Utilidad de
Blockchain y NFT
para autores

Antonio L. Flores Galea

Revista Digital de ACTA

2022

Publicación patrocinada por

ACTA representa en CEDRO los intereses de los autores científico-técnicos y académicos. Ser socio de ACTA es gratuito.

Solicite su adhesión en acta@acta.es

Utilidad de blockchain y NFT para autores

INTRODUCCIÓN

La palabra "blockchain" está de moda. Numerosas noticias aparecen vinculándola a otra palabra de moda: "criptomonedas". Aunque la tecnología de cadena de bloques (traducción del vocablo inglés "blockchain") está mayormente aplicada en la actualidad a las criptomonedas, también llamadas criptodivisas, sus aplicaciones potenciales van muchísimo más allá.

En este artículo no se va a tratar la aplicación de la tecnología blockchain para la creación y operación con criptomoneda, sino algo muy diferente: cómo probablemente afectará al trabajo de los autores de publicaciones de cualquier tipo, incluidas las escritas, en los próximos años. Para ello, se dará una visión inicial sobre en qué consiste y cómo funciona la tecnología blockchain, de manera fácilmente comprensible para cualquier persona ajena al entorno tecnológico, mostrando sus posibles usos futuros. Particularmente, se describirá el concepto de "contrato inteligente" (o "smart contract", en inglés), que hace uso de la tecnología blockchain para transformar de una manera radical la sociedad en la que vivimos actualmente (por si no hemos vivido ya suficientes transformaciones en la última década).

Antes de entrar en materia, es conveniente adelantar que, aunque una transformación tan profunda pueda sembrar incertidumbre, e incluso temor, en algunos autores, la tecnología blockchain supondrá un cambio muy positivo, especialmente para la defensa y preservación de los derechos de autor, así como para poner en valor la generación de contenidos, algo que ya comenzamos a oír de manera bastante distorsionada y errática en los medios de comunicación de masas con los denominados NFT (de "non-fungible tokens", en inglés, que se traduce literalmente como "testigos no fungibles" pero que el autor prefiere traducir mejor como "pruebas de unicidad"). Este concepto también se describirá en este artículo, siempre desde el punto de vista de la obra literaria científico-técnica y académica, y cómo estos NFT pueden afectar o resultar de utilidad para los autores.

QUÉ ES LA TECNOLOGÍA BLOCKCHAIN

Se puede afirmar que la tecnología blockchain es una tecnología digital (solo existe en el universo de los ceros y los unos) y que su aplicación principal es la de dar confianza a ciertas transacciones de información, de manera que varias personas – o máquinas – den por válida que esa información ha sido efectivamente transmitida.

Dicho de esta manera, se podría pensar que la tecnología blockchain tiene una utilidad bastante limitada y que, en el mundo real, tendrá poco impacto. Sin embargo, nada más lejos de la realidad. Hay que recordad que el ser humano es una especie animal que necesita vivir en sociedad y que, para ello, la transmisión de información es prácticamente igual de importante que alimentarse o respirar. Por otra parte, el mundo en el que vivimos está cada vez más digitalizado, basta darse cuenta de que gran parte de los trabajos actuales, incluso hasta el de repartidor a domicilio, consisten en estar toda la jornada laboral delante de un dispositivo digital, al igual que una gran proporción del ocio. Hasta ahora, parece que solamente el sueño y algunas horas esporádicas más del día han conseguido salvarse del fenómeno de la digitalización.

En este entorno digitalizado, que se dirige inefablemente a la adopción del Metaverso como herramienta fundamental para todos los quehaceres diarios (otra palabra de moda, frecuentemente adoptada por el mundo periodístico con más errores que aciertos en la actualidad). En este ecosistema, la tecnología blockchain se vuelve una cuestión fundamental: sin ella resultaría muy difícil continuar esta tendencia de digitalización mientras que, con ella, todo se vuelve mucho más "digitalizable", de manera segura.

DESDE UN PUNTO DE VISTA TÉCNICO

Para entender fácilmente en qué consiste la tecnología blockchain, primero es necesario introducir algunos conceptos previos, como son los protocolos, la criptografía asimétrica, los sistemas distribuidos, la firma o "hash", y los metadatos o metainformación. Como se ha mencionado anteriormente, se va a dar una definición básica, para que cualquier persona que no tenga conocimientos técnicos pueda entender el contenido del artículo:

- **Protocolos**: los protocolos de comunicaciones o de aplicación no son más que un conjunto de normas o reglas que le dicen a los sistemas informáticos cómo deben actuar. Hay protocolos de muy "bajo nivel" – término técnico -, que tienen normas, por ejemplo, del tipo "si recibes un mensaje de otro dispositivo, lo primero que viene en él es siempre su dirección IP" o "cada vez que recibas un mensaje de otro dispositivo envíale inmediatamente un mensaje con la palabra 'Ok' para que sepa que lo has recibido", mientras que hay otros de "alto nivel", como por ejemplo "cuando hayas recibido 1000 peticiones de usuarios guárdalas en el disco duro y envíale una copia al sistema X a las 10 de la noche". Se puede intuir que prácticamente todo el mundo digital funciona a base de protocolos y todos ellos tienen un nombre (por ejemplo, el protocolo para comunicarse por Internet se denomina "TCP/IP").
- **Sistemas distribuidos**: históricamente, la informática nació con grandes "ordenadores centrales", muy costosos tanto de fabricar como de operar. Posteriormente, conforme los microchips se fueron abaratando y a la vez volviéndose más potentes, nació la microinformática (el PC) y, en un determinado momento, alguien pensó que para hacer grandes cálculos o almacenar una gran cantidad de información, con tantos ordenadores distribuidos por el mundo, podría resultar atractivo que cada uno aportara un poco de su potencia de cálculo o capacidad de su disco duro para conseguirlo, sin necesidad de tener un superordenador o una súper-base de datos. Todo esto, claro, ocurrió cuando Internet estuvo lo suficientemente madura como para que todos estos dispositivos pudieran estar conectados con una *velocidad*[*] adecuada. Un sistema distribuido es, por lo tanto, una combinación de un conjunto elevado de ordenadores o dispositivos digitales, conectados mediante una red de comunicaciones, que utilizan un protocolo para realizar alguna tarea en equipo.
- **Criptografía asimétrica**: mientras el concepto de la criptografía resulta bastante sencillo de comprender (la criptografía es la ciencia que se dedica al estudio de códigos para ocultar y codificar mensajes para que solo el receptor adecuado pueda conocerlo), se podría decir que la criptografía asimétrica "tiene algo de magia". La criptografía tradicional que todos hemos utilizado desde el colegio es "simétrica". La simetría o asimetría de una técnica de codificación se refiere a si para descodificar un mensaje se utiliza el mecanismo inverso – simétrico – al que se utilizó para codificar el mensaje u otro distinto. Veamos la criptografía simétrica con un ejemplo muy sencillo:
    1. Antonio le dice a Bernardo: "vamos a utilizar el protocolo consistente en transformar las letras del mensaje en la N posición siguiente del alfabeto". Bernardo le contesta: "De acuerdo, *entiendo* ese protocolo". A continuación, Antonio dice: "voy a mover las letras 5 posiciones", o lo que es lo mismo, N=3 (esa es la clave secreta, cualquiera que la conozca puede descifrar el mensaje).
    2. Antonio le envía este mensaje a Bernardo: "WH FRPSUR WY FDVD".
    3. Bernardo, entonces, deberá aplicar el mecanismo *inverso* para descodificar el mensaje, es decir, restar 3 letras a cada letra, para descubrir que el mensaje es: "TE

[*] Se ha preferido utilizar el símil "velocidad" para combinar conceptos técnicos como los de ancho de banda y latencia, que no resultan esenciales para la compresión del artículo.

COMPRO TU CASA". Con la criptografía simétrica, Bernardo también podría enviarle mensajes a Antonio con la misma clave, por ejemplo: "GH DFXHUGR" y Antonio, restando 3 letras, leería: "DE ACUERDO".

La criptografía simétrica tiene una grave limitación: las dos partes tienen que ponerse de acuerdo antes sobre qué clave van a utilizar y esa información, obviamente, hay que enviarla sin codificar. Cualquiera que esté "escuchando", conocería la clave y, por lo tanto, la codificación no serviría de nada. La criptografía asimétrica, por su complejidad, no va a ser descrita en este artículo, pero sí su mecanismo de funcionamiento: en lugar de una clave compartida entre todos, cada uno utiliza dos claves, una pública y otra privada. Cada una de las partes – Antonio y Bernardo, en el ejemplo anterior – tiene una clave privada que solo ella conoce (y no necesita compartirla con nadie), la clave pública se la puede enviar a quien quiera, de hecho, la puede colgar en Internet. La magia funciona de la siguiente manera: todo lo que codifiques con la clave pública de alguien solo lo podrá descodificar ese alguien con su clave privada, y a la inversa, si quieres que alguien te envíe un mensaje cifrado, debes indicarle que lo codifique con tu clave pública y solo tú lo podrás descifrar con tu clave privada. Un símil en el mundo físico podría ser que distribuyes cajas fuertes abiertas a quienes quieres que te envíen un mensaje, pero la contraseña solo la conoces tú. Cuando esa persona mete el mensaje en tu caja fuerte (tu clave pública) solo tú la puedes abrir (con tu clave privada). En el mundo físico, enviar cajas fuertes a todo el mundo resulta bastante complicado, pero, en el mundo digital, solo se trata de un pequeño archivo.

