta a través de una mercancía. Si hay salto restante se dirige a cambiar o sombrar la dirección creando un/dos outputs. Usar denominaciones al recibir pagos y evitar cantidades raras. Y, por otro lado, obstaculizando el análisis en transacciones anteriores a través de mixers u otras técnicas menos comunes.

ANONIMATO

Las transacciones realizadas de Bitcoin u otras criptomonedas pueden verse a través de blockchain.com, y en el caso de la segunda más famosa, Ethereum, ¿CUAL? La información que se recoge de estos registros de dominio público son datos como, por ejemplo, de origen, destino, cantidades o saldos. A priori toda esta documentación facilita la investigación, pero debemos tener en cuenta al usuario real de que operar o posee esas mismas criptomonedas y controla su operativa.

Para ello, existen formas aproximadas de verificar esta identidad de los usuarios. En primero lugar, la mayoría de las plataformas existentes de cambio de monedas, ya sean

Bitcoin u otras, solicitan datos personales de los usuarios para que su identificación resulte más sencilla.

El segundo factor a tener en cuenta para garantizar el anonimato se dará en los casos donde se efectúen pagos con Bitcoin u otras criptomonedas de registro público. La trazabilidad se relaciona con una dirección IP (Interfaz de programación de aplicaciones) de la que se pueden obtener datos del usuario. Existen, por supuesto, formas de evadir estas verificaciones de seguridad; en el caso de querer ocultar nuestra identidad o datos relevantes hay ciertas técnicas de ofuscación como las VPN o red privada virtual, servidores proxi o Tor, red de comunicaciones distribuida que implementa la tecnología Onion Routing.

Finalmente, con el fin de descifrar la identidad, se buscará en foros donde, en ocasiones, usuarios publican datos personales. Este error da viabilidad a la apertura de información desde seudónimos o nombres de usuarios.

OFUSCACION A TRAVÉS DE MOVIMIENTOS

Dentro de las criptomonedas, existen numerosas criptomonedas alternativas a las 10 principales o, también, conocidas como altcoins. Dentro de estas podemos encontrar criptodivisas con unas características más ajustables a la comisión de delitos económicos como es el blanqueo, un ejemplo bastante empelado por organizaciones criminales es el de Monero.

Estas monedas encriptadas deben extraerse de la cadena de bloques lo más temprano posible; es decir, ser vendidas o enviadas con agilidad por moneda fiduciaria. Así se pretende evitar ser identificado como usuario o titular de las mismas. Estas monedas pasan por múltiples transacciones a través de mixers, ocultando así su origen. Los esquemas de mezcla que se utilizan en estos casos permiten difuminar el flujo y convertirse en transacciones mixtas. Y finalmente se consigue cambiar la forma y venderlas por otra moneda en un par de ocasiones.

3. BLOQUEO, INCAUTACION Y DECOMISO DE CRIPTODIVISAS

La ORGA o la Oficina de Recuperación y Gestión de Activos, es un órgano de la Administración encargado de ofrecer apoyo a los órganos judiciales durante la investigación, gestión y recuperación de activos que tienen su origen en actividades delictivas.

La naturaleza socioeconómica de estas acciones tipificadas en la legislación española provoca el desbordamiento de jueces y fiscales para su decomiso, por lo que esta agencia ejerce un gran apoyo con sus servicios.

Respecto a las monedas y activos virtuales, la ORGA, al igual que otros órganos judiciales se sitúen ante situaciones conflictivas. El valor variable de los activos virtuales deja en una posición incómoda a los tribunales. Desde los wallets fríos, teniendo en propio poder las claves privadas puede extraerse el activo sin posibilidad de evitarlo.

Algunos Exchange tienen convenios con instituciones y autoridades, pero no cuentan con el apoyo para poder congelar esas cuentas virtuales.

Este se podría decir que es uno de los grandes retos frente a las organizaciones criminales y sus técnicas con las nuevas tecnologías para el blanqueo y elusión de la justicia.

