Revista de Estudios Europeos
Nº 70, julio-diciembre, 2017-69-97
Monográfico-Economía colaborativa
ISSN: 2530-9854. http://www.ree-uva.es/

CONTRATOS ELECTRONICOS AUTOEJECUTABLES (SMART CONTRACT) Y PAGOS CON TECNOLOGÍA BLOCKCHAIN[1]

Marina ECHEBARRÍA SÁENZ
Universidad de Valladolid

Resumen: La aparición de contratos en formato electrónico y autoejecutables es el resultado lógico del progresivo proceso de automatización en la distribución y en el internet de las cosas. Nuestro régimen legal integra sin dificultad este formato de contratación, pero conseguir un proceso totalmente automatizado implica recurrir a mecanismos de pago en red que no siempre se adaptan al tipo contractual. El uso del dinero electrónico y las monedas virtuales como el bitcoin cubren esta función pero la escasa o nula regulación de las monedas virtuales y su doble carácter de unidad de valor y unidad de cuenta dificultan la funcionalidad y seguridad jurídica del uso de las tecnologías Blockchain en formatos estandarizados y automatizados de contratación.

Palabras clave: contratos auto ejecutables, moneda virtual, bitcoin, blockchain, sistemas de pago, sistemas descentralizados, sistemas disruptivos.

Summary: The appearance of smart contract in electronic and self-executable format, is the logical result of the progressive process of automation in the distribution and on called “Internet of things”. Law integrates this contracting format without difficulty, but achieving a fully automated process involves using online payment mechanisms that are not always adapted to the contractual type. The use of electronic money and virtual currencies, such as bitcoin, cover this function, but the scarce or null regulation of virtual currencies and their double character, as a unit of value and a unit of account, make the functionality and legal security of the use of Blockchain technologies difficult in standardized and automated contracting formats

Key words: Smart Contracts, virtual currency, bitcoin, blockchain, payment systems, decentralized organizations, disruptive systems.

1 Este trabajo se inserta dentro de las labores del proyecto de investigación del Ministerio de Economía y Competitividad, DER2014-58744-R "Competencia y Distribución: nuevos retos en la sociedad globalizada y en contextos de crisis económica", bajo la dirección de las profesoras Echebarría Sáenz, Marina y Herrero Suárez, Carmen.

1. LOS SMART CONTRACT O CONTRATOS AUTO EJECUTABLES:

Los llamados Smart contracts, son en realidad lo que podríamos definir como contratos en formato electrónico y de carácter autoejecutable.

Aunque existe tendencia a identificar los Smart contract con formatos que usan la llamada tecnología de bloques (Blockchain), [2] lo cierto es que conforme a un patrón de neutralidad tecnológica podemos considerar como Smart contract 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 conlleva la ejecución automática del resto del contrato, sin que quepa modificación, bloqueo o inejecución de la prestación debida.

Así pues, sin perjuicio de que el pacto pueda ser escrito en lenguaje humano, al menos una parte del mismo será transcrito a un código de programación o formato electrónico que, propiamente, es un programa de ejecución. En él se definen las reglas y las consecuencias de las mismas, lo mismo que en todo contrato, pero a diferencia del contrato ordinario, una vez fijadas las reglas de ejecución, por ejemplo; la entrega de la mercancía en almacén se señala como evento desencadenante, el mecanismo de ejecución no dependerá de la voluntad de las partes, sino de un programa que actuará automáticamente cuando identifique las reglas de ejecución. Para que esta respuesta automática sea posible es necesario poder programar un pago que no dependa de una orden posterior a la ejecución de parte y es por esto es lo que la mayor parte de los Smart contract terminan apoyándose en la tecnología de bloques y ejecutando el pago en criptomonedas o monedas virtuales como el bitcoin[3] pero, en realidad, cualquier otro formato tecnológico sería igualmente admisible y funcional si cumpliera con las características citadas:

La gran ventaja de los Smart contracts es que sus scripts son susceptibles de programarse en serie con sencillez al almacenarse en una cadena de bloques o en protocolos compartidos por redes de ordenadores. Cuando se produce un evento desencadenante, contemplado en el contrato, p. ejemplo, registro de un documento de trazabilidad en frontera[4], se envía la transacción a una dirección concreta y la máquina virtual ejecuta los códigos de operación del script (o cláusulas) utilizando los datos enviados con dicha transacción; esta tarea ejecutada puede ser sencilla, como votar en un foro, más compleja, como ejecutar un pago por un servicio o realmente compleja como activar garantías por un préstamo, ejecutar una opción de futuro, liberar un legado o una subvención, etc. etc.