El ejemplo más cercano que probablemente tengas de criptografía asimétrica es el certificado digital que utilizas, entre otras cosas, para firmar la declaración de la renta. En realidad, tienes dos certificados, uno es el tuyo (tu clave privada) y otro es el de la *entidad certificadora*, normalmente la Fábrica de La Moneda y Timbre (su clave pública). Codificas la declaración para que, cuando llegue a Hacienda, ella le pregunte a la FMT (que tiene tu clave pública) si efectivamente eres tú quien la ha enviado. Como vemos, al tener cada uno su clave privada única, **la criptografía asimétrica no solo sirve para transmitir mensajes en clave, sino también para dejar fuera de duda que un mensaje procede alguien en concreto**.

- **"Hash"**: el hash simplemente un algoritmo que extrae información de un documento o archivo para generar otro mucho más pequeño, casi único. Se utiliza para validar que un documento es auténtico. Aunque se utilizan algoritmos matemáticos muy complejos[†], una forma muy básica de entender cómo se obtiene la firma o "hash" de un documento es con el siguiente ejemplo:
  - Supongamos que queremos sacar el hash de una novela con un algoritmo consistente en extraer la primera letra de cada párrafo de la novela. Por ejemplo, el "hash" del Quijote empezaría así: "EECEEFPLSO…". Cuando lleguemos al final de la novela, tendremos un documento consistente en una lista bastante extensa de letras, pero mucho menos extensa que la novela en sí. Lógicamente, será imposible en la práctica que existan dos novelas con el mismo "hash" (a menos que alguien lo haga a posta, por eso se utilizan algoritmos matemáticos complejos para calcular el hash). Sin embargo, si alguien intenta venderte el Quijote, pero faltan algunos párrafos, el hash

[†] De hecho, los verdaderos algoritmos para el cálculo de hash deben considerar todos los caracteres del documento, de manera que no sea posible modificar ni una coma sin que el hash se convierta en otro distinto.

no coincidirá y, por lo tanto, tendrás un mecanismo muy rápido para argumentar que se trata de una copia errónea o falsa.

Como puedes adivinar, la técnica "hash" se utiliza para certificar que un documento es el original y no ha sido alterado. Puedes imaginar que esto, en cuestiones como transacciones bancarias, contratos, escrituras públicas, e incluso instrucciones de control de una central nuclear, es algo bastante importante.

- **Metadatos o metainformación**: a diferencia de los dos anteriores, este concepto es bastante sencillo. Los metadatos, también llamados metainformación, no son más que etiquetas que se añaden a la información que se desea almacenar o transmitir, para categorizarlas. Es lo que todos hacemos en las redes sociales cuando "etiquetamos", añadiendo un #. Los metadatos evitan que alguien necesite leer (o procesar, en el caso de sistemas) un documento para conocer de qué se trata, e incluso sirven para evitar errores de interpretación. Si etiqueto un documento con el metadato "Tipo de documento = Contrato" no quedará ninguna duda de que se trata de un contrato. Si posteriormente le añado otro metadato que indique "Fecha de firma = 14 de octubre de 2014" no hará falta leer nada en el documento para saber cuándo fue firmado. Esto es importante, especialmente, si el documento se encuentra codificado y no podemos acceder a su contenido, pero es importante cierta información para clasificarlo correctamente o avisar, por ejemplo, sobre su caducidad o si falta algo por hacer sobre él.

Conociendo los conceptos técnicos anteriores se puede decir que ya es posible estar al mismo nivel que un ingeniero para comprender la tecnología blockchain. Veámoslo a continuación.

La **tecnología blockchain** ("cadena de bloques", en inglés) es una estructura de datos que hace posible crear un registro digital de máxima confianza, que puede ser compartido en una red de entidades independientes. Es una tecnología distribuida, donde los algoritmos no corren en un ordenador central sino en los ordenadores o dispositivos móviles de quienes la utilizan o, cuanto menos, en una serie de nodos que son propiedad de distintas entidades que, voluntariamente o a cambio de alguna contraprestación, los ceden para correr esos algoritmos. Utiliza técnicas de criptografía asimétrica para generar los hashes de las transacciones o información que se almacenan en ese registro digital, para que quede constancia de quién ha solicitado la entrada en el registro y en qué momento. Una característica de la tecnología blockchain – de ahí su nombre – es que las entradas en el registro no se pueden ni modificar ni borrar. Con las entradas pasadas se van formando bloques de un número de entradas determinadas y las posteriores se van añadiendo como nuevos bloques sobre la "cadena de bloques" que ya existía. El "hash", como puedes adivinar, se calcula sobre el total de la cadena, haciendo imposible que nadie modifique ni el pasado ni el presente.

Esto, aunque pueda resultar extraño a priori, es esencial para que el sistema sea verdaderamente distribuido. Nadie puede borrar una entrada del registro, por más que sea la persona más rica y poderosa del planeta. Tecnológicamente no es viable.

¿POR QUÉ ES TAN IMPORTANTE QUE LA TECNOLOGÍA BLOCKCHAIN SEA DISTRIBUIDA?

La tecnología blockchain va a suponer, muy probablemente, un gran salto para la humanidad. Es muy probable que resulte tan importante para nuestro futuro como lo fue la invención del fuego, la electricidad o Internet, en el pasado. ¿Por qué? Veamos cómo han funcionado las redes de confianza del ser humano hasta ahora para comprender mejor qué nos espera en los próximos años.

Comencemos con una cuestión bastante importante, aunque probablemente no la más importante: los registros públicos. Es probable que tengas un título universitario. Ese título tiene un código que permite verificar que es verdadero, acudiendo al Registro Nacional de Títulos Universitarios, actualmente disponible de forma online, por ejemplo:

https://sede.educacion.gob.es/sede/login/inicio.jjsp?idConvocatoria=103

Tú confías en que el Estado mantendrá ese registro de manera correcta y sin errores… Acuérdate que, igual que tú, todos los universitarios en 1939 pensaron lo mismo en España pero, de la noche a la mañana, muchos de ellos vieron cómo sus títulos universitarios eran anulados y eliminados de tal registro por el nuevo régimen de la dictadura de Franco. Todos los estados mantienen registros *centralizados* donde, además, todas las garantías sobre la información que allí se encuentra depende directamente de una *autoridad*. Dos puntos débiles evidentes en esta relación de confianza que el ciudadano humildemente (por no decir forzosamente) deposita en el sistema.

Veamos otro ejemplo también cercano: las escrituras de tu casa. Firmaste ante notario que comprabas tu vivienda y te dieron un documento con la firma del notario, pegatinas, sellos, códigos, etc. Todo esto quedó depositado en el registro de la propiedad de tu provincia que, desde hace tiempo, digitaliza toda la información para garantizar que un incendio o inundación no destruye la información. Sin embargo, volvemos a tener un sistema *centralizado* (solo una entidad controla tus escrituras) y dependiente exclusivamente de una *autoridad* (el propio registro de la propiedad). ¿Quién asegura que alguien no podría cambiar en el registro la titularidad de tu casa y, de la noche a la mañana, pase a ser propiedad de otro? Y no me refiero a un soborno sino, nuevamente, a la humilde o forzosa confianza que depositamos en él. Puedes leer sobre las numerosas "desamortizaciones" que han sido dictadas por los gobiernos en el pasado, si quieres profundizar un poco más en este asunto.

Pero vayamos al asunto principal, el ejemplo crítico que ha disparado el éxito del blockchain: el dinero. En la cumbre de Bretton Woods, una pequeña localidad del boscoso y frío estado de Vermont en Estados Unidos, en 1944, se acordó un tipo de cambio fijo entre el dólar americano y el oro (35 dólares servirían para comprar 1 onza de oro). Con esto, automáticamente todos los países podían medir su capacidad para "comprar" dólares según la cantidad de oro de sus reservas nacionales. Este acuerdo, firmado por todos los países de occidentes (los miembros del FMI), funcionó bien hasta que, en 1971, Francia decidió cambiar una ingente cantidad de su oro por dólares. Esto "cabreó" (por cuestiones geopolíticas que no vamos a detallar aquí) a Nixon, presidente de EE. UU., que decidió, unilateralmente, romper los acuerdos de Bretton Woods y comenzar a fabricar más dólares que oro había en su Reserva Federal. A partir de ese instante, dado que todas las divisas estaban referenciadas al dólar, se perdió el patrón oro y esto nos llevó al momento actual, donde la humanidad vive – literalmente – con el esfuerzo y trabajo que harán nuestros bisnietos.

Seguramente la pregunta aquí es ¿y qué tiene que ver todo esto con el blockchain? Muy sencillo: el dinero es una fórmula de intercambio de valor entre dos partes. Si quiero la barra de pan que has horneado, pero yo me dedico a hacer zapatos y tú ya tienes los tuyos y no quieres más, te doy un trocito de oro o de plata, que seguro que hay más gente que lo quiere después (por lo escaso y valioso que es) y cuestión resuelta. Esto, siglos más tarde, ha evolucionado a que los estados acuñaban monedas con unos pesos concretos para hacer más fáciles las transacciones y, posteriormente, a convertir esto en trozos de papel certificados por el estado, afirmando "este trocito de papel vale por X gramos de oro que yo guardo en mi cámara acorazada de la reserva nacional". Todo este pragmatismo, de repente, sufrió de un abuso de autoridad y confianza, en 1971, cuando el presidente de los EE. UU. vino a decir "este trocito de papel vale lo que vale porque todo el mundo sabe lo que vale y porque EE. UU. es el estado más respetable y confiable del mundo. Tened fe en nosotros". Y este es el origen del dinero "fiduciario", con el que todos los humanos del planeta

humildemente (o forzosamente) convivimos. Todos tenemos fe ciega en que el dólar vale "lo que vale" … hasta que deje de valerlo.

