Consecuencias penales y tributarias a la modificación fraudulenta de los *smart contracts*. Especial referencia al caso The DAO

Marta María Aguilar Cárceles
Profesora contratada doctora de Derecho Penal y Criminología.
Universidad de Murcia

Norberto Miras Marín
Profesor asociado (acreditado a ayudante doctor)
de Derecho Financiero y Tributario.
Universidad de Murcia

Extracto

La modificación de los denominados *smart contracts* –«contratos» que se formalizan en el código de un *blockchain*– supone que, por su mecánica de funcionamiento en la cadena de bloques que los configura como «autoejecutables», en el caso de que se produzca una alteración fraudulenta de los mismos que derive una transmisión patrimonial, esta modificación sea difícilmente corregible, aunque sea detectable para las partes. El ejemplo paradigmático fue el conflicto de The DAO, en la que una parte los miembros de la red aceptaba el fraude por no infringir los principios de no intervención y modificación del código. El objetivo de este análisis es la determinación de las posibles consecuencias jurídicas que nacen en torno a este tipo de situaciones.

Palabras clave: criptodivisas; Ethereum; *smart contracts*; DAO.

Fecha de entrada: 22-01-2020 / Fecha de aceptación: 26-02-2020

Cómo citar: Aguilar Cárceles, M. M.ª y Miras Marín, N, (2020). Consecuencias penales y tributarias a la modificación fraudulenta de los *smart contracts*. Especial referencia al caso The DAO. *Revista CEFLegal*, *231*, 113-134.

Criminal and tax consequences to the fraudulent modification of smart contracts. Special reference to the case The DAO

Marta María Aguilar Cárceles

Norberto Miras Marín

Abstract

The modification of the smart contracts –«contracts» that are formalized in the code of a blockchain– supposes that, due to their mechanics of operation in the blockchain that configures them as «self-executing», in the event that a fraudulent alteration thereof that derives a transfer of assets, this modification is difficult to correct, although it is detectable for the parties. The paradigmatic example was The DAO conflict, in which one part of the network members accepted fraud for not violating the principles of non-intervention and modification of the code. The objective of this analysis is the determination of the possible legal consequences that arise around this type of situation.

Keywords: cryptocurrencies; Ethereum; smart contracts; DAO.

Citation: Aguilar Cárceles, M. M.ª y Miras Marín, N, (2020). Consecuencias penales y tributarias a la modificación fraudulenta de los *smart contracts*. Especial referencia al caso The DAO. *Revista CEFLegal*, *231*, 113-134.

Sumario

1. Consideraciones previas

Bitcoin, la primera de las criptodivisas, se creó como un proyecto de código abierto, por lo que es relativamente sencillo «clonar» su programación y crear una nueva «moneda virtual». A partir de esta pionera divisa virtual, se desarrolló una primera generación de divisas virtuales, idénticas a ella o muy parecidas.

El salto cualitativo, que nos lleva a la segunda generación de criptodivisas, y que abrió nuevas vías de transformación de los mercados financieros, la realiza Ethereum. El rasgo diferencial que distingue a esa segunda generación es la aportación del concepto de «dinero programable», bajo lo que se denominan *smart contracts*.

El proyecto de Ethereum tiene su origen en una fundación afincada en Suiza, desde la cual se creó la criptomoneda *ether*, que es lo que se mina para que haya un incentivo económico para formar parte de la red, al igual que en el caso de *bitcoin*, pero que es a su vez la moneda con la que se paga por el uso de la plataforma de Ethereum. Así, el valor del *ether* está conectado con el uso que se haga de Ethereum como plataforma de *blockchain*. Otro aspecto interesante del *ether* es que, al contrario del *bitcoin*, no tiene determinado el número máximo de *ethers* que sean emitidos.

La gran aportación de Ethereum ha sido la posibilidad de programar los nodos para que se ejecuten programas de *software* completos, pero siempre de manera distribuida, es decir, con las mismas propiedades que las transacciones de *bitcoins* –descentralizadas, seguras, automáticas, con su código inmutable, etc.–.

A partir de ese estado de cosas, se crean las organizaciones autónomas descentralizadas (DAO), que son «asociaciones» fundamentadas en *smart contracts*, porque es posible, en los sistemas de las monedas virtuales de segunda generación, realizar un contrato de sociedad «participativo» e incluirlo en el *blockchain*.

La DAO de Ethereum fue la primera aplicación de contratos inteligentes en dicha red y el mayor *crowdfunding* de la historia. Ahora bien, un miembro de la red fue capaz de modificar el código de los «contratos» y propagarlo, de forma que muchos miembros, por inercia, seguían prestando su consentimiento a un contrato modificado que desvió una tercera parte de todos los activos de la DAO a su propia cuenta. La comunidad de Ethereum podía impedir que se ejecutase a orden de transferencia, dado que el *smart contract* tenía un plazo

para la ejecución, que no se había cumplido cuando se percataron de la operación. Ahora bien, se produjo un serio debate: si se intervenía y se modificaba el código, para recuperar los fondos, la gestión sería «humana» y contravendría el fundamento de convertir el código en ley –vulnerando el viejo sueño de un automatismo de las organizaciones autónomas descentralizadas–, a la vez que cuestionaría la razón de ser de los *smart contracts*.

En el presente artículo reflexiona sobre estos hechos y sus eventuales consecuencias jurídicas, realizando, en primer lugar, una aproximación al concepto, régimen jurídico y tributario de los *smart contracts*.

2. Los *smart contracts*: delimitación conceptual, régimen jurídico y eventual tributación

Los programas que reúnen los requisitos establecidos en la legislación civil para configurar un contrato, escritos y ejecutados en la cadena de bloques, son llamados *smart contracts* o «contratos inteligentes». Supusieron un paso adelante decisivo en el ámbito de las monedas virtuales, puesto que la integración de esta modalidad algorítmica en *blockchain*, el poder «programar dinero», ha permitido abrir la puerta al desarrollo de infinidad de aplicaciones prácticas. A este punto le dedicaremos más adelante un prolijo desarrollo.

La plataforma Ethereum, cuya red no solo refleja transacciones de valor monetario, sino que es una red para la creación de contratos basados en Ethereum[1], contiene unos contratos de código abierto que pueden ser usados para ejecutar de forma segura una amplia variedad de servicios, entre los que se incluyen seguros, contratos financieros atípicos o plataformas de criptomecenazgo o de propiedad intelectual. Se ha producido la deriva en la utilización de la programación del *blockchain* de la divisa y su red como nicho para ofrecer *smart contracts*, que, a continuación, analizaremos en profundidad.

Así pues, la moneda virtual *ether* incluye la posibilidad de programar la criptodivisa para que ejecute *scripts* de *software* de manera distribuida, lo cual ha abierto la puerta a múltiples funcionalidades. Esos programas incluidos en el propio dinero, denominados *smart contracts*, han calificado a las monedas virtuales que los contienen como de «segunda generación».