---

[2] La asociación es habitual debido a la promoción de este modelo de contratación por plataformas como Selachii o Stash.
https://www.oroyfinanzas.com/2015/11/que-son-contratos-inteligentes-smart-contracts/

[3] El término e identificación entre Smart Contract como "dinero programable" se atribuye a Nick Szabo en 1997. La identificación de las monedas virtuales, criptomonedas o criptodivisas como tal es término habitual en toda la literatura financiera.
http://ojphi.org/ojs/index.php/fm/article/view/548/469

[4] Echebarría Sáenz, J. A "La carta de porte emitida electrónicamente" en Comentarios a la ley de transporte terrestre, Duque Domínguez, J/Martínez Sanz, F. (Dir.) Aranzadi Thomson-Reuters, Pamplona 2010, págs. 185-212

Los contratos autoejecutables presentan evidentes ventajas, pues, una vez superada la complejidad inicial de la programación, operan de manera sencilla, rápida, inmodificable, con ejecución asegurada al no permitir el arrepentimiento y con la ventaja de que la operativa puede ser totalmente automatizada, incluida la perfección de los contratos sucesivos al contrato marco, lo que permite que sea una solución para el llamado internet de las cosas o para la economía digital automatizada que opera sin personas.[5]

1.1. Posibles Funciones del Smart contract:

Las aplicaciones posibles a este modelo de contratación son muy variadas. Se puede usar Smart contracts en múltiples transacciones, como:

- Préstamos; Si el deudor no efectúa un pago, el contrato automáticamente podría revocar las claves digitales que le dan acceso a los fondos o activar las garantías.
- Depósitos en garantía: Compras por internet; Verificada la entrega (registro del código de barras en destino, seguimiento del documento electrónico de trazabilidad, huella digital del receptor…) se libera el pago.
- Controles de gasto: liberación de subvenciones y/o pagos a proyectos previa entrega de certificados.
- Herencias y donaciones: liberación de los fondos, legados etc. ante el registro del certificado de defunción…
- Piscinas de voto multifirma (multi-signature voting pools)[6]: se efectúa un depósito en una parte de confianza para garantizar el cumplimiento de una transacción, sin que ninguna de las partes partícipes tenga acceso al mismo hasta que dos o más de las partes señaladas en el acuerdo aprueben la transacción, liberando con ello el depósito en favor de a la persona indicada como cumplidora o beneficiaria de la prestación bloqueada. El servidor que ejecuta nuestro software nunca recibe fondos de los usuarios, ni transmite los fondos de los usuarios, ni puede acceder a sus fondos ni tiene la posibilidad de cambiar el saldo de un usuario, revertir una transacción, o confiscar el dinero. Sólo puede retenerlo o liberarlo válidamente.
- **Dobles depósitos**: De forma parecida a la anterior, sólo que se elimina a los terceros como fuente de verificación. Las partes, comprador y vendedor realizan una transacción de depósito vinculada a un contrato inteligente. El programa tiene un tiempo determinado. Si las partes no cumplen lo programado el dinero se transfiere a una tercera parte, se "quema" en alguna dirección de la que no tienen clave privada de acceso,

5 La concepción de la empresa o fábrica que no nos necesita se atribuye a Gill y Pratt en 2008. Sobre esta base, visionarios como Vitali Butterin creador de ethereum en 2014 (www.ethereum.org), defienden el uso de tecnologías blockchain para la creación de Organizaciones autónomas descentralizadas (DAOs). Véase Swartz, Lana, "El sueño del Blockchain. Imaginando alternativas tecnoeconómicas mas allá del bitcoin" en Castells, M. et al. Otra economía es posible. Cultura y economía en tiempos de crisis. Alianza editorial, Madrid, 2017, págs.. 123-155.

6 http://opentransactions.org/wiki/index.php/Voting_Pools

por lo que hay un fuerte incentivo para cumplir en plazo y liberar el depósito.

- **Oráculo:** validación de cláusulas en contratos inteligentes. Es decir, se señalan fuentes de información externa para decidir si una parte del contrato se ha cumplido (el índice de cotización ha llegado a x, la solicitud de préstamo ha sido aprobada, el documento de trazabilidad de la mercancía indica llegada a destino…) y otra parte (p. ej. El pago) ha de ejecutarse. Un oráculo indica que hay una tercera parte de confianza que desencadena consecuencias en nuestro contrato.[7]