Y, por fin, entra en escena la tecnología blockchain, con el bitcoin a la cabeza. Aunque, como se ha mencionado, en este artículo no se van a tratar las criptomonedas, es conveniente mencionar el bitcoin, como ejemplo, por ser la más famosa, aunque hay cientos o miles de criptomonedas más. El bitcoin nació porque alguien – no se conoce quién – presentó un algoritmo de blockchain para registrar transacciones económicas con una moneda inventada – el bitcoin. Aunque pueda parecer una locura, la realidad es que el bitcoin no tiene más ni menos confiabilidad que el dólar americano: vale "lo que vale". De hecho, su creador indicó al principio que el primer bitcoin valía un dólar. ¿Por qué? Porque quiso. Sin más. A partir de ahí, dado que la tecnología blockchain que controla el algoritmo es descentralizada (nadie puede borrar ni crear bitcoins a su antojo, el registro se encuentra distribuido por todo el mundo, en países de todos los colores, climas y sistemas políticos) y que no existe una autoridad que pueda intervenir en esos registros, mucha gente, sobre todo aquellos con más poder adquisitivo que buscaban fórmulas alternativas para diversificar su riqueza, comenzaron a comprar bitcoins (que son generados mediante unos algoritmos matemáticos que hacen cada vez más difícil crear nuevos bitcoins y esto solo es posible con el avance de los sistemas informáticos). Esto hizo que incrementara su valor, hasta los aproximadamente 40.000 dólares que cuesta un bitcoin actualmente. ¿Te parece una locura? Pues imagínate si a Newton le dijeran que un kilo de plutonio –material que se encuentra en la naturaleza pero que él ni conocía– se iba a vender a 4 millones de euros en la actualidad.

Volviendo al asunto del dinero, analicemos el sistema financiero actual: el propio dinero no tiene valor intrínseco alguno (vale "lo que vale"), casi ni existe como ente físico (la mayor parte del dinero son dígitos en las bases de datos de una empresa privada denominada banco), está sujeto no a una autoridad sino a varias (el estado, el banco, el FMI, el BCE, la Reserva Federal…).

USOS PRÁCTICOS DE LA TECNOLOGÍA BLOCKCHAIN

Hemos visto que el uso inmediato que se está dando a la tecnología blockchain es la del dinero digital o criptomoneda. Aunque es la más evidente, dada la gran debilidad del sistema de confianza del sistema financiero actual, no es la única y, probablemente, el uso de criptomonedas no va a transformar la sociedad en absoluto. A fin de cuentas, con el uso de tarjetas de crédito y otros mecanismos de pago digital, el dinero ya es digital, aunque todo esté montado sobre un sistema muy poco confiable.

McKinsey & Co. hace una clasificación de las aplicaciones de la tecnología blockchain en seis categorías:

1. **Registros estáticos**: aportando independencia y permanencia a los datos de registros oficiales, como son los registros de la propiedad, de la propiedad intelectual, mercantil, de patentes, de medicamentos, etc.
2. **Sistemas de identidad**: no solo evitando la falsificación de DNIs, pasaportes, registros civiles, sistemas de prestaciones sociales, censo electoral, etc. sino también permitiendo nuevas aplicaciones basadas en la identidad digital, como el voto electrónico, por ejemplo.
3. **Smart contracts, o contratos inteligentes**: serán tratados en la siguiente sección, aunque ya es posible deducir de su nombre que se trata de contratos que aplican ciertas reglas o condiciones automáticamente.
4. **Registros dinámicos**: permitiendo la existencia de registros globales para cuestiones que actualmente son imposibles, como medir al detalle las importaciones y exportaciones de un país, garantizar la trazabilidad de los alimentos (a qué temperatura han estado en todo momento, por qué manos han pasado, etc.), registrar las transacciones financieras, e

incluso asignar usos concretos del dinero y fecha de caducidad del mismo (por ejemplo, impedir que con una prestación social se puedan comprar artículos de lujo o dar una prestación social durante un período de desempleo y que, en el momento de encontrar un empleo, "caduque" todo el dinero no gastado de la prestación recibida en los meses pasados).

5. **Infraestructuras de pagos**: plataformas de intercambio de dinero entre particulares, sin intervención de un banco o una autoridad monetaria de ningún país.
6. **Otros usos**: este es un cajón de sastre donde irán apareciendo nuevas aplicaciones conforme la tecnología vaya ganando madurez y haya más personas o empresas aportando su imaginación para crear nuevas aplicaciones y usos para la tecnología blockchain.

Como puede apreciarse, las transformaciones más disruptivas vendrán con total probabilidad de las categorías 3 y 4 (smart contracts y registros dinámicos). Mientras el punto 5 (infraestructuras de pagos) ya está en marcha con el uso de criptomonedas, los primeros dos puntos (registros estáticos y sistemas de identidad) afectarán sobre todo a nuestra relación como ciudadanos con el Estado, mediante innovaciones incrementales, pero no transformando radicalmente nuestras vidas. El hecho de que el punto 3 se encuentre entre las cuestiones más disruptivas asociadas con la tecnología blockchain es el motivo por el que los autores literarios y de contenidos multimedia deben prestar especialmente a la cuestión de los contratos inteligentes, o smart contracts.

QUÉ SON LOS "SMART CONTRACTS"

Un "smart contract" (o "contrato inteligente", en español) es un contrato que tiene asociada, intrínseca e inseparable, una pequeña aplicación informática que hace uso de la tecnología blockchain para cumplir **tres funciones**:

1. dar fe y dejar constancia sin lugar a duda de la existencia y los términos del contrato,
2. verificar en tiempo real el cumplimiento o no de las distintas cláusulas del contrato, y
3. poner en marcha las acciones oportunas, recogidas en el contrato, tanto si se cumple o se incumple una cláusula.

Como vemos, el smart contract podría definirse como un contrato "automático" entre las partes, en el sentido de que no es necesario que ninguna de ellas, ni ningún actor externo, necesita estar pendiente de su cumplimiento o incumplimiento para que sean tomadas determinadas acciones. Las **implicaciones directas** de los smart contracts son enormes:

- No se necesita de un tercero – notario, árbitro, etc. – que de fe del contrato. El contrato se mantiene como si se tratara de un contrato privado pero, al estar protegido por la red blockchain, podrá ser utilizado como prueba fehaciente si llegara a ser necesario aunque esto, como se verá a continuación, tampoco será necesario.
- Las cláusulas son respetadas siempre, tanto si se cumple lo que estipulan como si no, pues la aplicación informática se encarga irremediablemente de que así sea, sin que nada ni nadie pueda impedirlo, ya que la programación se encuentra recogida en la blockchain oportuna, distribuida por el mundo.
- Cualquier indemnización, compensación o reclamación sobre el contrato, además de ser lanzada automáticamente, podrá ser inmediata (o no, según los términos que establezca el contrato).
- Con los smart contracts, se vuelve fundamental el respeto de la Ley, pues es imposible bloquear la ejecución de las acciones automáticas una vez firmado el contrato, incluso aunque la Ley disponga cuestiones en contra de las cláusulas del acuerdo. Solo se podrá reclamar una cuestión no legal a posteriori, una vez lanzadas estas acciones.

Aunque los smart contracts pueden ser utilizados para cualquier cosa, y en el futuro realizaremos seguramente hasta las compraventas inmobiliarias y las expediciones de títulos académicos por este medio, los primeros pasos en smart contracts se están dando en contratos con alcances más reducidos como es, por ejemplo, la entrega de mercancías.

Si alguna vez has comprado por Internet, habrás visto que primero debes pagar la mercancía y después esta llega a tu domicilio. De nuevo, es necesario hacer un acto de fe en que todo saldrá como se espera, pero la cadena podría fallar en cualquier momento, intencionada o inintencionadamente (la tienda online podría ser una estafa que no envía los productos, el producto podría estar agotado y la empresa dejarte esperando sin avisarte, el operador logístico podría perder o dar un golpe a la mercancía y que llegue rota, podrían dejársela a un vecino cuando no estás y que este no te diga nada, etc.).

Con un smart contract, toda la cadena de valor se vuelve de confianza: en lugar de pagar por la mercancía, firmas un acuerdo en el que, cuando esta llegue a tus manos, se realizará un pago desde tu tarjeta al vendedor. Esto será verificado porque el propio paquete llevará incorporado una etiqueta RFID (la misma que lleva la ropa en las tiendas y que hace que suene la alarma cuando sales de la tienda con una prenda sin pagar). El operador logístico leerá esa etiqueta al recoger la mercancía y tú la leerás también con tu móvil cuando te la entregue el mensajero, al que le aparecerá el paquete como no entregado hasta que tú no lo hagas. Posiblemente, la caja incorporará también un sensor de impacto para que, al hacer la entrega, se transmita instantáneamente si el paquete ha sufrido un golpe de gran impacto e, instantáneamente, el terminal del mensajero no permitirá la entrega, te llegará un aviso a ti y al vendedor y, automáticamente, el operador logístico compensará al vendedor según los términos acordados.

Todo esto, que parece bastante complejo y casi de ciencia ficción, se puede asimilar mucho más fácilmente si te metes en la página de AliExpress, por ejemplo, y ves lectores de RFID y sensores de impacto por pocos céntimos de euro. La tecnología ya está disponible; solo es cuestión de tiempo que se vaya extendiendo a todos los ámbitos.

BENEFICIOS DE LOS SMART CONTRACTS

En la Fig. 1 se resumen los beneficios que aportan los smart contracts:

- **Seguridad**: todos los términos del contrato son recogidos en un sistema blockchain que hace que siempre se encuentre disponible y distribuido por toda la red. Es imposible que el contrato "se pierda".
- **Siempre son precisos**: al estar codificados sus términos mediante un pequeño software (denominado "script", o guion, en inglés), las condiciones que permiten determinar si se cumple o no cada cláusula siempre deben ser absolutamente precisas o, de otra manera, no serían trasladables a lenguaje informático).
- **Se ejecutan muy rápidamente**: como cualquier servicio digital, los smart contracts se ejecutan en sistemas informáticos de manera casi instantánea. No es necesario realizar ningún trámite manual adicional ni estar pendiente para ver si se cumple o no una condición.
- **Son eficientes en coste**: al eliminar actores (principalmente terceros, como notarios e incluso el sistema judicial, a priori), son la solución más económica para obtener garantías en acuerdos, sobre todo entre partes distantes o desconocidas donde, frecuentemente, el sistema judicial suele fallar o ser extraordinariamente caro.
- **Aportan confianza total**: al encontrarse todos los términos y acciones recogidos en un sistema blockchain, ninguna de las partes necesita tener fe en ninguna cuestión. Una vez firmado, el contrato se ejecutará irremediablemente, con la única excepción de que Internet desapareciera de la faz de la Tierra.