Los *smart contracts*, contratos inteligentes, se definen como contratos que tienen la capacidad de cumplirse de forma automática una vez que las partes han acordado los términos (Bourque y Fung Ling Tsui). Por tanto, de manera sintética se configuran como contratos en formato electrónico y de carácter autoejecutable.

[1] Podemos encontrar gratuitamente en la web los editores para redactar estos contratos inteligentes, por ejemplo, EtherScripter. A mayor abundamiento –sobre todo técnico–, se puede consultar: «What is Ethereum?». En <http://www.etherscripter.com/what_is_ethereum.html>. Consulta el 14 de diciembre de 2019.

Aunque existe tendencia a identificar los *smart contracts* con formatos que usan *blockchain*, lo cierto es que conforme a un patrón de neutralidad tecnológica podemos considerar como *smart contracts* a cualquier acuerdo en el que se formalicen todas o algunas de sus cláusulas mediante *scripts* o pequeños programas, cuyo efecto sea que, una vez concluido el acuerdo y señalados uno o varios eventos desencadenantes, la producción de los eventos programados conlleve la ejecución automática del resto del contrato, sin que quepa modificación, bloqueo o inejecución de la prestación debida (Echebarría Sáenz, 2017, p. 70).

Así, se puede añadir a la moneda virtual, como un *script*[2], uno o más *smart contracts*, que se ejecutarán cuando se den las condiciones acordadas[3]. Pongamos varios ejemplos: se puede programar una moneda virtual para que, en el caso de un determinado tipo de subastas, puje automáticamente; otros son *templates* de sorteos de monedas virtuales, en el que la propia moneda se sortea y se transmite al ganador. Incluso existen *scripts* de compraventa en el que una moneda virtual analiza la red buscando el precio más bajo de un artículo y se autopaga (Navarro Lérida, 2018, p. 23).

Existen plataformas disponibles con «smart contracts as a service», lo que implica que se pueden crear distintos tipos de contratos sobre «bitcoin» o «ethereum», sin necesidad de saber programación de código, basta con una sencilla programación visual por bloques[4].

En principio, los *smart contracts* serían calificados como contratos, con el valor y la eficacia jurídica que corresponda a su respectiva naturaleza, pues consagrado el principio de libertad de forma, si concurren consentimiento, objeto y causa de un contrato[5], el que se plasme en formato digital, código binario de unos y ceros susceptibles de ejecución por una máquina, no le resta ninguno de los elementos necesarios para su validez, atendiendo al principio de equivalencia funcional entre los medios de expresión físicos y documentos electrónicos que se recoge en el artículo 3, en sus epígrafes 6, 7 y 8 de la Ley 59/2003, de firma electrónica.

Un *smart contract* sigue las reglas generales de cualquier contrato concertado por vía electrónica, por lo que a falta de pacto o de foro imperativo por protección del consumidor,

---

2 Podríamos definir «plugin» como un programa informático de complemento que se relaciona con otro programa para aportarle una función nueva y generalmente muy específica. Esta aplicación adicional es ejecutada por la aplicación principal e interactúan por medio de la API.

3 Los contratos inteligentes siempre han estado ahí. Existe la posibilidad de prestar consentimiento y programar un pago en una plataforma bancaria, pero la tecnología de registro distribuido ha hecho que se no se tengan costes, debido a que se realiza en ordenadores imparciales donde se ejecuta el programa, aspecto que soluciona el carácter descentralizado de la cadena de bloques. En este sentido, Bellany y Hill, (2016) o Butler, Al Khalil, Ceci y O'Brien (2017, p. 2). Y, manteniendo una opinión parecida, pero haciendo específica referencia a las criptomonedas, Kost de Sevres, Chilton y Cohen (2016, p. 3).

4 Por ejemplo: las empresas SEIF y Kratos Innovation Labs ofrecen *templates* (plantillas) de *smart contracts* en <https://seif.io/ y https://kratosinnovationlabs.com/smart-contracts-as-a-service>. Consultado el 16 de diciembre de 2019.

5 El consabido artículo 1.261 del Código Civil.

se entenderá concertado conforme a la regla del artículo 1.262 del Código Civil y 50 del Código de Comercio, en el domicilio del oferente, y seguirá la regla del artículo 54 del Código de Comercio en lo referente al momento de la perfección. Lo cierto es que dicho artículo en su párrafo final contiene una norma que viene pintiparada: «En los contratos celebrados mediante dispositivos automáticos hay consentimiento desde que se manifiesta la aceptación».

Respecto al tratamiento tributario se podría argumentar que los *smart contracts* se pueden configurar como contratos mixtos o complejos[6]; encontrando la determinación de la existencia de prestaciones dependientes, infiriéndose que si entendemos a la divisa virtual como un programa informático *online*, esto es, un servicio electrónico en sede de IVA, se trata de dos o más servicios vinculados.

Sin embargo, la sentencia *Heqvist* del TJUE ha calificado como divisa a las divisas virtuales. Por tanto, su naturaleza jurídica sería distinta a los *smart contracts* por más que técnicamente estuvieran vinculados. Así, una vez aislados y calificados, los contratos, introducidos en el código de las divisas, pero con una funcionalidad diferente a la de ser medio de pago, tributarían como tales.

En definitiva, la divisa virtual y el *smart contract* se encuentran estrechamente ligados, pero objetivamente no forman una sola prestación económica indisociable cuyo desglose resultaría artificial, de forma que todos los elementos que integran la operación de que se trata resultan necesarios para llevarla a cabo y están estrechamente vinculados entre sí. Están vinculados, pero resultan independientes, a la par que con naturalezas jurídicas distintas[7].

3. Concepto de «organización autónoma descentralizada» (DAO)

El poder de coordinación de una *blockchain* no se limita al registro de operaciones de transmisión de criptodivisas. También permite la ejecución e interconexión de una variedad de *smart conctracts* que interactúan entre sí de manera descentralizada y distribuida. Estos *smart conctracts* pueden ser unidos para formar organizaciones descentralizadas (DAO) que operan de acuerdo a reglas y procedimientos específicos definidos por contratos inteligentes[8].

---

6 El Tribunal de Justicia de la Unión Europea en sus sentencias de 25 de febrero de 1999, asunto C-349/96 (NFJ007331), y de 29 de marzo de 2007, asunto C-111/05 (NFJ025247), se planteó cuáles deben ser los criterios para decidir, en materia del impuesto sobre el valor añadido, si una operación que está compuesta por varios elementos debe ser considerada como una prestación única o como dos o más prestaciones diferentes que deben ser apreciadas separadamente.

7 Véase, por analogía, la Sentencia del Tribunal de Justicia de la Unión Europea (Sala Primera), de 27 de octubre de 2005. Levob Verzekeringen BV y OV Bank NV vs. Staatssecretaris van Financiën, asunto C-41/04 (NFJ021025).

8 El que ideó las DAO tiene nociones de economía. En realidad, está fundamentándose en la teoría mantenida por M. C. Jensen y W. H. Meckling en su libro *Theory of the Firm: Managerial Behavior, Agency Costs*

Las organizaciones autónomas descentralizadas son un tipo específico de organización que es a la vez autónoma[9] –en el sentido de que, después de su creación, e inclusión en la cadena de bloques, ya no necesita operadores humanos–, autosuficiente –en el sentido de que puede acumular capital, como monedas digitales– y descentralizada, dado que no existe un centro de decisión.