1.2. Régimen legal de los Smart contract

¿Plantean alguna duda de legalidad los Smart contract? Inicialmente y atendiendo al principio de libertad de forma (art. 51 C.Co.), que el consentimiento, objeto y causa de un contrato (art. 1261 .C.) 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 legal atendiendo al principio de equivalencia funcional entre los medios de expresión físicos y los digitales que se recoge en el art. 3 nº 6, 7 y 8 de la ley 59/2003 de firma electrónica y art. 326 de la ley de enjuiciamiento civil. Es cierto que el común de los humanos no somos capaces de interpretar directamente un código binario, pero no es menos cierto que poseemos máquinas para descifrarlos, y que podemos pactar simultáneamente los elementos del contrato en lenguaje humano y en lenguaje binario, de forma que se salven los posibles errores en el consentimiento. Es cierto, igualmente, que en determinados contratos será necesaria la plasmación en lenguaje humano de los términos del contrato autoejecutable para salvar el consentimiento de la parte, como ocurrirá necesariamente siempre que haya un consumidor implicado o si no existe una percepción directa de las cláusulas secundarias en cualquier contrato. Finalmente, es cierto que en caso de discrepancia entre el script o programa de ejecución y los términos pactados en lenguaje humano siempre se deberá dar prioridad a este último, que es el que finalmente recaba la manifestación de voluntad requerida por nuestro ordenamiento (art. 1261 C.C.), pero una vez manifestado el consentimiento, el pacto es susceptible de automatización y repetición estandarizada como contrato marco, y que la totalidad de los procesos de ejecución pueden ser automatizados sin reparo legal.

¿Constituye en problema la renuncia a la *exceptio non adimpleti contractus*, es decir, el carácter autoejecutable? Podría parecer que sí, ya que, en nuestros códigos, frente al incumplimiento de una parte cabe la excepción de incumplimiento, pero analizada convenientemente la situación la respuesta es negativa: la ejecución automática es una respuesta a un evento desencadénate que implica el cumplimiento por la contraparte de aquello que se ha considerado relevante. Lo único a lo que se renuncia en el sistema es al "derecho a incumplir" y este no se haya consagrado en nuestro sistema legal. Si podemos pactar cláusulas penales y sistemas de ejecución reforzados, ¿Qué ha de impedirnos

7 Crear "ecosistemas" de fiabilidad es el objetivo de algunas plataformas como Orisi http://orisi.org/

pactar un sistema que no nos permite incumplir una vez que la contraparte ha cumplido conforme a parámetros pre establecidos y libremente convenidos?

¿Plantea alguna duda el régimen legal en cuanto al momento del consentimiento, lugar de celebración, ley aplicable etc. etc.? Pues no, un contrato autoejecutable 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, se entenderá concertado conforma a la regla del 1262 C.C. y 50 C.Co., en el domicilio del oferente, seguirá la regla del art. 54 C.Co en lo referente el momento de la perfección, comúnmente las reglas de los art. 333 y 334 C.Co. para la transmisión del riesgo y seguirá lo dispuesto en el art. 3 del Reglamento Roma I en lo tocante a ley aplicable[8], y lo dispuesto en los reglamentos Bruselas I[9] y Bruselas I bis[10] a efectos de fijación de jurisdicción en los casos con componente Internacional.[11]

Así las cosas, el único problema reseñable es, por un lado el de solventar el cómo de la constitución de un contrato electrónico, para lo que existen múltiples compañías que aportan el bagaje técnico,[12] y el de completar la totalidad de la operación por medios electrónicos, ya que de otro modo, solo automatizaríamos una parte del proceso y siempre, finalmente, dependeríamos de

8 Reglamento (CE) n. 593/2008 del Parlamento Europeo y del Consejo de 17-6-2008 sobre ley aplicable a las obligaciones contractuales. En el mismo se consagra la autonomía de la voluntad como primera opción, no existiendo pacto el art. 4 b señala la ley del Estado de residencia habitual del prestador de servicio aunque el reglamento admite cláusulas de escape por existencia de vínculos más cercanos con el caso, y aquí en especial la opción del consumidor por acogerse a la normativa tutelar propia. En materia de compraventa, sin embargo, en defecto de pacto (art. 3), caben diversas posibilidades según se entienda que es una compraventa general (art. 4); ley del Estado del vendedor, un contrato de distribución; ley de residencia habitual del distribuidor, o venta mediante subasta; ley del prestador del servicio de subastas. Si es compraventa de servicios financieros se aplicará la ley del Estado del mercado (art. 4.1.h). En los supuestos de carácter mixto se aplicará la ley del Estado de residencia habitual de quien deba realizar la prestación característica del contrato (art. 4.2) pero siempre existirá cláusula de escape (art. 4.3) si el contrato presenta vínculos más estrechos con un ordenamiento distinto. Véase, Calvo Caravaca, A./Carrascosa González, J. "problemas de extraterritorialidad en la contratación electrónica" en Echebarría Sáenz, J. (Dir) *El comercio electrónico*, págs. 145-217. Vicente Blanco, D.J. "Problemas de jurisdicción competente y ley aplicable en los mercados electrónicos" en Velasco, Echebarría, Herrero (Dir) *Acuerdos horizontales, mercados electrónico y otras cuestione actuales de competencia y distribución*, Valladolid, Lex Nova Thomsom-Reuters, 2014, págs. 644-666. Y del mismo "medios electrónicos de pago y jurisdicción competente en supuesto de contratos transfronterizos en Europa", en Mata Martín, R./Javato Martín, A. *Los medios electrónicos de pago*, págs. 270-319.