VI. CONCLUSIONES

La constante evolución que sufren las nuevas tecnologías las hace vulnerables y tentadoras para las organizaciones criminales. Es un sector ágil, barato, accesible, global, descentralizado y carente de regulación.

Los principales retos que se presentan ante esta convergencia se evalúan de una forma más correcta y objetiva desde cada una de las tecnologías.

Los riesgos que supone la tecnología blockchain desde el blanqueo de capitales se centra en la falta de regulación y supervisión para gobiernos e instituciones financieras reguladoras. También los riesgos desde la ciberseguridad, por la vulnerabilidad de las plataformas de compraventa o intercambio a ataques informáticos y aquellos en relación con la estabilidad del mercado económico y su integridad. La falta de protección de los usuarios ante estafas u otros delitos cibernéticos como el fraude debido al anonimato y dificultad para trazar o rastrear de las transacciones. Lo que afecta directamente a la debida identificación de los usuarios y, por consiguiente, a sus obligaciones de información con el fin de prevenir este delito.

La atracción de los delincuentes por esta tecnología viene dada por la inmutabilidad del sistema, su anonimato, la ausencia de terceros -instituciones financieras-, el ahorro de costes y, su transparencia.

Aunque relaciones la tecnología blockchain con las criptomonedas, y en parte, es cierto; las cadenas de bloques son sistema DLT, pero no todos los sistemas DLT son cadenas de bloques. Con esto podemos decir que esta tecnología no únicamente se centra en dinero, sino que también es un medio alternativo muy útil para el envío de datos.

Una de las ventajas más importantes dentro de esta convergencia es el anonimato, de manera de dificultar la trazabilidad a partir del alejamiento de las instituciones financieras permite a los delincuentes adueñarse de las identidades y de las criptomonedas. Esto provoca la pérdida del activo sin opción a reclamación penal.

El phishing o robo de credenciales de forma online también para su utilización en web ilegales, incluso también en las webs de plataformas bancarias legales y oficiales.

La custodia de las criptomonedas no está supeditada a control formal de instituciones bancarias reguladas, lo que puede provocar una invalidación del software, un robo de las

claves de usuario o una mala praxis por parte de los exchanges para la gestión del riesgo de ciberataques.

En conclusión, la convergencia de tecnologías ofrece una inmensidad de opciones prácticas y beneficiosas para nuestro futuro, sin embargo, no podemos abandonar el pensamiento critico de los riesgos y amenazas que entran dentro de su implementación. Las organizaciones criminales poseen una cualidad notable de adaptación y con las nuevas formas de criminalidad y modus operandi, las autoridades policiales y gubernamentales se sitúan en un constante dinamismo controlador.

La tecnología blockchain dentro de las criptomonedas, supone un vació legislativo temporal. Como hemos estudiado, las dificultades de consenso internacional para su regulación establecen un terreno, de momento, prácticamente llano para el blanqueo. La inteligencia artificial añadiría una capacidad superior en el análisis de datos, pero es necesaria la formación de personal cualificado para poder interpretar correctamente y aplicar soluciones eficientes.

Desde la perspectiva más negacionista y obsoleta de prohibir este avance, se propone la prohibición de las criptomonedas y de la IA. Esto solo ralentizaría procesos, estancaría innovaciones y obstruiría el paso hacia el futuro.

Por lo tanto, tanto la IA como las monedas virtuales seguirán operando, con o sin regulación de por medio. En definitiva, la mejor opción valorada tras el estudio es continuar observando la evolución.

VII. BIBLIOGRAFIA

Agrasar González, B. (2020, abril). *La utilización de criptomonedas en relación con el fraude fiscal y blanqueo de capitales*. Universidad Pontificia Comillas. Consultado en https://repositorio.comillas.edu/rest/bitstreams/408617/retrieve por última vez 13/10/2021.