Las organizaciones autónomas descentralizadas dejan la administración en manos de los miembros participantes, quienes pueden presentar propuestas a la comunidad y, luego, contar con la aprobación de otros miembros. A partir de ahí, no son necesarios los representantes o administradores, las propias DAO se ejecutarán de forma automática siguiendo los planteamientos que previamente hayan sido aprobados por todas las partes y establecidos en el programa. En definitiva, cada miembro de la DAO, si se quiere constituir una «sociedad de inversión automatizada», puede presentar a la comunidad una propuesta de inversión. Una vez que los usuarios hayan aprobado los detalles establecidos en la propuesta a través del proceso de votación, la ejecución de esta se llevará a cabo y será ejecutada de forma autónoma e inteligente por el código (Merkle, 2016, pp. 28-40).

Así, una idea que se planteó en las comunidades de informáticos fue crear, por ejemplo, un fondo de inversión a través de una red de *smart contracts* que se ejecutarían sobre la base del sistema de red de una criptomoneda. Este fondo de inversión funcionaría sin supervisión humana[10].

Desde el punto de vista del derecho privado, la calificación como sociedad de las DAO sería compleja. Según el Código Civil, la sociedad civil es aquel contrato por el cual dos o más personas se obligan a poner en común dinero, bienes o industria, con ánimo de repartir entre sí las ganancias, pero si, como puede ser el caso, vemos atisbos de mercantilidad en una DAO, podría aplicársele la doctrina de la sociedad nula, que se aplica a las sociedades en formación e irregulares[11].

---

and Ownership Structure (3 J. FIN. ECON. 305, 310-11, 1976). Esta teoría sostiene que las corporaciones son un conjunto de contratos interrealcionados. Las DAO han transformando la teoría de Michael Jensen y William Meckling en realidad. A través de A. Wright y P. De Filippi. Decentralized Blockchain Technology and the Rise of Lex Cryptographia. En <https://ssrn.com/abstract=2580664> o <http://dx.doi.org/10.2139/ssrn.2580664>. Consulta el 17 de diciembre de 2019.

9 En realidad, más que «autónomas» deberíamos decir que son «automatizadas», pero la traducción literal del inglés sería la primera.

10 Todo debería estar automatizado. Por ejemplo, este fondo se debe invertir replicando el índice de bolsa «x», teniendo por «x» el IBEX, S&P, NASDAQ, etc.

11 Si una sociedad es nula porque falta alguno de los elementos esenciales del contrato para su validez, debería entenderse que es nula desde el principio (ex art. 1.303 CC) y, por lo tanto, no tendrían efecto los contratos celebrados por la sociedad con terceros, desde su nacimiento. Pero una vez puesta en marcha e inserta en ese entramado o tejido de relaciones jurídicas, que es el tráfico, tal eficacia retroactiva resulta contraproducente y, a veces, imposible de ejecutar.

4. La DAO de Ethereum

En mayo de 2016, en la plataforma Ethereum se creó un fondo de capital riesgo de gestión descentraliza mediante *smart contracts*; una DAO cuya actividad se centraba en la inversión en *start-ups* relacionadas con *blockchain*. Se denominó The DAO. Fue la mayor operación de *crowdfunding* de la historia[12].

4.1. La *initial coin offering* (ICO) de The DAO

Los que participan en una DAO, lo hacen, generalmente, a través de una *initial coin offerings* (ICO). Las ICO, u ofertas iniciales de monedas virtuales, consisten en una oferta pública previa al lanzamiento al mercado de una divisa virtual o de un *smart contract.* La expresión ICO puede hacer referencia tanto a la emisión propiamente dicha de monedas virtuales, como a la emisión de cupones virtuales, denominados *tokens*. Estos activos se ponen a la venta a cambio de criptomonedas como *bitcoins* o *ethers* o de divisa oficial (por ejemplo, euros).

El intercambio de un cupón virtual o *token* derivado de una ICO por una moneda virtual constituye una permuta, conforme a la definición contenida en el artículo 1.538 del Código Civil español. Dicho intercambio da lugar a una alteración en la composición del patrimonio, ya que se sustituye una cantidad cupón virtual por una cantidad de otra moneda virtual, y con ocasión de esta alteración se pone de manifiesto una variación en el valor del patrimonio materializada en el valor de la moneda virtual que se adquiere en relación con el valor al que se obtuvo del cupón virtual que se entrega a cambio[13].

En consecuencia, el intercambio entre cupones virtuales y monedas virtuales diferentes realizado al margen de una actividad económica da lugar a la obtención de renta que se califica como ganancia o pérdida patrimonial conforme al artículo 33.1 de la LIRPF.

En la cuantificación de dichas rentas será de aplicación lo previsto en los artículos 34.1 a), 35 y 37.1 h) de la LIRPF. El artículo 34.1 a) establece con carácter general que el importe de las ganancias o pérdidas patrimoniales será, en el supuesto de transmisión onerosa o lucrativa, la diferencia entre los valores de adquisición y transmisión de los elementos patrimoniales, valores que en el caso de adquisiciones y transmisiones a título oneroso vienen definidos en el artículo 35 de la misma ley[14].

---

[12] En torno a 150 millones de dólares y 11.000 inversores en todo el mundo.

[13] La aplicación de este criterio se sustenta en una aplicación analógica de la Resolución de la Dirección General de Tributos V0999-18 respecto al intercambio de monedas virtuales y en que no hay distinción entre *token* y criptodivisa a efectos de su naturaleza jurídica.

[14] Y el artículo 37.1, que recoge determinadas normas específicas de valoración de las ganancias y pérdidas patrimoniales, en su letra h) establece que cuando la alteración patrimonial proceda de la permuta de bienes

Durante la ICO de la DAO, realizada en mayo de 2016, el único requisito para ser inversionista y miembro de la DAO era invertir *ethers*. A cambio, los participantes recibieron *tokens* DAO, 100 *tokens* DAO por 1 *ether*, que otorgaban derecho de voto para ser utilizado durante la selección de los proyectos que serían financiados[15].

4.2. La modificación de los *smart contracts* y la «llamada recursiva»

El 17 de junio de 2016, un miembro de la red Ethereum logró que se transfirieran *ethers* por valor de 50 millones de dólares del DAO a su monedero electrónico; aprovechaba la posibilidad de hacer una modificación a la programación del *smart contract* que permitía incluir un bucle de retiradas de criptomoneda antes de que finalizara el tiempo y cerrar el proyecto y actualizar el balance.

Se logró llamar recursivamente a la función de recuperación de su inversión y recuperó sus fondos reiteradamente, antes de llegar al paso donde el código verificaba el saldo del fondo DAO, en lo que se conoce como una «llamada recursiva».