99 Reglamento (CE) n. 44/2001 del Consejo de 22-12-2000, relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil.

10 Reglamento UE n. 1215/2012 del Parlamento Europeo y del Consejo de 12-12-2012, relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil.

11 A saber: libre elección de foro por elección expresa o sumisión tácita (sin paralización por excepción de Litis pendencia), y en su defecto será competente el juez del domicilio del demandado o del lugar de ejecución de la obligación (como foro de ataque). En materia de compraventa sin embargo, Bruselas I Bis consagra el principio de "fortaleza europea" que protege a los domiciliados en la UE frente a demandas del exterior, protegiendo de la ejecución de sentencias extranjeras y permitiendo la demandar en la UE a domiciliados extranjeros o la aplicación de foro exorbitantes, mientras que si resulta aplicable la Convención e Viena de 1980, esta resulta de aplicación prioritaria sobre las normas conflictuales anteriores.

12 Como ejemplos: BitHalo (https://bithalo.org/), BlackHalo (http://blackhalo.info/), Codius (https://codius.org/) Counterparty (http://counterparty.io/) Rootstock (https://www.oroyfinanzas.com/2015/10/rootstock-contratos-inteligentes-smart-contracts-ethereum-bitcoin/) Ethereum (https://www.oroyfinanzas.com/2015/07/ethereum-proyecto-bitcoin-2-0-mas-ambicioso-lanza-plataforma-descentralizada-frontier/) (www.ethereum.org).

la voluntad de cumplir de la contraparte si esta puede paralizar o bloquear la respuesta. El problema más evidente en este campo es el de asegurar un pago, por medios electrónicos, automatizado.

2. EL PROBLEMA DEL PAGO ELECTRÓNICO AUTOMÁTICO COMO FORMA DE EJECUCIÓN DE LOS SMART CONTRACT: DINERO ELECTRÓNICO Y CRIPTO MONEDAS VIRTUALES

Desde que la humanidad abandonó el trueque para adoptar el dinero como signo o medio de cambio, unidad de valor y sistema de medida de las cosas, éste y los restantes medios de cambio han sufrido una transformación notable. Comencemos por aclarar que, ***medio de pago.*** es todo aquello que tenga un poder liberatorio de las obligaciones, como el dinero, la permuta, las prestaciones de hacer o no hacer, los efectos de comercio, etc. etc.[13] Por el contrario**,** ***instrumento de pago*** es el vehículo empleado para hacer efectivo el medio de pago, y por tanto hablamos de monedas, cheques, letras de cambio, trasferencias, giros etc. Si a un instrumento de pago le añadimos el adjetivo electrónico estaremos indicando que para la satisfacción de la obligación se utilizan instrumentos o sistemas electrónicos para transferir a distancia el valor entre las partes acreedora y deudora. Por seguir la terminología de la Recomendación UE 97/489 de 30 julio. Instrumento electrónico de pago es aquel que permite a su titular efectuar transacciones (transferencias, retiradas de efectivo, pagos carga o descarga de dinero en dispositivos, etc.) mediante un mecanismo electrónico. Instrumento que se divide en dos categorías, a saber: instrumentos de pago a distancia e instrumentos de dinero electrónico. Por **instrumento de pago a distancia**: entenderíamos aquel que permite a su titular acceder a fondos depositados en cuenta en entidad de crédito por el que se autoriza el pago a un beneficiario domiciliado en otra cuenta, utilizando para ello códigos de identificación o pruebas de identidad (servicios de banca electrónica, sistemas de tarjeta de crédito o débito y tarjetas T&E). Por ***instrumento de dinero electrónico*** por el contrario entenderíamos al instrumento de pago recargable, distinto de un instrumento de pago a distancia, bien sea tal instrumento de carga una tarjeta o una memoria de ordenador en el que se almacenan electrónicamente los valores que permiten a su titular efectuar transacciones como la transferencia de fondos, el pago en entidades distintas del emisor o el reintegro de los valores.

A la vista de las definiciones podremos concluir que para realizar un contrato autoejecutable necesitamos un instrumento de pago electrónico y que los instrumentos de pago electrónico a distancia no nos resultan útiles, en la medida que requieran la autorización del pago, prueba de identidad y otros factores que excluyan el automatismo. Maticemos, no es que sea imposible pactar, por ejemplo, una transferencia electrónica de fondos que opere automáticamente ante

13 En nuestro Código civil el pago es el medio para promover la satisfacción debida a una obligación. El pago es pues genéricamente todo cumplimiento de una obligación debida, el *solvere* o liberación de la carga (art. 1157 C.C.). Los medios de pago admitidos se detallan en el art. 1156 C.C. (hacer, no hacer, permuta, compensación y entrega y dentro de estas últimas la entrega de dinero). Sin embargo, en sentido más popular pago se identifica con el cumplimiento de las obligaciones pecuniarias en dinero en las que cambiamos capital real (bienes o servicios) por capital monetario (dinero signo que lo represente). Aquí es donde la doctrina distingue entre el pago líquido o en moneda de curso legal y el pago que para el C.C. son fórmulas de dación en pago mediante medios de pago o signos representativos del dinero.