Banafa, A. (2019, 6 mayo). *Blockchain y la inteligencia artificial: ¿La pareja ideal?* BBVA - Open Mind. Consultado en octubre de 2021, en https://www.bbvaopenmind.com/tecnologia/inteligencia-artificial/blockchain-y-la-inteligencia-artificial-la-pareja-idealblockchain-y-la-inteligencia-artificial-la-pareja-ideal/.

Banco de España. (2021, febrero). *Comunicado conjunto de la CNMV y del Banco de España sobre el riesgo de las criptomonedas como inversión*. Banco de España Eurosistema. Recuperado febrero de 2022, de https://www.cnmv.es/portal/verDoc.axd?t=%7be14ce903-5161-4316-a480-eb1916b85084%7d

Blog de Registradores de España. Las 3 fases del blanqueo de capitales: colocación, encubrimiento e integración. Consultado en http://registradores.org/blog/fases-del-blanqueo-de-capitales/ por última vez el 01/12/2021.

Centro Criptológico Nacional. *CARLA*. Consultado en https://www.ccn-cert.cni.es/soluciones-seguridad/carla.html por última vez 23/10/2021.

Centro Criptológico Nacional. (2020). *Las 10 claves del Centro Criptológico Nacional para gestionar ciberincidentes*. Consultado en https://www.ccn-cert.cni.es/seguridad-al-dia/actualidad-ccn/11261-las-10-claves-del-centro-criptologico-nacional-para-gestionar-ciberincidentes.html por última vez 21/11/2021.

Comisión Nacional del Mercado de Valores. (2018). Consideraciones de la CNMV sobre "criptomonedas" e "ICOs" dirigidas a los profesionales del sector financiero. Consultado en https://www.cnmv.es/loultimo/comunicadoCNMV_ICO_ES%20final.pdf por última vez el 05/11/2021.

ComputerWorld. (2021, diciembre). *España quiere atajar los riesgos de la inteligencia artificial*. Recuperado enero de 2022, de https://www.computerworld.es/legislacion/espana-quiere-atajar-los-riesgos-de-la-inteligencia-artificial

Dai, W. (1998). B-money. Consultado en http://www.weidai.com/bmoney.txt por última vez el 05/10/2021.

De la Cueva González-Cotera y Gómez Barrero. (2018). La tributación del bitcoin y las criptomonedas en las personas físicas. Consultado en http://www.elderecho.com/contenido_juridico/consultas_legales/bitcoins-tributacion-fiscalidad-criptomonedas-impuesto_11_1194430001.html por última vez 22/01/2022.

EBA. (2013). Aviso a los consumidores sobre las monedas virtuales.

EUROPOL. (2017). Internet Organised Crime Threat Assessment (IOCTA). Consultado en https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2017 por última vez el 09/02/2022.

Interpol. (2020). *Project Titanium*. Recuperado enero de 2022, de https://www.interpol.int/es/Who-we-are/Legal-framework/Information-communications-and-technology-ICT-law-projects/Project-Titanium

Glover, H. (2019). ¿Qué es y en qué consiste el proyecto Titanium de la Unión Europea contra el crimen organizado? *Confilegal*. Consultado en

https://confilegal.com/20180731-que-y-en-que-consiste-es-el-proyecto-titanium-de-la-union-europea-contra-el-crimen-organizado/ por última vez 14/11/2021.

Godoy, G. (2019, 27 septiembre). *El lavado de dinero con criptomonedas: ¿Cómo funciona el criptolavado?* COINTELEGRAPH. Consultado el 13 de octubre de 2021, en https://es.cointelegraph.com/news/money-laundering-how-does-cryptolaundering-work.

Gonzalez Cappa, D. (2021, 2 octubre). *Cómo funciona la hawala, el sistema financiero informal con siglos de historia que mueve millones de dólares en el mundo*. BBC NEWS. Consultado en https://www.bbc.com/mundo/noticias-58735962 por última vez el 13/11/2021.