El miembro de la red publicó una carta abierta dirigida a la comunidad Ethereum. En esta carta abierta, afirmaba que el código regulaba la DAO, y al estar permitida su modificación, sus acciones fueron legítimas. Únicamente, hacía uso de una función (*split*) codificada explícitamente en los términos del contrato inteligente. Y continuó señalando que «tomar medidas equivaldría a incautar [su] *ether* legítimo, reclamado legalmente a través de los términos de un contrato inteligente». En definitiva, manifestaba que, según su opinión, no alteró de forma fraudulenta una programación para acceder a los *ether* sustraídos de la DAO.

4.3. La escisión de Ethereum y la recuperación de los fondos

En las condiciones legales a las que se adherían quienes participaban en The DAO se asumía la filosofía *code is law*, entendiendo que únicamente les vinculaba la ejecución del código.

---

o derechos, incluido el canje de valores, la ganancia o pérdida patrimonial se determinará por la diferencia entre el valor de adquisición del bien o derecho que se cede y el mayor de los dos siguientes: el valor de mercado del bien o derecho entregado y el valor de mercado del bien o derecho que se recibe a cambio.

15 El supervisor norteamericano –la conocida SEC– dio el visto bueno a The DAO y aplicó el test Howey para determinar que la emisión de los *token* a través de la ICO de The DAO cumplía con los tres requisitos que deben darse para considerar la existencia de un activo, a saber: que se trata de una inversión en dinero, con una expectativa razonable de beneficio y que tal beneficio se debe principalmente al esfuerzo de «gestión» de terceros ajenos a los titulares de esos *token* (SEC).

Code is law es una expresión coloquial referida al artículo de Lawrence Lessing y al libro *Code and other laws of cyberspace*, que no establece la sustitución de leyes por *software*, sino algo bastante diferente y, francamente, mucho más interesante (Lessing).

Lessing sostiene que el código no reemplaza a la ley, sino que el ciberespacio es un entorno que está en sí mismo regulado únicamente por las reglas del código. El punto de hacer esa observación es centrar la atención en quién decide qué se programa, es decir, quién tiene voz en el diseño de estas nuevas estructuras reguladoras basadas solo en el código informático[16]. Nos habla de forma de gobierno o toma de decisiones, no de reemplazo del ordenamiento jurídico.

La plataforma Ethereum está gobernada por la Ethereum Foundation, que toma las decisiones mediante votación. Después de la modificación del código, se debatieron qué medidas tomar. Para algunos se trataba de un robo o de una estafa, y como existía la posibilidad de modificar el código para «corregir» los *smart contracts*, debía realizarse esta segunda modificación aun a costa de no cumplir la filosofía *code is law*, interviniendo en la autoejecución. Otros pensaban que, aunque la modificación era engañosa, no se debía reescribir el código por ir en contra del principio de autoejecución. Y una tercera parte opinaba que era una vulnerabilidad típica de código y por lo tanto un riesgo inherente a un contrato inteligente, y que los participantes en The DAO debían asumir las pérdidas.

Al final, se decidió implementar un *hard fork*, una manipulación consensuada del *blockchain* que permite la generación de una nueva cadena de bloques[17], iniciándose desde el momento anterior al bloque que contiene la transferencia motivada fraudulentamente. Esto se logró por un acuerdo de mayoría de los nodos que actúan como mineros del sistema Ethereum, buscando su adhesión a la nueva línea de la cadena, que no incluye la transferencia de fondos recursivamente. De esta forma, se consiguió evitar un perjuicio patrimonial cifrado en casi 60 millones de dólares.

Esta decisión llevó a la Ethereum Foundation a un cisma que se dirimió por desmembración en dos plataformas: Ethereum y Ethereum Classic. El código no fue la ley, nunca lo es, y aunque lo hubiera sido, hubiera sido una ley injusta, viciada en su nacimiento, que se modificó justamente, con verdaderos criterios de equidad.

Ahora bien, convendría plantearse, no obstante, qué hubiese sucedido si el *hard fork* no hubiese sido posible, es decir, si los miembros de Ethereum no se hubiesen puesto de

---

16 El que realizó la sustracción lo interpretó literalmente, según vemos.

17 Cuando varios «mineros» terminan de forma consensuada la prueba de trabajo y remiten al sistema su bloque encabezado por el hash del mismo, algunos de los mineros reciben esa transacción, pero es posible que otros reciban la de otro minero que ha terminado su prueba de trabajo de una forma simultánea. De esta forma se produce un «tenedor» o bifurcación: se forman dos líneas de bloques, cada una con un hash distinto, por lo que se quiebra la condición unívoca del repositorio.

acuerdo, o si la modificación del código para evitar la transacción hubiese sido inviable. Seguramente, se habrían iniciado acciones de diversa naturaleza con el objetivo de la recuperación de los fondos.

5. Consecuencias jurídicas

Dividiremos las consecuencias jurídicas en tributarias y penales. En primer lugar, se estudiarán las consecuencias en la tributación, en sede de IRPF, de una eventual pérdida patrimonial causada por la modificación fraudulenta de *smart contracts*, para continuar el con análisis de las consecuencias penales de este tipo de conductas.

5.1. Consecuencias tributarias: deducción de pérdidas patrimoniales en el IRPF

Como hemos referido con anterioridad, en el caso The DAO no hubo pérdidas porque se pudo atajar la transacción gracias a que la cadena de bloques se bifurcó por la fuerza de una gran mayoría que rechazó la posibilidad de que se realizaran los pagos a la persona que modificó el código –aunque el consentimiento fuera prestado a los contratos inteligentes que contenían dicha modificación–, por mucho que una parte de los miembros se opusiera en defensa del principio formal de no intervención en los contratos autoejecutables.

Ahora bien, deberíamos plantearnos qué consecuencias, desde el punto de vista tributario, tendría una transacción de la misma naturaleza con éxito: ¿podría calificarse como pérdida patrimonial en el impuesto sobre la renta de las personas físicas (IRPF)? Lo cierto es que en un primer momento no sería posible. Desde la configuración legal de las ganancias y pérdidas patrimoniales, el importe de una operación, como la que habría tenido lugar, no constituiría de forma automática una pérdida patrimonial. Esto es así porque, en principio, la constitución de la DAO se realizó por los cauces apropiados, siendo modificado el *smart contract* en un único extremo: el de transferir fondos a uno de los miembros. La aportación de fondos a la DAO está correctamente realizada y se mantienen los derechos frente a ella. Así, solo en el caso de que el derecho de crédito frente a la DAO resulte judicialmente incobrable, será cuando se produzca la existencia de una pérdida patrimonial a efectos de liquidación del IRPF. Una vez que se entienda producida dicha pérdida, al tratarse de una pérdida que no se puso de manifiesto con ocasión de la transmisión de elementos patrimoniales, formará parte de la renta general, debiendo integrarse en la base imponible general del impuesto[18].

[18] Como señalan los artículos 45 y 48 de la LIRPF.