Fig. 1. Beneficios de los smart contracts (fuente: 101blockchain.com)

- **Están libres de interrupciones**: como se ha mencionado, nada puede detener la ejecución de un smart contract hasta el final. Ni las partes ni fenómenos externos pueden interrumpir su ejecución.
- **Son autónomos**: una vez firmados, funcionarán como entes independientes de las partes. Incluso aunque una de las partes desapareciera, el contrato continuará su ejecución.

CÓMO FUNCIONA UN SMART CONTRACT

En la Fig. 2 se muestran los pasos para realizar un smart contract en una operación de compra-venta, ya sea de un bien o de un servicio. Como puede comprobarse, el smart contract sustituye completamente al contrato escrito tradicional. A la izquierda de la figura aparecen el vendedor ("*seller*"), el comprador ("*buyer*") y el activo que se quiere transmitir entre ambos ("*asset*").

Una de las diferencias entre el smart contract y el contrato tradicional es que estos tres elementos tienen un papel activo en el contrato mientras que, en el contrato tradicional, el activo tiene un rol meramente pasivo. Esto es así porque, atendiendo al cumplimiento o no de las distintas cláusulas particulares del contrato ("*term & conditions*"), el activo actuará de una determinada manera u otra. Así, el smart contract se autoejecuta, es decir, el algoritmo que implementa verificará en todo momento el cumplimiento de las cláusulas e "informará" al activo sobre cómo proceder. En el caso más sencillo, si se confirma el pago de una mercancía, se dará automáticamente la orden de entrega. En otros casos más complejos podrían establecerse, por ejemplo, penalizaciones o incluso generar un aviso formal a un tercero para denunciar una irregularidad o, incluso, una demanda.

Hemos visto el funcionamiento *teórico* del smart contract, que resulta bastante sencillo. Sin embargo, su implementación práctica conlleva bastante más complejidad. En particular, existen dos retos fundamentales a resolver:

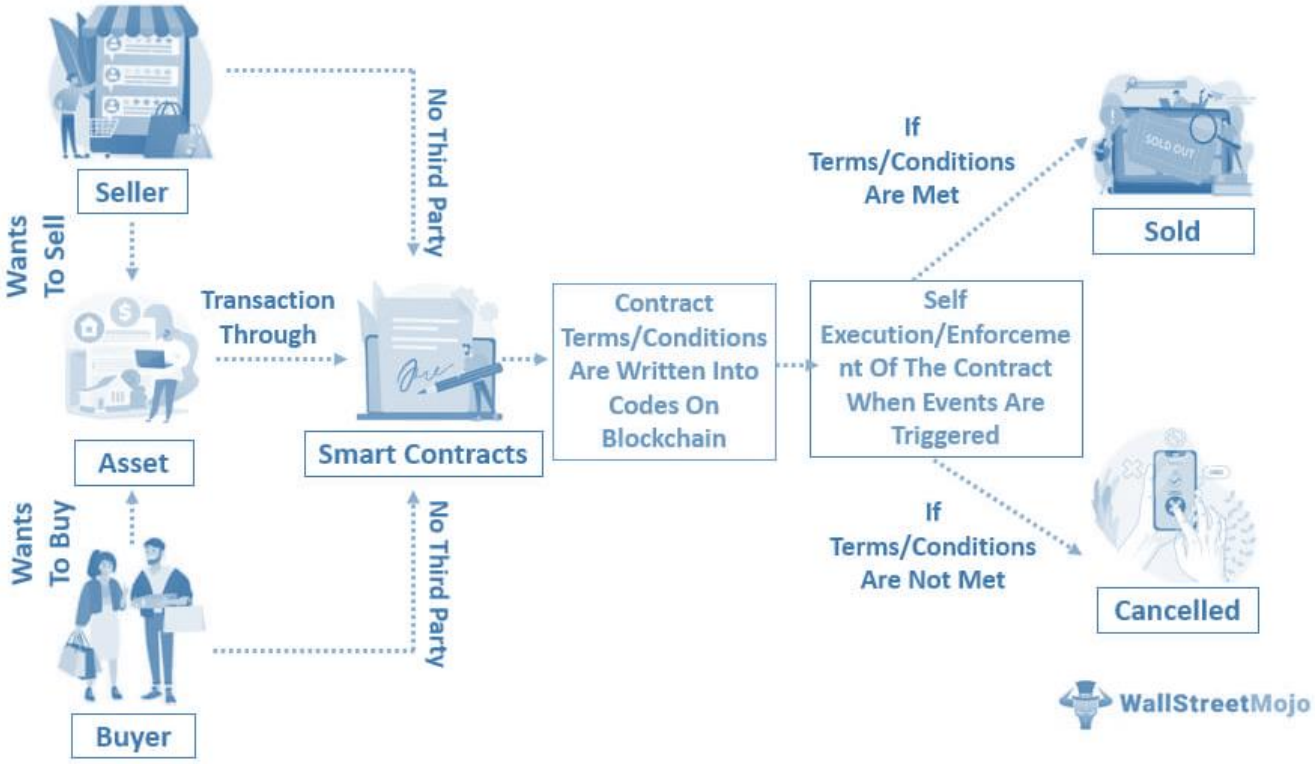

Fig. 2. Pasos para formalizar y ejecutar un smart contract en una transacción comercial

- Es sumamente importante que las cláusulas del contrato se encuentren correctamente programadas en el smart contract, para que no existan errores en su interpretación y ejecución. Aunque numerosas encuestas realizadas a todo tipo de perfiles de personas demuestran siempre mayor confianza en las máquinas que en las propias personas, también es cierto que la tecnología falla cada día más, principalmente debido al progresivo incremento de la complejidad de los sistemas, que hace imposible controlar lo que se denomina técnicamente "estados de error" (coloquialmente, dónde podría acabar un algoritmo si alguna de las variables implicadas no tiene un valor considerado "normal"). Por tanto, es muy importante que los algoritmos que implementan smart contracts tengan la robustez, probablemente asociada a su sencillez, suficiente.
- Para que un smart contract pueda tomar decisiones automáticas sobre el cumplimiento o no de las cláusulas que contiene es necesario que tenga acceso a la información sobre cuestiones relevantes en torno a ellas. Se podría decir que necesita "ojos" para "ver" qué ocurre en el entorno y, así, determinar las acciones siguientes. Dado que un smart contract es un algoritmo – digital por naturaleza –, es necesario que toda esa información llegue de forma digital al sistema que contiene el algoritmo. Esto se traduce en la necesidad de ubicar sensores digitales capaces de medir en todo momento los valores de una determinada variable. En el caso de un transporte de alimentos frescos o congelados, por ejemplo, puede resultar fundamental en el contrato preservar la cadena de frío, por lo que será necesario un sensor digital de temperatura. En otros casos, por ejemplo en una transacción con distintas divisas involucradas, será necesario un conector con los sistemas de información de los tipos de cambio. En los más complejos, por ejemplo un smart contract para contratar a un "paseador de perros" (tan famosos en la ciudad de Nueva York), sería conveniente que el perro tenga un collar con GPS. Y, sin pensar en cuestiones tan estrambóticas, un smart contract para auxilio en carretera debería contar con un conjunto bastante numeroso de sensores en un vehículo para llamar automáticamente a los servicios de emergencia e informar de si los pasajeros están conscientes o no, qué tipo y fuerza de impacto ha sufrido el vehículo, si hay riesgo de incendio por escape de combustibles, si el vehículo ha quedado

dentro o fuera de la calzada, si está del revés, etc. Con este ejemplo aprovechamos para recordad que la gran ventaja de un smart contract frente a simplemente utilizar un sistema privado sin protección probada y aceptada generalmente frente a fraude es que, con el smart contract implementado en vehículos, estos podrían automáticamente "avisar" a la señalización activa de las carreteras, a los servicios de emergencias y al resto de vehículos para tomar acciones concretas (bloquear un carril o un tramo completo de la carretera, cambiar los límites de velocidad, etc.).

En conclusión, aunque la red Ethereum está avanzando cada día como la primera en ofrecer tecnología Blockchain para implantar smart contracts y la enorme proliferación de sensores digitales a un coste muy reducido, como consecuencia del auge de estos en la industria de los teléfonos móviles, es ya una realidad, es posible que vayamos viendo cada vez una mayor adopción de smart contracts en distintos sectores, aunque todavía quedan algunos años para que sea una tecnología generalizada.

CINCO EJEMPLOS DE EMPRESAS QUE YA HAN IMPLANTADO SMART CONTRACTS

Aquí se muestran algunos ejemplos de smart contracts que ya están utilizando algunas empresas para distintos usos:

Slock.It y Share & Charge

Slock.it es una empresa que nació proporcionando cerraduras inteligentes ("smart locks") que utilizan smart contracts basados en Ethereum para los alquileres de viviendas. Así, la cerradura responderá a las peticiones para abrir y cerrar del inquilino solo durante su período de estancia y al dueño del inmueble durante el resto del tiempo. Como nueva aplicación de su tecnología a nuevas aplicaciones, en 2015 comenzó a aplicar sus smart contracts al mundo de la Internet de las Cosas (IoT) y a la movilidad. En concreto, una colaboración con la empresa Share & Charge ha permitido que, con la ayuda de esta nueva tecnología, el proceso de pago del alquiler de las estaciones de carga de vehículos eléctricos esté automatizado.