GDPR.eu. (2019, 19 febrero). *General Data Protection Regulation (GDPR) Compliance Guidelines*. Consultado en https://gdpr.eu/ por última vez el 15/12/2021.

Gorjón, S. (2014). Divisas o Monedas Virtual: El caso de Bitcoin. Banco de España.

K. Salah, M. H. U. Rehman, N. Nizamuddin and A. Al-Fuqaha, "Blockchain for AI: Review and Open Research Challenges," en IEEE *Access*, vol. 7, pp. 10127-10149, 2019, doi: 10.1109/ACCESS.2018.2890507 consultado por última vez 14/11/2021.

Krugman, P. (2013). Bitcoin is evil. The New York Times. Consultado en https://krugman.blogs.nytimes.com/2013/12/28/bitcoin-is-evil/ por última vez el 02/03/2022.

La Información. (2016). 25 formas de "cazar" a un blanqueador de capitales. Consultado en https://www.lainformacion.com por última vez a 27/10/2021.

Martínez, O. (2016). Bitcoins y prevención de blanqueo de capitales. Expansión. Consultado en

http://www.expansion.com/juridico/opinion/2016/09/29/57ed56ff468aebfe2d8b4629.html por última vez el 25/11/2021.

Murga, A. (2021, junio). *Tecnológicas y paraísos fiscales bajo el foco: ¿qué es el impuesto global y cómo funcionaría?* Forbes. Recuperado en febrero de 2022, de https://forbes.es/empresas/102878/tecnologicas-y-paraisos-fiscales-bajo-el-foco-que-es-un-impuesto-global-y-como-funcionaria/

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.

Natour, L. (2017). El bitcoin, ¿la moneda de los cibercriminales? Consultado en http://www.abc.es/tecnologia/redes/abci-bitcoin-moneda-cibercriminales-201706021218_noticia.html por última vez el 22/10/2021.

Párraga, V. (2021, 20 septiembre). Vuelta de tuerca a la ciberdelincuencia: cuando los objetivos son fábricas inteligentes y servicios esenciales. *Cloud Computing*.Consultado en https://www.revistacloudcomputing.com/2021/09/vuelta-de-tuerca-a-la-ciberdelincuencia-cuando-los-objetivos-son-fabricas-inteligentes-y-servicios-esenciales/ por última vez 17/01/2022.

Pastor, J. (2018b, septiembre 23). *Qué es blockchain: la explicación definitiva para la tecnología más de moda*. Xataka. Consultado en https://www.xataka.com/especiales/que-es-blockchain-la-explicacion-definitiva para-la-tecnologia-mas-de-moda por última vez el 03/01/2022.

Pérez Medina, D. (2020, septiembre). Blockchain, criptomonedas y los fenómenos delictivos: entre el crimen y el desarrollo. *BOLETIN CRIMINOLOGICO*, *ARTÍCULO 10/2020_EJIC (N.º 206)* (EDICIÓN ESPECIAL. II Encuentro de Jóvenes Investigadores en Criminología.). Consultado en https://www.revistas.uma.es/index.php/boletincriminologico/article/view/11283/11690 por última vez el 03/11/2021.

Pina, C. (2022). *El Gobierno creará una Agencia Española de Supervisión de Inteligencia Artificial*. Garrigues. Recuperado 2022, de https://www.garrigues.com/es_ES/garrigues-digital/gobierno-creara-agencia-espanola-supervision-inteligencia-artificial

SEPBLAC. Prevención del blanqueo de capitales y de la financiación del terrorismo (normativa nacional). Consultado en https://www.sepblac.es/es/normativa/prevencion-del-blanqueo-de-capitales-y-de-la-financiacion-del-terrorismo/ por última vez el 29/10/2021.

Tondini, B. M. (2009). Blanqueo de capitales y lavado de dinero: Su concepto, historia y aspectos operativos. Centro Argentino de Estudios Internacionales.