5.2. Consecuencias penales: hacia una eventual calificación de estafa informática

Los contratos inteligentes de *bitcoin*, por su autonomía, automaticidad y posibilidad de ejecución, suponen una importante revolución que afecta al ámbito jurídico en sus diferentes ramas, siendo imprescindible la puesta en marcha de una cobertura legislativa adecuada en cuanto al alcance y posibilidades dentro del mercado empresarial. En este sentido, una vez revisadas las consecuencias que a nivel tributario pudieran acontecer, se procede en este momento a matizar algunos de los aspectos que pudieran afectar al ámbito penal, comenzando por su relevancia y prosiguiendo por los posibles tipos penales implicados y su especial relevancia en el caso The DAO.

5.2.1. Consideraciones generales a nivel penal

Como parte del sistema de cadena de bloques[19], y más allá de la revolución que pudiera suponer la criptomoneda como parte de dicha tecnología, en los últimos años vienen a desarrollarse nuevas apuestas vinculadas, ahora, con los *smart contracts*. Definidos los contratos inteligentes como una nueva aplicación o servicio de la tecnología *blockchain*, y entendidos como programas ejecutables que responden a un conjunto de condiciones acordadas contractualmente, habría que decir que en los posibles efectos jurídicos, y principalmente penales, de esta nueva revolución, deben tenerse muy en cuenta los aspectos ya señalados anteriormente, a saber:

- Los acuerdos entre las partes se traducen a programación o lenguaje informático donde, a partir del cumplimiento de ciertas condiciones algorítmicas, se ejecuta la acción.
- Como todo acuerdo entre dos partes, genera un conjunto de obligaciones y genera un valor, siendo aquel de origen público.
- Existe un desconocimiento físico entre las partes, por lo que la confianza entre ellas para llegar al acuerdo se logra a través de la ya citada tecnología.
- No requiere de intermediarios, no siendo necesario el paso de instituciones financieras que lo controlen o den su «visto bueno», lo cual, pese a abaratar posibles intereses, también lleva añadida la necesaria consecuencia de la verificación de la otra parte (p. ej., firma digital) para asegurar los pagos en línea.
- Tiene un carácter descentralizado, siendo totalmente visible su código y no siendo propiedad de nadie. En el caso de servicios que sean centralizados, estos po-

[19] Basado en la función hash como tecnología criptográfica.

drían llegar a descentralizarse usando Ethereum, evitando así la existencia de una empresa intermedia que cobrase comisiones (p. ej., eBay).

- Puede ser creado tanto por personas físicas como jurídicas, de la misma forma que por programas informáticos que lo ejecuten de manera independiente, incluso por defecto.
- Se ejecuta automáticamente y de manera autónoma, independencia que se hace extensible a la comprobación de su veracidad.

La agilidad de los intercambios propia de este tipo de contratos, unida a su automaticidad, genera en el usuario una serie de beneficios ya aludidos, principalmente el hecho de no ser necesaria la autenticidad de veracidad del otro agente por tercera entidad (intermediario centralizado), no siendo necesario el registro para la certificación de la información que se trata. Así pues, mediante el intercambio de la información a nivel transaccional, la cadena de bloques va validando su contenido de manera sucesiva, consolidando así la cadena y permitiendo la identificación y ausencia de manipulación de forma retroactiva una vez queda grabada, lo que otorga una mayor fehaciencia y confianza para las partes implicadas.

En línea con lo anterior, y tomando como referente Ethereum como plataforma de cadenas de bloques más idónea o adecuada para llevar a cabo el tipo de intercambios u operaciones propias de los *smart contracts*, habría que tener en cuenta que el aseguramiento de las transacciones en la nueva era *business* tiene como objeto, precisamente, el de evitar cualquier tipo de acción ilícita que pudiera llevarse a cabo. De esta forma, los comportamientos delictivos se entienden que se verían minorados si no hay alteración de la fuente que «organiza» o «conviene» dichos contratos, incluso, que se vería disminuida si se reduce el número de intermediarios que son necesarios para garantizar la identificación y registro de los datos (p. ej., bancos). Ahora bien, ¿no se podría llevar a cabo ningún tipo de acción delictiva que afectase a los contratos? ¿Se podría llegar a defraudar a los usuarios? ¿Cómo localizar posibles agujeros? Todo ello se presenta a continuación.

5.2.2. Potencial delictivo en materia de *smart contracts*

Como se ha comentado con anterioridad, los conocidos como *smart legal contracts* facilitarían la ejecución automática de un contrato previa verificación de usuarios[20] ante la inexistencia de intermediarios, y lo harían, precisamente, con base en la existencia de una lógica programable basada en condiciones muy objetivas de los contratos, y que vienen a resultar en transacciones económicas. El problema que en estos casos pudiera llegar a plantearse redunda en la posible subjetividad de los contratos que se acuerdan en sus cláusu-

[20] Una forma de asegurar la veracidad de los intercambios sería mediante el envío de una clave generada entre las partes, firmando criptográficamente un contrato digital y dando así una mayor seguridad al usuario.

las, lo que vendría a justificar el porqué sería más adecuado hablar de un tipo de ejecución automática para un «borrador» contractual, pero no para el contrato en sí mismo.

En orden con lo anterior, las posibilidades que definen al dinero programable que pudiera venir derivado de los contratos inteligentes no siempre tienen resultados positivos, mejor dicho, aunque los efectos pudieran resultar beneficiosos para determinados agentes, la legalidad podría llegar a verse cuestionada. Así pues, y rozando el ámbito que afecta a la ilegalidad, sería importante analizar y conocer las posibles consecuencias que, tanto a nivel de persona física como jurídica, podrían derivarse.

Siguiendo a Tur Fáundez (2018, pp. 18 y 19), los citados contratos inteligentes permiten «la autoejecución del contrato de acuerdo con la programación preestablecida», lo que puede llegar a generar algunas dificultades y problemáticas diversas si no se informa suficientemente al consumidor de la complejidad de este tipo de contratos. De la misma forma, debe advertirse sobre el riesgo intrínseco que comporta el propio empleo de la criptomoneda como medio de pago. Igualmente, advierte el autor sobre las siguientes consideraciones: a) existe un conjunto de beneficios en su empleo por cuanto permite la abstención de la entidad financiera (plano o procedimiento ejecutivo más breve), y b) existe un acuerdo o hecho contractual que pudiera considerarse «relativo», siendo cuestionable si la autoejecución de este tipo de contratos sitúa al consumidor al frente de un «contrato real» o no, pues en todo caso podría considerarse un proceso *ex ante*.

En línea con lo anterior, como indican Wang *et al*. (2019, pp. 291 y ss.), «el contrato inteligente impone un rendimiento específico en usuarios anónimos sin centralización. Facilita la equidad de pago en el comercio al proporcionar transacciones irreversibles», a lo que añaden precisamente los efectos que ello pudiera tener en el ámbito jurídico, concretamente en lo que atañe a las actividades ilícitas o ilegales. Del mismo modo, especifican dichos autores que «los contratos inteligentes también se utilizan para actividades ilegales como el lavado de dinero y el *ransomware*. Dichos contratos incluyen contratos inteligentes criminales (*criminal smart contracts* o CSC) […], que pueden implementarse de manera eficiente en los lenguajes de *script* existentes».