Fizzy AXA

La multinacional francesa de seguros AXA comenzó a utilizar smart contracts para automatizar las indemnizaciones por retrasos en los vuelos. En realidad, la idea era bastante simple. Recibir una indemnización por un vuelo retrasado es difícil y, lo más importante, a veces el seguro que se tiene contratado no la contempla, pues depende de la causa del retraso, entre otros factores. Con la ayuda de la app Fizzy, se podía obtener una compensación si el vuelo llega con un retraso de más de dos horas y se ha cargado previamente la información de la aerolínea en la app. Una notificación nos informaba de las opciones para ser indemnizado y, después de haber elegido una, el dinero iba directo a nuestra cuenta bancaria. En este caso, el uso de los smart contracts eliminaba cualquier reclamación relacionada con la aerolínea y compensaba por las pérdidas, incluso fuera de la cobertura del seguro. El seguro funcionaba simplemente con un desencadenante y, para Fizzy, el desencadenante era el retraso de más de dos horas en un vuelo. En la actualidad, este servicio ha sido retirado por la compañía, después de tres años de pruebas, aunque la aprovecharán para continuar desarrollando servicios basados en smart contracts.

Propy

Uno de los casos de uso más comunes de los smart contracts es automatizar el negocio inmobiliario. Para hacer esto realidad, la compañía Propy comenzó a integrarlos en su sistema hace ya unos años. La primera transacción en su plataforma basada en smart contracts tuvo lugar en

septiembre de 2017, cuando una persona compró un apartamento por 60.000 dólares en Ucrania. Este tipo de acuerdos transfronterizos puede desvelar el verdadero potencial de los smart contracts en el sector inmobiliario. Así, un usuario puede buscar propiedades en otros países del mundo y lanzar ofertas. Después de pasar por ciertos procedimientos de comprobación, se incorporarán medidas de seguridad y confianza en el smart contract para garantizar que no se produce fraude. Un comprador potencial puede reservar una propiedad dando una entrada y, después, pagar el resto, una vez realizados todos los trámites necesarios. Si, por alguna razón, el vendedor no quisiera vender la propiedad en el último momento, al comprador se le devolvería el dinero.

PolySwarm

PolySwarm es una compañía que opera en el entorno de la ciberseguridad. En este mundo, es una práctica bastante frecuente que determinadas organizaciones (públicas o privadas) lancen retos relacionados con potenciales ciberataques para que los profesionales encuentren la forma de atacar los objetivos y, por ende, la mejor forma de protegerlos (algo similar al sparring en boxeo). Gracias al uso de tecnología Blockchain para implementar smart contracts entre los profesionales de la ciberseguridad y las organizaciones que buscan detectar y solventar vulnerabilidades de sus sistemas, cualquier empresa o representante puede publicar su reto en la plataforma PolySwarm, junto con la recompensa asociada. El profesional que lo hace correctamente es recompensado con la criptomoneda creada por la propia plataforma, llamada Néctar. Después de evaluar que sus acciones y resultados son correctos, los fondos se liberan automáticamente a su cuenta.

Populous

La financiación de facturas ("factoring") es una forma que las empresas tienen para conseguir flujo de caja. El *factor* (persona o empresa intermediaria), a cambio de una comisión, pagará a la empresa el importe total de una factura que tiene vencimiento diferido (por ejemplo, pago a 30 o 60 días) de manera inmediata y se hará cargo de cobrar la factura cuando llegue el momento. La iniciativa Populous (PPT) es una plataforma digital en la que cualquier persona puede actuar como factor por un importe concreto (por ejemplo, hasta 5.000 €). La plataforma utiliza entonces smart contracts para combinar todas las cantidades de los factores en un solo montante y ofrecerse como factor único a grandes empresas (por ejemplo, para adelantar una factura por importe de 300.000 €). El uso de smart contracts permite que todo el proceso de pagos, reclamaciones de facturas y liquidaciones a los factores individuales se realice de manera automatizada. No hay error humano posible (duplicaciones de facturas, errores de cálculo, etc.). Con la ayuda de Populous, después de que cada empresa cargue sus facturas en la plataforma y defina los términos específicos en los que está dispuesta a recibir el dinero (comisión máxima, tiempo, divisas, etc.), las transacciones se realizan automáticamente, con la ayuda de los smart contracts.

UTILIDAD DE LOS SMART CONTRACTS PARA AUTORES

Los smart contracts pueden transformar el sector editorial profundamente durante los próximos años, principalmente en tres líneas:

- La correcta atribución de la autoría de los contenidos encontrados en Internet, habitualmente copiados y transcritos masivamente en la actualidad, trasgrediendo los derechos de autor, en ocasiones sin que el propio autor tenga constancia de ello.
- La posibilidad de que los autores creen contenidos dinámicos, facilitando una trazabilidad y actualización instantánea de los contenidos en todos los medios donde estos se encuentren publicados.
- Aprovechar los NFTs, que veremos en la siguiente sección, como una fórmula para producir contenidos únicos y no replicables, incrementando así su valor.

Entremos un poco más en detalle en cada una de las cuestiones anteriores:

Atribución de derechos de autor

Aunque, sobre el papel, los derechos de autor se encuentran perfectamente regulados en el derecho nacional e internacional, lo que sucede en la realidad es bastante diferente. Al igual que lo que sucede en otras muchas disciplinas, la sociedad global está evolucionando lenta pero inexorablemente hacia un modelo neo-feudal, en el que un grupo finito de grandes corporaciones multinacionales comienzan a tener más poder que los estados. Esto no solamente ocurre a nivel formal, en cuanto a que algunas leyes deben tener en cuenta las premisas de ciertos gigantes para permitirles operar en el país so pena de quedar relegados a un segundo plano tecnológico y económico respecto de sus vecinos, sino también a nivel social, donde se instauran concepciones como que las redes sociales son empresas privadas y, por lo tanto, tienen todo el derecho a imponer las normas de censura que deseen. Muy lejos quedan ya las ideas que defendían, por ejemplo, el derecho universal a la telefonía o a la electricidad, que obligaban a empresas privadas a prestar servicios públicos con una serie de normas que garantizaban derechos de los ciudadanos.

En este contexto, donde desaparecen progresivamente las herramientas para garantizar que se cumple la ley, los smart contracts se vuelven imprescindibles. Esto es posible comprobarlo simplemente observando determinadas circunstancias que ocurren frecuentemente en la actualidad: ¿quién no ha tenido problemas para reclamar sus derechos de autor con el gigante Amazon, con libros descatalogados, en distintas versiones, ámbitos geográficos, etc.? ¿Quién no ha visto sus contenidos copiados al pie de la letra en blogs, sin que nadie pueda hacer absolutamente nada? ¿Quién no ha visto sus publicaciones pirateadas en menos de 24 horas, especialmente ebooks y material publicado en formato digital? El derecho te asiste, sí, pero seamos sinceros: para los pocos euros que vas a obtener por esos derechos de autor (cuando es el caso y no se trata simplemente de derechos morales por haber contribuido sin remuneración), ¿quién cursa una demanda judicial?

Los smart contracts pueden vincular la publicación de ciertos contenidos a ciertos medios, por ejemplo, de tal manera que si el documento no es expuesto en la URL correcta, directamente será borrado. También pueden asociar irremediablemente el nombre y condiciones de cesión de derechos del autor, para que cualquiera pueda ver si es contenido legal o ilícitamente distribuido. También, un documento protegido por un smart contract podría generar una cadena de registros de todas las transacciones (copias) que se hacen de él en una blockchain, que el autor podría consultar para verificar si hay alguna copia ilegítima. Y, por último, los autores y editoriales tendrían en tiempo real las ventas de ejemplares de cualquier editorial o distribuidor, respectivamente, de cara a recibir una justificación exacta de la liquidación de derechos que, por este motivo, podría realizarse mensual, semanal o, incluso, individualmente por ejemplar, frente a la tradicional liquidación anual.

Publicaciones dinámicas

Hace unos años estábamos acostumbrados a que los contenidos fueran estáticos (un libro, un artículo, un informe) y que se sucedieran distintas *ediciones*, cuando se hacía necesario modificar o actualizar parte de este contenido. Con la llegada de Internet esto ha ido cambiando progresivamente, pues mucho material de calidad, útil para consulta y referencia, se encuentra publicado en páginas web que, por su propia naturaleza, pueden ser actualizadas al instante, sin que nadie sea consciente de ello a priori, excepto quien realiza los cambios. Este hecho representa un problema pues, tanto el propio autor de los contenidos como lectores que hayan consultado o referenciado esos contenidos publicados en una web, pueden no ser conscientes de que, con posterioridad, alguien los ha modificado, incluso inconscientemente (piensa en páginas que, al ser migradas de servidor, pierden las imágenes, por ejemplo). Otras veces, el propio autor desea actualizar los

contenidos, sin que exista una forma generalmente aceptada de indicar que se trata de nuevas "ediciones" del contenido. Por supuesto, además ocurre que nadie que haya referenciado ese contenido será consciente de que referenció un contenido anterior y no el actualmente disponible en esa web.

Mediante el uso de smart contracts, un autor podría tener trazabilidad instantánea de qué ocurre con sus contenidos publicados en páginas webs, sobre todo en el caso de que se produzcan cambios. Además, los smart contracts permitirían determinar una serie de acciones, penalizaciones o condiciones si tal caso se produjera. Para quienes referencien esa web, un servicio que haga uso de la tecnología Blockchain para monitorizarla sería útil para avisar de que se ha producido una nueva edición del contenido y el smart contract actualizaría automáticamente la referencia en el documento, sin que el segundo autor tenga que hacer nada.