una señal convenida, es a fin de cuentas un mecanismo similar al funcionamiento de los créditos documentarios garantizados, pero factores como la aceptación de la orden de pago, el protocolo de identificación del cliente, la comprobación de fondos, la posible retirada de los mismos, los plazos de ejecución bancaria y de verificación, etc. etc. hacen que no haya oferta comercial financiera articulada para este modelo de contratación, y que se pueda abrir la puerta a vías de bloqueo a la ejecución del contrato, que por definición, atentan contra el espíritu y finalidad del tipo contractual. Sólo los mecanismos de entrega automatizados se adaptan a la finalidad del negocio y aquí están principalmente, los instrumentos de dinero electrónico o la entrega/trasferencia de valor por medios electrónicos articulada en criptomonedas virtuales, entendiendo por tales a las representaciones digitales de valor que pueden ser intercambiadas por medios telemáticos y que sirven como instrumento de cambio y/o unidad de valor o almacenamiento de valor pero que no tienen un estatus legal de respaldo como divisa pues no están garantizadas por ninguna jurisdicción, por lo que cumple con las citadas funciones solo por el acuerdo de la comunidad de usuarios en la que se utiliza.[14]

2.1. El dinero electrónico como instrumento de pago en los contratos autoejecutables.

El dinero electrónico se rige actualmente por tres bloques normativos básicos.

En **primer lugar** están la Directiva 2009/110/CE, de 16 de septiembre de 2009 sobre el acceso a la actividad de las entidades de dinero electrónico y su ejercicio, así como sobre la supervisión prudencial de dichas entidades,[15] y la ley 21/2011 de 26 de julio de dinero electrónico.[16] Conforme a dichas normas, dinero electrónico es todo valor monetario almacenado por medios electrónicos o magnéticos que represente un crédito sobre el emisor, que se emita al recibo de fondos, con el propósito de efectuar operaciones de pago según se definen en el artículo 2.5 de la Ley 16/2009, de 13 de noviembre,[17] de servicios de pago, y que sea aceptado por una persona física o jurídica distinta del emisor de dinero electrónico.[18] Conforme a dicha normativa el dinero electrónico es la representación digital de una divisa, como el euro, por lo tanto dinero en el propio sentido de la palabra pues goza del respaldo del sistema financiero.

El **segundo cuerpo** normativo que nos afecta es el de la propia concepción del pago que deriva del Código Civil y de Comercio. Por encuadrar el fenómeno

---

14 Siguiendo a Financial Action Task Force (FATF), Virtual currencies – key definitions and potential aml/cft risks, 2014.

15 por la que se modifican las Directivas 2005/60/CE (LA LEY 10372/2005) y 2006/48/CE y se deroga la Directiva 2000/46/CE.

16 BOE 27 julio 2011, que sustituye al régimen de Ley 44/2002, de 22 de noviembre, de medidas de reforma del sistema financiero y el Real Decreto 322/2008, de 29 de febrero, sobre el régimen jurídico de las entidades de dinero electrónico, que lo desarrollaba.

17 A saber, "una acción, iniciada por el ordenante o por el beneficiario, consistente en situar, transferir o retirar fondos, con independencia de cualesquiera obligaciones subyacentes entre ambos".

18 No entendiéndose en la categoría el valor almacenado en instrumentos que puedan utilizarse para la adquisición de bienes o servicios únicamente en las instalaciones del emisor o, en virtud de un acuerdo comercial con el emisor, bien en una red limitada de proveedores de servicios o bien para un conjunto limitado de bienes o servicios.

que ahora nos interesa acotar, para nuestro Código Civil las obligaciones *pecuniarias* pueden solventarse (pagarse), mediante pago en moneda o mediante medios de pago (signos representativos del dinero o daciones en pago). Entre los medios tradicionales de pago estarían los efectos de comercio (cheques, letras de cambio, pagarés, giros postales), la transferencia bancaria y el reembolso. Pero lo cierto es que la dación en pago es más amplia, y un medio de pago ordinario, o si se prefiere un instrumento de pago auténtico frente a quienes han defendido que la dación es una compraventa de crédito o una novación del crédito original. El debate doctrinal acerca de la naturaleza jurídica del pago oscilaba entre quienes lo consideraban un hecho jurídico (concepción romana) un acto jurídico (doctrina italo-germana del siglo XX), o un negocio jurídico. De este modo el pago se realizaría en ocasiones mediante un acto (p. ej. Abstenerse de hacer) o mediante un hecho que puede ser un negocio jurídico (p. ej. Entregar un cheque). Realizar un pago, por ello, podría ser tanto un acto unilateral como un negocio jurídico bilateral[19]. Y por ello un pago puede tener diversos objetos posibles (art. 1166, 1170, 1157 C.C.), pero no se admite el pago de una prestación mediante otra (art. 1166C.C.) o el pago fraccionado o diferido sin el consentimiento de la otra parte.