Entrando de lleno en lo que algunos autores denominan como «tecnojurídica» (Tur Fáundez, 2018, p. 19), y de manera específica en lo que compete al ámbito penal, el campo de los delitos informáticos, así como todos aspectos que vienen a afectar de un modo u otro a componentes tecnológicos, este campo ha sido objeto de un importante debate y tratamiento en los últimos años. Así, precisamente por el crecimiento de la era tecnológica y la gran propagación de sus efectos, los tipos penales y las consecuencias jurídicas de aquellos no han ido sino respondiendo a las demandas sociales que tales medios han ido produciendo.

Con base en todo lo anterior, ni que decir tiene que también la idoneidad del *blockchain* vendrá determinada por la existencia de bienes digitales sobre los que se comprueba la idoneidad de lo pactado y se actúa (p. ej., «ceder A una cantidad de dinero a B si sucede C»,

para lo cual debe comprobarse si C ha ocurrido o no –sí/no–, mediante una información que esté disponible en un buscador y a la que se pueda acceder digitalmente).

Una exégesis exhaustiva de los diferentes tipos penales advierte sobre la inexistencia de un tipo delictivo específico dedicado a los delitos informáticos. Así, bien por atentar directamente contra el propio equipo tecnológico, bien por emplearlo como medio para la realización de la acción comisiva, lo verdaderamente cierto es que el Código Penal no refiere en un precepto exclusivo todo lo que compete al citado ámbito. De este modo, si bien es cierto que se han ido creando algunos tipos penales para albergar todas aquellas conductas de especial lesividad que atentasen contra bienes jurídicos vinculados con aquellos medios, lo verdaderamente cierto es que la mayoría de los tipos penales se han adaptado a los nuevos modos comisivos del siglo XXI. En esta línea, y dada la complejidad de los tipos delictivos que se vinculan a las nuevas tecnologías, no puede afirmarse que un único precepto recoja toda la diversidad de acciones vinculadas a los medios indicados, de manera que el Código Penal recoge todas aquellas conductas típicas vinculadas a las nuevas tecnologías de una manera transversal en sus diferentes tipos delictivos.

Para el caso específico que aquí se trata, y tomando como referencia las conductas típicas que podrían estar presentes en las acciones descritas con anterioridad, y que quedarían vinculadas a los *smart contracts*, lo cierto es que la seguridad, la autonomía, la velocidad y el ahorro de tiempo y coste propio de dichos contratos podrían llegar a verse cuestionados en el orden penal. Si bien se evita la intervención de un tercero, que sería el que verificaría lo sucedido –pues ya la programación informática permitiría obtener tal conocimiento–, lo cierto es que podrían llegar a producirse ciertas defraudaciones en el citado ámbito. Así pues, entendiendo que es posible la firma de contratos en el mundo físico sobre la base de ciertas irregularidades no constatadas, lo cierto es que también podría extenderse tal extremo al mundo digital, siendo más compleja su detección, precisamente, por la inexperiencia o desconocimiento del lenguaje de programación (p. ej., error o vicio en el código) y la irretroactividad ya aludida previamente.

Las posibilidades delictivas o el potencial criminal al que pudiera responder el hecho de convenir un contrato sobre cláusulas u obligaciones contractuales criminales son inmensas, más aún cuando, por regla general, existente un desconocimiento social elevado del lenguaje programador. De la misma forma, la ausencia de retroactividad o posibilidad de borrado de información en la cadena de bloques, ya aludida, hace que cualquier tipo de información registrada permanezca ilimitadamente, pudiendo acceder a ella desde cualquier parte del mundo y siendo un ejemplo evidente de su descentralización.

En resumen, lo cierto es que el desarrollo de nuevas aplicaciones digitales para la optimización de recursos ha venido de la mano de una incertidumbre a nivel legislativo, que pudiera llegar a cuestionar la seguridad jurídica dentro del siglo XXI. Es por ello que, ante el tipo de situaciones previamente aludidas, así como la que a continuación se analizará, lo que viene a plantearse es si la regulación actual podría llegar a abarcar todas aquellas conductas vinculadas a la era digital, o bien se hace necesario el desarrollo de una regulación jurídica más acorde a las nuevas demandas y modos comisivos, en definitiva, al posible y potencial *modus operandi*.

5.2.3. Aplicación específica al caso The DAO

Poniendo en antecedentes, baste advertir que el caso The DAO, y su significado como organizaciones autónomas descentralizadas y justificadas en la aplicación de contratos inteligentes, se basa en la ya citada descentralización, posibilidad de acumulación de capital (monedas digitales), autonomía e inmutabilidad del código gestionado, siendo precisamente el debate el qué sucedería si se interviniera dicho código. Como se comentó con anterioridad, las DAO, tras su inclusión en la cadena de bloques, no requieren de la intervención humana, no existiendo centro de decisión y situando este en los participantes. De esta forma, las decisiones tomadas por cada uno de estos se traducen en código y se ejecutan automáticamente sin supervisión humana.

En cuanto a la regulación jurídica para el caso The DAO, y partiendo del aprovechamiento de un error de código que permite a un participante un desvío de 50 millones de euros, una vez ya creado aquel como parte de la programación que hace nacer el *smart contract*, se cuestiona si el citado usuario, aprovechando un error ya existente, podría actuar de manera fraudulenta estafando al resto de beneficiarios que participaban del contrato. En este caso, los creadores originan un código erróneo que permitiría dicho desvío no visible a la mayoría de los participantes adheridos, error que es aprovechado de forma recurrente (llamada recursiva)[21].

[21] La Sentencia 326/2019 (NCJ064122) del Tribunal Supremo versa sobre unos hechos calificados como delito continuado de estafa y apropiación indebida. El acusado, actuando a través de una empresa de su titularidad denominada Cloudtd Trading, de la que era administrador único, y a través de la página web de dicha empresa, suscribió diversos contratos de «trading de alta frecuencia», en virtud de los cuales se comprometía a gestionar, a cambio de una comisión, *bitcoins* entregados en depósito, obligándose a reinvertir los eventuales dividendos y entregar al vencimiento del contrato las ganancias obtenidas.

La audiencia de instancia consideró probado que en el momento de concertar los expresados contratos el acusado tenía la intención de apoderarse de los *bitcoins* recibidos sin ánimo de cumplir sus obligaciones, sin realizar operación alguna, ni devolver cantidad alguna; por tanto, condenó al acusado como autor responsable de un delito continuado de estafa a penas de dos años de prisión e inhabilitación especial para el ejercicio del derecho de sufragio pasivo durante el tiempo de la condena, debiendo abonar las costas procesales. Además, le condenó a indemnizar en el valor de la cotización del *bitcoin* en el momento de la finalización de cada uno de sus respectivos contratos, más el interés legal, con declaración de responsabilidad civil subsidiaria de la entidad Cloudtd Trading. Contra esta sentencia se interpuso recurso de casación por la acusación particular, con un único motivo de casación por infracción de ley, al amparo del artículo 849.1 de la Ley de Enjuiciamiento Criminal, al entender indebidamente aplicados los artículos 110 y 111 del Código Penal. Los contratos suscritos se referían a la entrega de determinadas unidades de *bitcoins* y sostiene, dicha acusación, que los artículos 110 y 111 del Código Penal obligan a la restitución de la cosa en el mismo bien, por lo que lo procedente sería que la sentencia condenara al acusado a restituir los *bitcoins* sustraídos. Sin embargo, aun cuando la jurisprudencia del mismo Tribunal Supremo ha expresado la obligación de restituir cualquier bien objeto del delito, incluso el dinero, la sentencia señala que las víctimas del delito no fueron despojadas de *bitcoins* que deban serles retornados, sino que el acto de disposición patrimonial que debe resarcirse se materializó sobre el dinero en euros que, por el engaño inherente a la estafa, entregaron al acusado para invertir en *bitcoins*.