Una vuelta adicional de tuerca se podría dar utilizando los propios smart contracts para la generación automática de determinados contenidos en un documento. Un autor podría incluir o eliminar determinados párrafos de un documento digital según se den determinadas condiciones. Por ejemplo, un autor que quisiera ilustrar el comportamiento de un sistema de colas saturado podría incluir un ejemplo sobre las caravanas en carreteras de playas en verano, durante ese período del año, y otro de colas en los primeros fines de semana del mes en los supermercados, durante el resto del año. Sería un libro "dinámico", con un smart contract que cambiaría el contenido del propio libro según las cláusulas establecidas por el propio autor. Aunque el ejemplo es un poco inútil, da una idea de qué tipo de opciones abren los smart contracts (imaginemos el potencial para los libros de texto, donde parte de su contenido se incluye o se omite cada año según los designios políticos sobre lo que está de moda o no enseñar, entre otros factores).

Publicaciones digitales únicas

Aunque la derivada más interesante del uso de smart contracts para publicaciones únicas son los denominados NFTs, que veremos en la siguiente sección, es interesante destacar que el uso de smart contracts permite, como se puede deducir de lo visto hasta ahora, mantener el control exhaustivo de cualquier contenido digital. Esto se hace gracias a la tecnología "hash" que ya se ha visto, para detectar copias modificadas de cualquier archivo y a la propia red blockchain distribuida, que deja constancia de todas las transacciones (envíos o descargas de archivos) a cualquier persona que la consulte.

CUESTIONES IMPORTANTES SOBRE LOS SMART CONTRACTS

Para concluir esta sección, se detallan las tres cuestiones probablemente más relevantes a tener en cuenta en el uso de smart contracts:

- **Definir muy bien los términos**: dado que las cláusulas del contrato son vigiladas en tiempo real por la red blockchain elegida para implantarlo y que se ejecutan acciones automáticas, sin intervención humana, en virtud de ellas, es fundamental que todos los términos se encuentren perfectamente recogidos en las cláusulas del contrato. Por su propia construcción, los smart contracts no permiten dejar vacíos o inconsistencias en sus términos, funcionan de manera puramente lógica, con cláusulas del tipo "Si… entonces…". Es necesario, por tanto, definir los smart contracts como habitualmente se definen los algoritmos (quizás veamos, en breve, "abogados informáticos" o despachos de abogados con un equipo significativo de informáticos.
- **Respetar la Ley**: el smart contract no "conoce" la Ley, a priori. Todos sabemos que las leyes tienen primacía sobre los contratos, pero esta cuestión normalmente es dirimida por un juez o árbitro. Aunque un smart contract podría ser reclamado por vía judicial, su objetivo

es justamente evitar esta cuestión al realizar un acuerdo entre las partes, con confianza plena. Por este motivo, mientras la propia legislación de un país no se encuentre regulada mediante reglas "entendibles" por los smart contracts, es posible que algún contrato vulnere la realidad. No es algo distinto a lo que ocurre en la actualidad con los contratos regulares, pero hay que recordar que el smart contract ejecuta automáticamente penalizaciones y consecuencias de su incumplimiento. Por lo tanto, cuando haya que reclamar una cuestión contraria al ordenamiento jurídico firmada en un smart contract, es bastante probable que haya que reclamar también las penalizaciones que puedan haber sido ejecutadas. Veámoslo con un ejemplo: en un smart contract para un alquiler de una vivienda, se firma una cláusula que establece que, si el inquilino no paga su renta mensual dentro de los primeros cinco días del mes en curso, se desactivará el suministro de gas de la vivienda. Si la Ley establece que no se puede dejar sin suministro de gas intencionadamente a ningún hogar, esta cláusula sería ilegal. Si el contador de gas está situado dentro de la vivienda, esta cláusula no tendría ningún sentido en un contrato tradicional, pues el inquilino podría simplemente no dar acceso a nadie en la vivienda y no sería posible cerrar la llave del gas. Sin embargo, un smart contract estaría conectado, por una parte a la cuenta bancaria del casero y, por otra, a una llave de paso eléctrica para el gas. Si el inquilino no paga la renta dentro de los primeros días del mes, a las 0:00 del sexto día se queda sin gas. Mientras en un contrato tradicional, simplemente *no habría pasado nada* por haberse incluido esa cláusula ilegal, en un smart contract tendría que reclamar judicialmente que se le restableciera el servicio de gas.

- **Que esté bien implementado**: aunque parezca una perogrullada, los smart contracts implementan las cláusulas que contienen – en forma de algoritmo, como se ha visto – en un código o software y, ya estamos acostumbrados a ello en nuestra "era digital", las aplicaciones informáticas pueden fallar. No solo es fundamental utilizar una red blockchain para smart contracts de confianza –siendo Ethereum la más famosa y reconocida en la actualidad –, sino también que la forma de implementarlo sea la correcta. Si bien es cierto que actualmente la práctica de los smart contracts no está muy extendida, en los próximos años iremos viendo aparecer cada vez más proveedores de smart contracts que, gratis o por un módico precio, ofrecerán esa programación de reglas o cláusulas en código. Será entonces importante confiar en proveedores reconocidos y, muy probablemente, huir de posibles estafas y proveedores que tengan muchas limitaciones. En este punto, sin embargo, cabe resaltar que, dado que el smart contract residirá en la red correspondiente (por ejemplo, Ethereum) y no en ninguna entidad, no tiene relevancia alguna que estos proveedores puedan desaparecer después de haberse programado el smart contract. A diferencia de los contratos que utilizan las actuales técnicas de "escrow" (traducido como "dejar en consigna", "fianza" o "en depósito", del inglés), donde hay un tercero que se encarga de verificar que se cumplen las cláusulas de un contrato para liberar bienes o fondos procedentes de una de las partes a la otra, que sí supondrían un problema muy serio si el tercero de confianza desaparece como entidad o no resulta ser de tanta confianza, en el smart contract no es necesario que haya nadie: aunque la vida se extinguiera súbitamente del planeta Tierra, las condiciones del contrato se ejecutarían normalmente, siempre que exista un solo ordenador conectado a la red (Ethereum, por ejemplo) en cualquier lugar del mundo.

QUÉ SON LOS NFT

NFT son las siglas de "Non-Fungible Token", que se traduce literalmente del inglés como "testigos no fungibles", pero que el autor prefiere traducir mejor como "pruebas de unicidad"). La razón es que un NFT es un trozo de código (software) que hace uso de la tecnología Blockchain, normalmente bajo la forma de un smart contract donde el "objeto físico" del contrato es un activo digital (un archivo incrustado, o pegado irrevocablemente a este trozo de código) que declara su unicidad.

Veamos un ejemplo más sencillo: supongamos que sacamos una fotografía con el móvil. Esa foto se almacena, lógicamente, en un archivo digital (activo digital) en el teléfono. Podemos compartir esa foto con nuestros amigos y familiares, en nuestro perfil en las redes sociales o, incluso, hacer una copia de seguridad en la nube o en nuestro ordenador. Eso no tiene nada de NFT: por su propia naturaleza, los archivos digitales se pueden copiar ilimitadamente y siempre serán iguales.

Sin embargo, decidimos instalar una aplicación para convertir archivos en NFT en nuestro teléfono. Cuando sacamos la foto, la procesamos con la app y esta le añade un trozo de código (token) basado en Blockchain (recordemos que una de las características de esta tecnología es el uso de "hash" para evitar que se modifique ni un solo bit del archivo) que viene a "sellar" esa foto, dejando constancia de que es el original. Ese token se comparte en la red Blockchain correspondiente y queda almacenado en una cadena de bloques. Acabamos de convertir una fotografía en un activo único, que se puede comprar, vender y almacenar, incluso copiar, pero no *duplicar*.

Un momento… ¿No es lo mismo *copiar* que *duplicar*? En el mundo digital, no. Los lectores de libros, y especialmente los autores, podemos comprender muy bien esta diferencia con el ejemplo de los libros impresos: mientras una editorial puede imprimir miles de ejemplares de un libro (*copiar*), cuando, como autor, firmamos un libro, ya no es posible replicar exactamente ese libro (*duplicar*). Algo similar ocurre con los NFT en el mundo digital. De hecho, como autor, podemos dedicar un ebook a una persona, añadiendo un mensaje ("dedicado a Ana") y protegiendo el conjunto con un NFT. Aunque Ana pueda hacer todas las copias de seguridad que desee de su ebook, en todas ellas aparecerá "dedicado a Ana" y será distinto al resto de ebooks, sin dedicatoria.

Pero, ¿qué utilidad puede tener esto? Veamos primero las características fundamentales de los NFT:

- **Unicidad**: cada NFT es único. No es posible tener dos NFTs iguales. Cada uno tendrá un código "hash" diferente y un registro concreto dentro de la cadena de bloques de la red Blockchain que se haya utilizado para generarlo.
- **Indivisibilidad**: un NFT, una vez generado, es indivisible. Si creamos un NFT con un libro, por ejemplo, cualquier extracción de un capítulo o cualquier eliminación (de la página del copyright, por ejemplo) será detectable, pues no concordará con el registro existente en la red Blockchain correspondiente.
- **Transferibilidad**: al registrar un NFT en una red Blockchain, quedan también registrados datos asociados al activo digital (normalmente quién es su dueño, al igual que ocurre con las criptomonedas). Aunque, como propietarios, podemos realizar tantas copias de seguridad de un NFT como deseemos, formalmente todas estarán asociadas a nuestro identificador y, legalmente, la propiedad del activo será nuestra. Es más, el propio archivo normalmente está encriptado dentro del NFT registrado en la Blockchain y solo nuestro código personal podrá desencriptarlo, al igual que sucede con las criptomonedas (nadie puede acceder a ellas, salvo que se las transfiramos a su cuenta, registrando la transacción en la Blockchain y, consecuentemente, cambiando nuestro código por el del destinatario). Con los NFTs ocurre lo mismo. Una vez generados, solo nosotros podremos tener acceso al archivo, o quien nosotros queramos, transfiriéndoselo (a un solo destinatario, como ya se ha visto).
- **Escasez**: como consecuencia de todo lo anterior, los NFTs son escasos por naturaleza. En realidad, se generan de uno en uno, o podríamos pedir a un algoritmo que genere a partir de un archivo (una foto, un vídeo, un libro, una canción, la lista de los códigos secretos para lanzar los misiles nucleares de EE. UU., etc.) un número finito de NFTs. Este algoritmo, en realidad, los iría generando de uno en uno y registrándolos secuencialmente en la red Blockchain correspondiente.