O dicho de otro modo, para pagar una deuda de dinero por otro medio distinto del dinero líquido hace falta el cometimiento de las dos partes. Existiendo consentimiento de las dos partes (art. 1166 C.C.) es licito extinguir una obligación mediante la entrega de medios de pago distintos del dinero, que extinguirán la obligación primitiva, eso sí, acogiéndose a lo dispuesto en el art. 1170 C.C. y en especial a lo dispuesto en su párrafo segundo, a tenor del cual "la entrega de pagarés a la orden letras de cambio u otros documentos mercantiles, sólo producirá los efectos del pago cuando hubieren sido realizados o cuando por culpa del acreedor se hubieren perjudicado. Entre tanto, la acción derivada de la obligación primitiva quedará en suspenso".[20] Para nuestro legislador decimonónico, sólo el pago en numerario en el sentido más estricto de la palabra era un medio de pago ***pro soluto*** o de plena eficacia liberatoria (1170.1 C.C.), mientras que los restantes medios sustitutivos del pago en dinero sólo eran medios de pago o daciones en pago sin efecto liberatorio inmediato o con efectos ***pro solvendo***, "salvo buen fin", que sólo realizan la extinción cuando demuestran ejecutarse correctamente (art. 1170.2 C.C.). Además, nuestro legislador explica que sólo el pago en moneda es de aceptación obligada por ser el dinero de curso legal, mientras que, para aceptar el pago mediante medios o instrumentos de pago, incluidos las representaciones del dinero (transferencias, cheques, etc.), hace falta el consentimiento de ambas partes para aceptar la fórmula de pago…. O como ocurre con frecuencia en la actualidad que una norma nos obligue a realizar el pago mediante instrumentos de pago.

Este rígido planteamiento inicial desapareció con la teoría nominalista del dinero y la desaparición del patrón oro o metal precioso o la convertibilidad de la moneda en metal precioso: primero se admitió como dinero con efectos de pago

19 El tema es arduo. Véase Nussbaum, *Teoría jurídica del dinero*, Madrid, 1929 (Traducción Sancho Seral) para las posicione nominalistas clásicas europeas y Bonet Correa, J. *Las deudas de dinero*, Madrid, Civitas, 1981 para una revisión más cercana al modelo actual. Específicamente Echebarría Sáenz, J. A., "El dinero electrónico; construcción del régimen jurídico emisor-portador" en Mata/Javato, Los medios electrónicos de pago, págs. 219-267.

20 Con mayor extensión, Echebarría Sáenz, J.A., "El dinero electrónico: construcción del régimen jurídico emisor-porteador" en Mata Martín, R./Javato Martín A. *Los medios electrónicos de pago*, Granada Comáres, 2007, págs. 219-267.

pro soluto al pago en billetes (convertibles en monedas), luego al pago en monedas y billetes no convertibles en metal precioso, después al pago en dinero bancario, y ya con la directiva 2000/46, cuando se nos dice que un euro digital equivale a un euro en moneda-divisa con equivalencia-paridad y convertibilidad, se nos dijo que el pago en dinero electrónico equivalía al pago en euros nominales ordinarios, y por tanto, que también era un pago con *efecto solutorio inmediato o pro soluto* (art. 1170.1 C.C.), pero no nos dice que sea dinero de curso legal, puesto que es un instrumento electrónico de pago.[21] Es decir, el dinero electrónico regulado en la directiva 110/2009 y en la ley 21/2011 es dinero de curso legal en forma digital y por ello dinero convertible de emisión privada, pero autorizada y supervisada por la autoridad financiera (Banco Central Europeo y bancas centrales nacionales), lo mismo que el dinero bancario. Las entidades emisoras de dinero electrónico han de cumplir con requisitos legales y de solvencia tasados, y a cambio de su registro y supervisión gozan de una exclusión de denominación en el uso del término "dinero electrónico". El dinero electrónico es una reproducción en el ámbito digital de los efectos del dinero tradicional y por ello una moneda oficial o divisa aunque su emisión sea privada y en formato electrónico. Ahora bien, con mayor claridad, al no declararse que la moneda digital de euro sea moneda de curso legal o pago en líquido, sino instrumento de pago, no es de aceptación obligada, lo mismo que no lo es el pago en dinero bancario como instrumento de pago[22], pero se incluiría en el art. 1170.1 del C.C. y no en el párrafo segundo del mismo precepto: Se puede aceptar el pago en euros digitales o no, pero de ser aceptados la entrega de los mismos produciría un efecto solutorio inmediato. Dicho esto, es igualmente necesario aclarar que la concepción del dinero liquido o de curso legal como medio de pago de aceptación obligada está en clara crisis, primero desde que las propias administraciones públicas decretaran por ley la aceptación obligada de sus pagos por medio de dinero bancario y finalmente impidieran el pago en nominal a sus propios funcionarios y contratantes, y después desde que la normativa sobre control fiscal y blanqueo de capitales restringiera el pago en nominal a 3000 € y el uso de billetes de 500 €, obligando a que la mayor parte de las transacciones mercantiles se hagan por instrumentos de pago con apoyo en Cuentas Corrientes bancarias.[23] No es exagerado decir que la inmensa mayoría de los pagos de deuda dineraria en España se realizan por medio de anotaciones bancarias.