Bajo la perspectiva de que el «código es ley» en el ámbito del ciberespacio, se ampara el citado usuario para indicar la legalidad de la acción empleada, pero no es posible afirmar que el código venga a reemplazar a la ley o regulación jurídica existente o aplicable al ámbito digital. La ley es la misma extensible a dicho contexto. En este sentido, lo que viene a cuestionarse es la legitimidad de la acción por hacer uso de las funciones permitidas dentro del contrato, no habiendo existido ningún tipo de alteración por su parte. Podría plantearse entonces la nulidad del contrato convenido sobre la existencia de un error en el mismo con base en los fines para los que venía siendo destinado, ya que la modificación del código *a posteriori* supondría la intervención humana, lo cual es contraria a la filosofía propia del *blockchain* al afectar a la autoejecución, pese a que fuera consensuada (*hard fork*). Ahora bien, ¿y si no hubiera sido posible llevar a cabo tal modificación?

Desde el ámbito nacional, pudiendo cuestionar la calificación jurídica del caso desde el punto de vista de una posible defraudación, o bien acercarlo al campo de su consideración como «nulidad contractual», lo cierto es que habría que analizar detenidamente cuáles son los antecedentes, y cuáles serían los requisitos exigidos como para considerar la conducta de aquel usuario, un fraude.

Para poder analizar si efectivamente los hechos podrían admitirse bajo el calificativo de estafa *online* o fraude cibernético, debe examinarse si verdaderamente se reúnen todos los elementos necesarios. Por ello, y siguiendo el artículo 248 del Código Penal[22], como aspectos esenciales o más significativas para la valoración del precepto que enmarca este tipo de ilícito se hallan: a) el ánimo de lucro a partir del patrimonio ajeno, siendo el tercero el que realiza el desplazamiento patrimonial en perjuicio de sí misma o de un tercero, afectando así no solo al mismo patrimonio, sino también a las relaciones de confianza entre las partes y, b) el engaño bastante y suficiente, precedente o concurrente, que resulta en la producción de error en el sujeto que realiza la acción.

[22] Tal y como refiere el tenor literal del artículo 248 del Código Penal:

> 1. Cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno.
>
> 2. También se consideran reos de estafa: a) Los que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro. b) Los que fabricaren, introdujeren, poseyeren o facilitaren programas informáticos específicamente destinados a la comisión de las estafas previstas en este artículo. c) Los que, utilizando tarjetas de crédito o débito, o cheques de viaje, o los datos obrantes en cualquiera de ellos, realicen operaciones de cualquier clase en perjuicio de su titular o de un tercero.

A este respecto cabría advertir que, pese a la última modificación por Ley Orgánica 1/2019, por la que se modifica la Ley Orgánica 10/1995 del Código Penal, y a sabiendas de los objetivos que precedían el citado planteamiento de cambio en tal regulación, lo cierto es que, en lo que compete a la estafa informática en el ámbito que aquí se trata no se han producido cambios.

Por su parte, y atendiendo al tenor literal del apartado segundo en cuanto a su redacción más específica y acorde con lo que en este momento se valora, deben tenerse en cuenta las siguientes consideraciones:

a) Tal y como refiere el tipo: «Los que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro». Se aprecia por tanto la consecuencia jurídica ante una conducta de manipulación o artificio semejante para la transferencia patrimonial, afectando directamente a la buena fe que pudieran traer consigo las relaciones. Así, conforme a ello, vienen a obtenerse las siguientes consideraciones:

   - Parece obvio que la acción realizada por el usuario que se hizo con los 50 millones de dólares pudiera llegar a plantearse en tal sentido, más aún cuando el propio «engaño» viene a entenderse de forma amplia en cuanto crea error en cualquiera de sus modalidades, comprendiendo dentro de este el mero hecho de no hacer, o callar, del propio sujeto, y al cual siempre subyace intencionalidad[23].
   - No es inactividad lo que se produce, sino que se emplea una llamada recurrente a los activos, utilizando un agujero del código para el beneficio propio del que no se da constancia, pues, de haberse conocido tal extremo como presente en las «cláusulas», el contrato no se hubiera convenido.
   - La ocultación de dicho error permite la obtención de un importante beneficio patrimonial a costa de terceros usuarios participantes en el contrato.
   - De la misma forma, existe una evidente proporcionalidad como caracterización del engaño, así como su idoneidad en la producción del resultado, más aún cuando se hace compleja la revisión y comprensión de los códigos digitales, de su significado y de su efecto. Si bien, en este caso el engaño podría llegar a asemejarse a la astucia o inteligencia del sujeto, pudiendo advertir cómo determinados conocimientos más especializados en dicho ámbito le permiten llevar a cabo la acción.
   - La acción realizada mantiene la apariencia coherente y realista que caracteriza al contrato, pero precisamente porque del mismo error desconocían los creadores del código. No obstante, y pese a ello, la protección del resto de usuarios frente a un participante fraudulento pudo subsanarse de la manera previamente expuesta, adoptando las medidas necesarias para la compensación victimal.

[23] *Vid*. más información sobre intencionalidad en Cuello Contreras (2019, pp. 1-43).

- Conforme a lo anterior, el error en los participantes produce un conocimiento no verídico de la realidad contractual, esto es, del efecto de sus acciones en relación con las cláusulas pactadas, motivo que justifica el vicio en la voluntad.
- El perjuicio es autogenerado, pues se entiende que el mismo participante del contrato lo genera con sus acciones, si bien, sobre la base del citado error, explicando así la relación causal entre ambos.
- Finalmente, el ánimo de lucro se hace evidente con la suma de dinero adquirida paulatinamente por el estafador, resultado todo ello del aprovechamiento de la acción llevada a cabo por los restantes participantes del contrato.

b) Por su parte, señala el artículo 248.2 b) del Código Penal que «los que fabricaren, introdujeren, poseyeren o facilitaren programas informáticos específicamente destinados a la comisión de las estafas previstas en este artículo». Atendiendo a esta afirmación, si los creadores del código fuente que rige los contratos inteligentes hubieran actuado en tal sentido con la finalidad de estafar a usuarios sobre la base de un contrato ya engañoso, pudiera llegar a apreciarse este tipo penal, pero no es el caso.