Quizás ahora se entienda un poco mejor la razón de ser de los NFTs: producir bienes escasos en el mundo digital donde, tradicionalmente, todo se podía copiar hasta el infinito.

PLATAFORMAS MÁS CONOCIDAS PARA CREAR Y TRANSACCIONAR NFTS

Antes de nada, es importante destacar que, al igual que la propia tecnología Blockchain, el uso de NFTs está todavía en una fase muy incipiente, por lo que es de esperar que el ecosistema de proveedores y el catálogo de servicios disponibles varíe considerablemente durante los próximos años.

La mayoría de las plataformas han nacido como iniciativas independientes y, como ya estamos acostumbrados en otros casos de aplicaciones y servicios digitales masivos, es muy probable que algunas de ellas terminen siendo adquiridas por algún gigante tecnológico en pocos años, llámese Google, Microsoft, Meta, Amazon, Apple o Elon Musk.

Se muestran a continuación las plataformas para crear, vender y comprar NFTs más conocidas en la actualidad.

OpenSea

OpenSea, que se autodefine como la mayor plataforma de NFTs del mundo, ofrece una variedad de categorías, como obras de arte, tarjetas coleccionables y hasta nombres de dominio (la utilidad del NFT aquí es cuestionable, ya que quien mantiene estos registros son los organismos oficiales para cada tipo de dominio). La plataforma exige que los activos digitales cumplan con los estándares ERC-721 y ERC-1155 –que garantizan la autenticidad y efectiva propiedad– en colecciones asociadas a entidades externas de registro, como Axies, nombres de dominio ENS (Ethereum Name Service), CryptoKitties o Decentraland, entre otras. Además de la fórmula de subasta, OpenSea permite vender NFTs a precios fijos. Trabaja principalmente con la red Ethereum, aunque está implementando otras como Solana.

Mintable

Respaldada por el multimillonario estadounidense Mark Cuban, Mintable es una plataforma de compraventa de NFTs que pretender ser un mercado abierto, similar a OpenSea.

La plataforma, que funciona con la red Ethereum, también permite generar NFTs de distintos tipos (Fig. 3) a creadores de contenido que quieran vender sus obras como activos digitales únicos. Una de sus ventajas es que permite crearlos sin coste, incluyendo las tarifas que cobra la propia red Ethereum por su propio uso (también denominadas "gas").

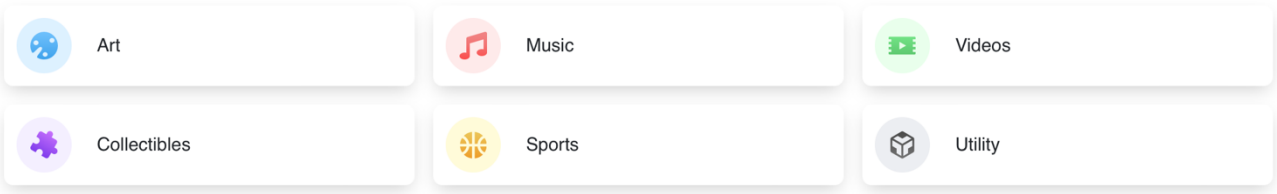

Fig. 3. Categorías de activos digitales que permite la plataforma Mintable

Rarible

Estrenada en 2020, Rarible es considerada una de las mejores plataformas para comercializar NFTs, justo detrás de OpenSea. Ofrece un mercado descentralizado con negociación directa entre

compradores y vendedores. Cuenta con una interfaz bastante completa (Fig. 4), que permite conocer los NFTs que son tendencia (comprados y vendidos con mayor frecuencia) y los vendedores y compradores con más transacciones durante los últimos días.

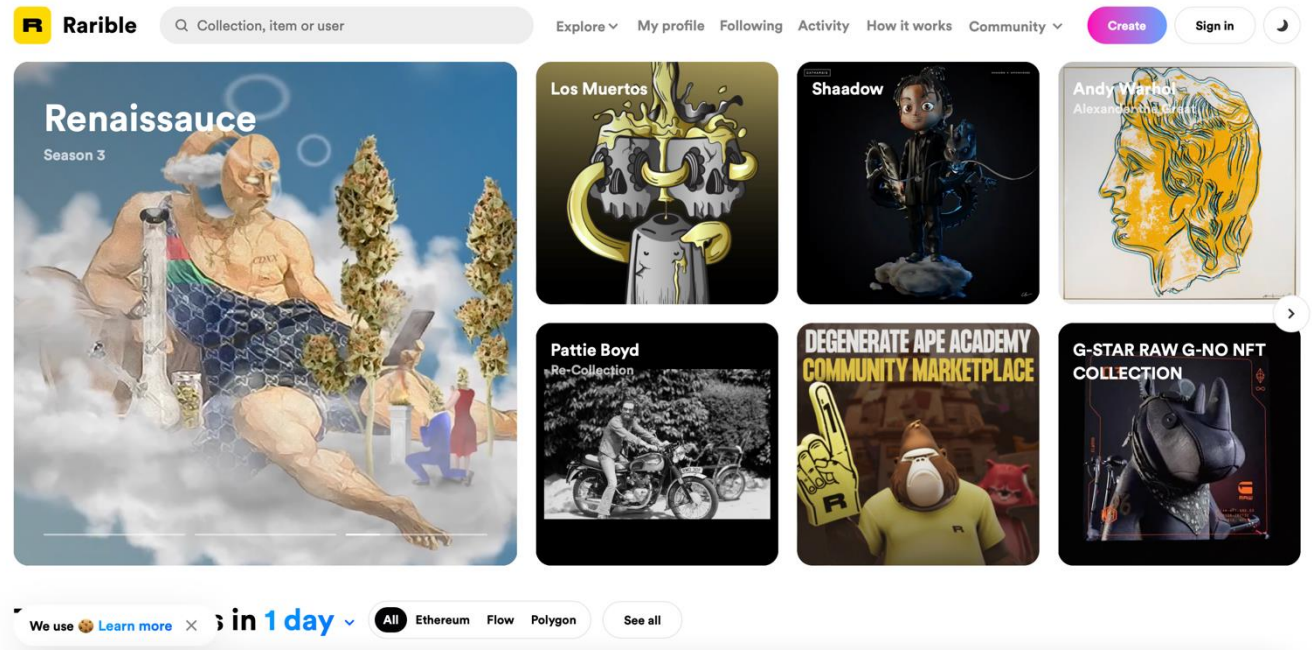

Fig. 4. Aspecto de la Plataforma Rarible, muy similar a los portales de compraventa tradicionales tipo Ebay

La plataforma no solo permite comprar o vender NFTs. También permite crear tokens sobre activos digitales propios, mediante un proceso guiado para quienes no son especialistas en la materia. Para los autores, permite incluso obtener derechos de autor de hasta el 50% por ciento en futuras reventas, aunque lo habitual es que se sitúen entre el 5% y el 10%. Este es, por ejemplo, uno de los nuevos usos que permite la tecnología NFT frente a las transacciones tradicionales de activos: al encontrarse toda la información sobre las transacciones en la Blockchain, es posible que el autor obtenga derechos adicionales de autor por las ventas posteriores, "de segunda mano", de sus obras.

Ethernity

Ethernity es una plataforma que permite la venta de NFTs exclusivos y de edición limitada, con un especial foco en el deporte, como el fútbol o el fútbol americano. De hecho, figuras como los futbolistas Lionel Messi y Luis Suárez se han sumado a utilizar este portal. Ethernity ofrece dos mecanismos para adquirir un NFT: mediante subasta o compra, este último solo para NFTs que ya han sido vendidos previamente en subasta. Se puede decir que sus tarifas son totalmente abusivas, pues la plataforma se queda con el 75% de la venta, dejando al autor solo el 25%. Opera con Ethereum.

Valuables

A diferencia de otras plataformas de compraventa de NFTs, Valuables solo permite comercializar tuits "autografiados" por sus creadores. De hecho, fue la plataforma escogida por el fundador de Twitter, Jack Dorsey, para subastar el primer tuit de la historia por $2.9 millones de dólares (Fig. 5). Es posible revisar las subastas en curso o añadir el enlace a cualquier mensaje de Twitter y decidir si se prefiere venderlo o comprarlo. Todas las transacciones se hacen a través de la red Ethereum.