El **tercer bloque normativo** es el que aporta la ley 16/2009 de 13 de noviembre de servicios de pago, que tiene origen en la Directiva 2007/64 sobre servicios de pago,[24] derogada por Directiva (UE) 2015/2366 del Parlamento

21 La argumentación es compleja y larga y ahora no procede. Para ello, Echebarría Sáenz, J. "El dinero electrónico…. Págs. 248 y ss. En especial 261-266.

22 Dicho esto, aclarar que hablamos de las relaciones entre particulares y que aquí cabe pacto en contrario, o que, como ocurre con el pago por las administraciones públicas, que estas hayan establecido por ley la obligación de aceptar el pago mediante anotación de dinero bancario.

23 Principalmente RD 304/2014 de 5 de mayo en desarrollo de la ley 10/2010 de 28 de abril de prevención del blanqueo de capitales y la financiación del terrorismo. Véase http://www.sepblac.es/espanol/legislacion/norma-blanqueo.htm

24 Directiva 2007/64/CE del Parlamento Europeo y del Consejo, de 13 de noviembre de 2007, sobre servicios de pago en el mercado interior por la que se modifican las Directivas 97/7/CE, 2005/65/CE y 2006/48/CE. También interesa Reglamento (CE) n o 924/2009 del Parlamento Europeo y del Consejo, de 16 de septiembre de 2009, relativo a los pagos transfronterizos en la Comunidad y Libro Verde de la Comisión, de 11 de enero de 2012, titulado «Hacia un mercado europeo integrado de pagos mediante tarjeta, pagos por internet o pagos móviles»,

Europeo y del Consejo de 25 de noviembre de 2015 sobre servicios de pago en el mercado interior (DSP2),[25] así como el Reglamento (UE) n o 260/2012 del Parlamento Europeo y del Consejo, de 14 de marzo de 2012, por el que se establecen requisitos técnicos y empresariales para las transferencias y los adeudos domiciliados en euros, y se modifica el Reglamento (CE) n o 924/2009 . Esta normativa regula los servicios como transferencias, los adeudos directos y las operaciones de pago directo efectuadas mediante tarjeta. Estas normas unifican los derechos de los usuarios de los servicios de pago en el SEPA (Single Euro Payment Area) e incluso puede aplicarse a pagos en los que uno de los operadores reside fuera del espacio económico europeo, todo ello bajo la supervisión del Banco Central Europeo y de los Bancos Centrales Nacionales. La Ley establece la reserva de actividad para prestar los servicios de pago en favor de los proveedores que se enumeran como posibles prestadores de forma exhaustiva. Se trata de las entidades de crédito y de las nuevas entidades de pago, cuyo régimen jurídico se establece en el Título II, y que quedan sometidas a una regulación similar a la bancaria y bajo la supervisión, en nuestro caso, del Banco de España. La ley de servicios de pago establece un estatuto de derechos de los usuarios, *irrenunciable* (plazos de ejecución, información precontractual, limitaciones en las condiciones de cobro por servicio, etc).

Pues bien, la ley de servicios de pago se aplica a la ejecución de operaciones de pago incluidas las transferencias y domiciliaciones, pagos por tarjeta y dispositivos similares, la emisión y transmisión de instrumentos de pago (por ejemplo dinero electrónico) y en especial, "La ejecución de operaciones de pago en las que se transmita el consentimiento del ordenante a ejecutar una operación de pago mediante dispositivos de telecomunicación, digitales o informáticos y se realice el pago a través del operador de la red o sistema de telecomunicación o informático, que actúa únicamente como intermediario entre el usuario del servicio de pago y el prestador de bienes y servicios" (art. 1 LSP). Conviene señalar que el art. 4 de la LSP otorga reserva de actividad a las entidades de crédito, de dinero electrónico del artículo 1.1 b) del Real Decreto Legislativo 1298/1986, de 28 de junio y demás entidades admitidas (entidades de pago, correos, administraciones públicas) prohibiendo prestar, con carácter profesional, cualquiera de los servicios de pago enumerados en el artículo 1 a quienes no sean operadores autorizados e inscritos (art. 6 LSP). El Banco de España, en ejercicio de sus funciones de vigilancia del funcionamiento de los sistemas de pago se encargará de supervisar el cumplimiento de lo establecido en este artículo, resultando de aplicación lo establecido en el artículo 16 de la Ley 13/1994, de 1 de junio, de autonomía del Banco de España. La condición de entidad de pago implica que se dispone de los requisitos de capital y recursos propios exigidos por la ley, un control de concentración de riesgos y unos coeficientes de solvencia y liquidez tasados.