En definitiva, ante la existencia de un contrato inteligente firmado públicamente del que se entiende su veracidad, incluso para los creadores, y visto el aprovechamiento sobre el error en el código de uno de los participantes que hace llamadas recurrentes a una previsible inversión automática, podría extenderse la aplicación del fraude informático al caso The DAO, todo ello sobre la base del silencio e intencionalidad de la acción engañosa de manera continuada sobre los activos patrimoniales de terceros que actuaban de buena fe[24].

6. Conclusiones

La modificación de *smart contracts* con finalidades fraudulentas puede suponer graves problemas para aquel que ha invertido un dinero en la operación, de una parte, nos encontramos con una materia que no se encuentra regulada –salvo en cuestiones de blanqueo de capitales–; de otra, la propia naturaleza material de los *smart contracts* conlleva que las transacciones sean difícilmente reversibles al ser autoejecutables y sin un control «humano» que verifique su licitud.

Esta complejidad se multiplica cuando nos referimos a las DAO, las organizaciones autónomas descentralizadas, que son un tipo de organización, creada a través de *smart contracts*,

[24] *Vid*. a este respecto, y con base en dicha posible calificación jurídica, el pronunciamiento del Tribunal Supremo analizado en Padilla Ruiz (2019).

que es a la vez autónoma –pues no necesita operadores humanos–, autosuficiente –tiene fondos propios– y descentralizada –dado que no existe un centro de decisión, un administrador–.

El caso paradigmático de los problemas que se pueden presentar se dio en la plataforma Ethereum, en la que se creó un fondo de capital riesgo de gestión descentraliza mediante *smart contracts*; una DAO cuya actividad se centraba en la inversión en *start-ups* relacionadas con *blockchain*. Se denominó The DAO y fue, en su momento, la mayor operación de *crowdfunding* de la historia.

Ocurrió el desastre: un miembro de la red Ethereum logró que se transfiriera moneda virtual por el valor de 50 millones de dólares de la DAO a su *wallet*. Lo hizo aprovechando la posibilidad de hacer una modificación a la programación del *smart contract*, que permitía incluir un bucle de retiradas de criptomoneda antes de que finalizara el tiempo y cerrar el proyecto y actualizar el balance. Se consiguió llamar recursivamente a la función de recuperación de su inversión y recuperó sus fondos reiteradamente, antes de llegar al paso donde el código verificaba el saldo del fondo DAO.

La programación permitía esta operación sin mayores truculencias, pero es evidente que regalarle todo ese dinero a ese señor no era la finalidad de la operación, lo cual supuso que se cerrara el *blockchain* antes de ese punto y se constituyera uno nuevo. No existió, entonces, la modificación, ni se produjo la transferencia de fondos, pero, para muchos, se vulneró el principio de automatización y no intervención humana que rige en el *blockchain*.

Las consecuencias, desde un punto de vista tributario, a un caso en el que una transacción de la misma naturaleza tuviera éxito, ¿podrían calificarse como pérdida patrimonial en el IRPF? En principio no lo sería, porque el importe no constituiría de forma automática una pérdida patrimonial. Esto es así porque la constitución de la DAO fue válida, siendo modificado el *smart contract* a efectos de transferir fondos a uno de los miembros. La aportación de fondos a la DAO está correctamente realizada y se mantienen los derechos frente a ella. Únicamente, en el caso de que el derecho de crédito resulte judicialmente incobrable será cuando se produzca una pérdida patrimonial, que formará parte de la renta general, debiendo integrarse en la base imponible general del impuesto, al tratarse de una pérdida que no se puso de manifiesto con ocasión de transmisión de elementos patrimoniales.

Por su parte, en lo que compete a nivel penal, se ha podido comprobar cómo el caso en cuestión puede llegar a considerarse una estafa digital o fraude informático, habiendo comprobado la adaptación de los elementos necesarios para su concurrencia en el caso The DAO. Así pues, se aprecia cómo, partiendo del aprovechamiento de un error de código, un usuario consigue que se desvíe una cantidad concreta de activos previamente introducidos por los participantes del contrato en cuestión. En este caso, se entiende el fraude mediatizado por el vicio en la voluntad, el cual viene a surgir del error ya indicado, y el cual conlleva el desplazamiento patrimonial de los activos de ciertos participantes a favor de uno de ellos. De este modo, se aprecian importantes distinciones con otros tipos delictivos, como pudiera ser el delito de robo.

Como se puede comprobar, el actuar de forma fraudulenta se hace eco en el ciberespacio a partir de sus múltiples modalidades, mostrando cómo, en este caso específico, los *smart contracts* también podrían llegar a sufrir las vulnerabilidades cibernéticas. Ello deja constancia de dos aspectos fundamentales: el potencial delictivo creciente que brinda el ciberespacio y la necesidad de optar por mayores mecanismos de prevención o estrategias de seguridad cibernéticas eficaces.

Referencias bibliográficas

Bellany y Hill (2016). Can the Blockchain Make Our Contracts Smarter? *Cyberspace Lawyer* NL 2, *21*.

Bourque, S. y Fung Ling Tsui, S. (s. f.). A lawyer's introduction to smart contracts. Recuperado de <http://www.crypto-law.com>. Consulta el 15 de diciembre de 2019.

Butler, Al Khalil, Ceci y O'Brien (2017). Smart contracts and distributed ledger technologies in financial services: keeping layers in the loop. *Banking & Financial Services Policy Report*, *36*(9).

Cuello Contreras, J. (2019). La intencionalidad como criterio de distinción entre la estafa y el ilícito civil. *InDret*, *2*.

Echebarría Sáenz, M. (2017). Contratos electrónicos autoejecutables (smart contract) y pagos con tecnología blockchain. *Revista de Estudios Europeos*, *70*.

Kost de Sevres, Chilton y Cohen (2016). The Blockchain Revolution, Smart contracts and Financial Transactions. *Cyberspace Lawyer* NL 3, *21*(5).

Lessing, L. (s. f.). Code Is Law. On Liberty in Cyberspace. Recuperado de <https://harvardmagazine.com>. Consulta el 20 de diciembre de 2019.

Merkle, R. (2016). DAOs, democracy and governance. *Cryonics*, *37*(4), 28-40. Recuperado de <http://alcor.org>. Consulta el 19 de diciembre de 2019.

Navarro Lérida, M. S. (2018). Gobierno corporativo, Blockchain y Smart contracts. Digitalización de las empresas y nuevos modelos descentralizados (DAO). *RDMV*, *23*.

Padilla Ruiz, P. (2019). Los Bitcoins no se restituyen a la víctima de estafa al no ser dinero. Giro radical de la doctrina del Tribunal Supremo. *Revista Aranzadi Doctrinal*, *10*.

Securities and Exchange Commission (SEC). Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO. Recuperado de <https://www.sec.gov>. Consulta el 12 de diciembre de 2019.

Tur Fáundez, C. (2018). *Smart contracts. Análisis jurídico*, Madrid: Reus.

Wang, Y., Bracciali, A., Li, T., Li, F., Cuia, X. y Zhaoc, M. (2019). Randomness invalidates criminal smart contracts. *Information Sciences*, *477*. doi <https://doi.org/10.1016/j.ins.2018.10.057>.