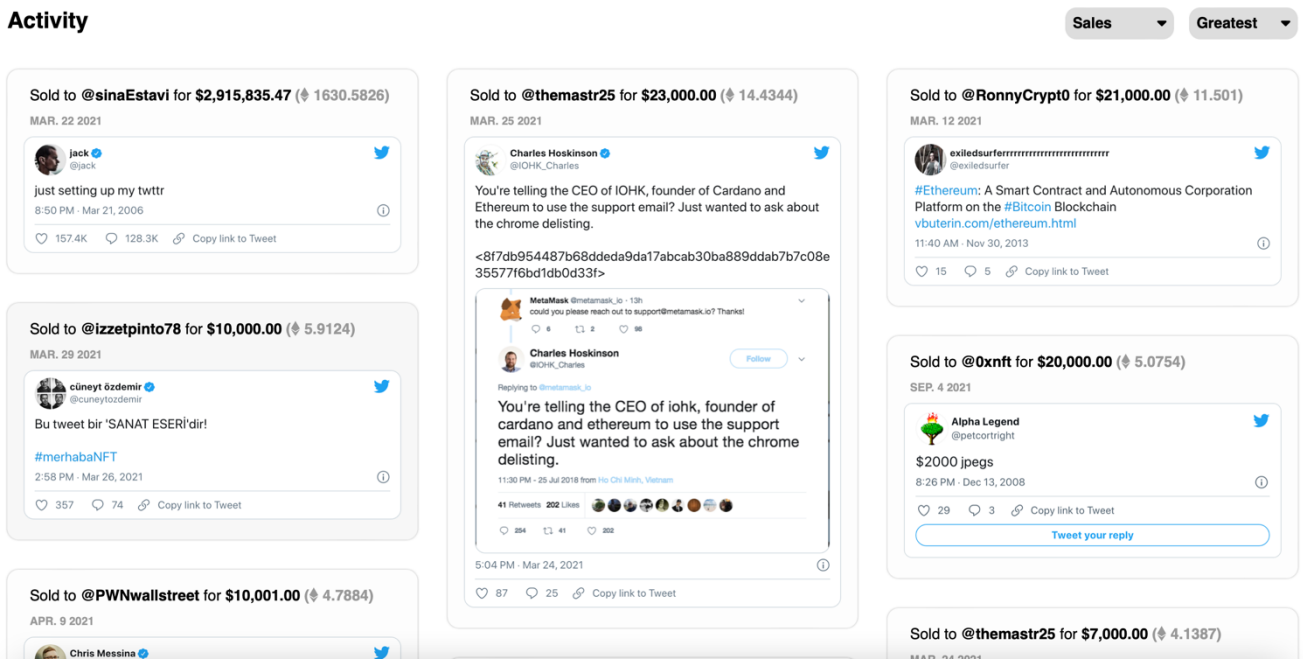

Fig. 5. Pantalla de inicio de la Plataforma Valuables, con algunos ejemplos de transacciones de compraventa de twits

Foundation

Estrenada en febrero de 2021, Foundation reúne a creadores y coleccionistas, con un enfoque centrado en el arte digital. En sus inicios nacio para que los creadores experimentaran con criptomonedas, aunque poco tiempo después consiguió convertirse en uno de los principales sitios para comercializar NFTs. Los creadores reciben el 85% del valor total de la transacción. Además, si el NFT fue generado en la plataforma Foundation, cada vez que se revenda en cualquier plataforma basada en la red Ethereum, obtendrá el 10% de la transacción. Según cifras de la propia plataforma, desde su lanzamiento, los creadores han ganado más de 40 millones de dólares en total y hay más de 425 artistas que han ganado más de 12.000 dólares cada uno.

KnownOrigin

KnownOrigin es un mercado donde se puede encontrar y coleccionar obras de arte digitales exclusivas y únicas. Los creadores pueden usar la plataforma para exhibir y vender su trabajo a coleccionistas que se preocupan por la autenticidad y originalidad. Además, la plataforma se encarga de elegir a los creadores, que deben enviar sus ilustraciones con los archivos en el protocolo IPFS, que permite rastrear sus versiones en el tiempo. Funciona también con la red Ethereum.

Axie Marketplace

Axie Marketplace es la tienda online del videojuego Axie Infinity, donde es posible comprar "axies", como se denominan las criaturas que pueden ser "entrenadas" por un jugador y, posteriormente, vendidas a otro jugador, como ocurría en el mundo físico con los gladiadores romanos en el pasado o con los futbolistas, en el presente. Los usuarios pueden comprar *axies* (Fig. 6), terrenos y otros elementos del juego bajo la forma de NFTs, para usarlos dentro del propio juego. Además, como los NFTs "Axie Shards" (como son denominados) están basados en la red Ethereum, se pueden comercializar en las otras plataformas NFT compatibles con esta red.

Fig. 6. "Axies", del juego Axie Infinity

SuperRare

SuperRare se autodefine como una mezcla entre la famosa casa de subastas Christie's e Instagram, ya que busca facilitar el coleccionismo de arte digital y que los usuarios presuman de ello en sus redes sociales, mediante una galería personal. Es un sitio dirigido a quienes buscan comprar y vender obras digitales exclusivas: se identifican con un NFT único, protegido y rastreable en su propia red Blockchain, que sigue el estándar ERC-721.

Al igual que Foundation, los creadores reciben el 85% de la primera venta y obtienen derechos extra por el 10% de cada transacción posterior, en el mercado secundario. Por el momento, está restringida a una pequeña cantidad de artistas, que deben solicitar su admisión. Todas las transacciones se realizan sobre la red Ethereum.

Nifty Gateway

Fundada en 2018 por los hermanos Duncan y Griffin Cock Foster, Nifty Gateway también sigue el modelo centralizado para la compraventa de activos digitales. Su estrategia consiste en asociarse con artistas y marcas para crear colecciones exclusivas y de edición limitada. Cobra una comisión del 5% del precio de venta, además de 30 centavos de dólar para cubrir los gastos de transacción. Por cada venta en el mercado secundario, el artista recibe el 10%. La plataforma ha recibido algunas críticas de artistas, que la acusan de cobros pocos transparentes y suspensiones arbitrarias de subastas en curso.

CONCLUSIONES

En este artículo hemos visto los fundamentos básicos de la tecnología Blockchain y como, a través de ellas, se pueden obtener smart contracts, capaces de ejecutar cláusulas automáticamente. Estos contratos podrán transformar en gran medida los contratos de derechos de autor, haciéndolos más completos, transparentes y con mayores posibilidades, sobre todo en el ámbito del mundo de los contenidos digitales.

Por otra parte, se ha presentado el concepto de NFT y cómo puede ser una herramienta bastante útil para productores de contenidos, en general. Sin embargo, su adopción es muy incipiente aún y será necesario que transcurra algún tiempo antes de que los NFTs tengan aplicaciones útiles y generalizadas, más allá de la mera especulación y el interés que generan en las noticias determinadas transacciones millonarias, de vez en cuando.

Sin duda, los autores tenemos por delante un gran programa de cambios profundos en el sector, que debemos comprender, aprender y acometer, cuando llegue el momento.

BIBLIOGRAFÍA

[1] DI PIERRO, Massimo. What is the blockchain?. Computing in Science & Engineering, 2017, vol. 19, no 5, p. 92-95.

[2] NOFER, Michael, et al. Blockchain. Business & Information Systems Engineering, 2017, vol. 59, no 3, p. 183-187.

[3] XU, Min; CHEN, Xingtong; KOU, Gang. A systematic review of blockchain. Financial Innovation, 2019, vol. 5, no 1, p. 1-14.

[4] BASHIR, Imran. Mastering blockchain. Packt Publishing Ltd, 2017.

[5] DAVIDSON, Sinclair; DE FILIPPI, Primavera; POTTS, Jason. Economics of blockchain. Available at SSRN 2744751, 2016.

[6] BELOTTI, Marianna, et al. A vademecum on blockchain technologies: When, which, and how. IEEE Communications Surveys & Tutorials, 2019, vol. 21, no 4, p. 3796-3838.

[7] MOHANTA, Bhabendu Kumar; PANDA, Soumyashree S.; JENA, Debasish. An overview of smart contract and use cases in blockchain technology. En 2018 9th international conference on computing, communication and networking technologies (ICCCNT). IEEE, 2018. p. 1-4.

[8] LEGERÉN-MOLINA, Antonio. Los contratos inteligentes en España (La disciplina de los smart contracts)/Smart contracts in Spain; the regulation of smart contracts. Revista de Derecho civil, 2018, vol. 5, no 2, p. 193-241.

[9] WANG, Shuai, et al. An overview of smart contract: architecture, applications, and future trends. En 2018 IEEE Intelligent Vehicles Symposium (IV). IEEE, 2018. p. 108-113.

[10] SÁENZ, Marina Echebarría. Contratos electrónicos autoejecutables (smart contract) y pagos con tecnología blockchain. Revista de estudios europeos, 2017, no 70, p. 69-97.

[11] RASKIN, Max. The law and legality of smart contracts. Geo. L. Tech. Rev., 2016, vol. 1, p. 305.

[12] REY, Jorge Feliú. Smart Contract: Concepto, ecosistema y principales cuestiones de Derecho privado. La Ley Mercantil, 2018, no 47, p. 1.

[13] ZHENG, Zibin, et al. An overview on smart contracts: Challenges, advances and platforms. Future Generation Computer Systems, 2020, vol. 105, p. 475-491.

[14] WANG, Qin, et al. Non-fungible token (NFT): Overview, evaluation, opportunities and challenges. arXiv preprint arXiv:2105.07447, 2021.

[15] CHOHAN, Usman W. Non-fungible tokens: Blockchains, scarcity, and value. Critical Blockchain Research Initiative (CBRI) Working Papers, 2021.

[16] KUGLER, Logan. Non-fungible tokens and the future of art. Communications of the ACM, 2021, vol. 64, no 9, p. 19-20.

[17] ANTE, Lennart. The non-fungible token (NFT) market and its relationship with Bitcoin and Ethereum. Available at SSRN 3861106, 2021.

[18] WILSON, Kathleen Bridget; KARG, Adam; GHADERI, Hadi. Prospecting non-fungible tokens in the digital economy: Stakeholders and ecosystem, risk and opportunity. Business Horizons, 2021.

[19] TRAUTMAN, Lawrence J. Virtual art and non-fungible tokens. Available at SSRN 3814087, 2021.