Una entidad de pago, finalmente, puede prestar servicios operativos o servicios auxiliares como la garantía de la ejecución de operaciones de pago, servicios de cambio de divisas, actividades de custodia y almacenamiento y tratamiento de datos y sobre todo, la gestión de sistemas de pago. Todo lo cual las convierte en sujetos aptos para establecer mecanismos de ejecución automatizada de pago.

25 y por la que se modifican las Directivas 2002/65/CE, 2009/110/CE y 2013/36/UE y el Reglamento (UE) no 1093/2010 y se deroga la Directiva 2007/64/CE

Esta introducción es necesaria para explicar, que, por efecto de la normativa comunitaria y nacional sobre la materia, la entrega del llamado dinero electrónico o instrumento de dinero electrónico, hoy regulado por la ley 21/2011 tiene un régimen jurídico concreto y un reconocimiento oficial, y por tanto una seguridad jurídica, además de la ya mencionada paridad de cambio y convertibilidad.

Si, como indica la ley 21/2011, entre las funciones del dinero electrónico está la de articular prestación de servicios de pago (art. 8.1 a LDE) todo nos indicaría que la solución más evidente a la automatización del pago en un *Smart contract* sería el dinero electrónico, ya que es más difícil pensar en la articulación de un mecanismo de pago irrevocable por sistema de trasferencia, domiciliación o pago por tarjeta. El dinero electrónico nos aportaría un medio de pago con estabilidad (la misma que la moneda real que representa), convertibilidad garantizada, garantía de solvencia razonablemente asegurada por la autoridad de supervisión financiera, reconocimiento legal y adaptación al medio electrónico por su propia naturaleza. Entre los inconvenientes sólo podríamos contar el de necesitar fondos previo para la conversión de euros "normales" en euros digitales, pero la superposición con mecanismos como la apertura de crédito salvarían este obstáculo.

¿Qué es lo que explica entonces que la inmensa mayoría de las plataformas de contratación automática no usen la moneda digital de curso "legal" (o más bien reconocido como instrumento de pago) y en su lugar se la jueguen con criptomonedas de emisión privada (bitcoins, ethers, y otras de las 1200 criptodivisas existentes), sin reconocimiento legal, frecuentemente inestables por su función especulativa,[26] y sin supervisión ni garantía de solvencia de la autoridad financiera? Cuando expliquemos el funcionamiento de estas plataformas, se entenderá mejor las ventajas que ofrecen, pero de momento baste con indicar que el principal motivo por el que las plataformas de contratación automática no siempre usan dinero digital, es por la escasez de oferta comercial. El sector de la emisión de dinero electrónico está fuertemente bancarizado y las entidades de crédito no terminan de lanzar y promover este instrumento de pago en la dimensión que su potencial aporta. A día de hoy, cuesta articular un sistema de pago automatizado en euros digitales porque las entidades de pago, mayormente entidades de crédito, siguen dando prioridad a los instrumentos de pago a distancia que implican la necesaria posesión de una cuenta corriente y el pago de comisiones por transferencia o tarjeta, que les resultan enormemente lucrativas. Mientras tanto, las criptomonedas de emisión privada han ido ocupando el hueco que el sistema legal no ha querido o no ha sabido llenar.

Por el contrario, el pago en las cripto monedas de creación privada que han ido sucediéndose desde los años 80 del siglo XX nos plantean una duda de encuadramiento jurídico fundamental.

26 AA.VV. Polasik-Piotrowska-Wisniewski-Kotkowski-Lightfoot, "Price Fluctuation and the use of Bitcoin", en *International Journal of Electronic Commerce*, Vol. 20, n. 1, 2016, 9.

2.2. La aparición del Bitcoin y restantes criptomonedas virtuales con tecnología Blockchain:

Previamente a la exposición propuesta conviene explicar que el intento de crear monedas virtuales ya es antiguo y se remonta a los años noventa del siglo XX. Diversos emisores intentaron crear divisas virtuales (mondex, liberty reserve dollars, e-gold, second life linden dollars, webMoney) con resultados diversos, pero mayormente fallidos.[27] Entre los factores que precipitaron al fracaso la mayor parte de estos intentos se pueden señalar:

- Factores técnicos, como el de asegurar al cliente frente al riesgo de doble pago
- Factores sistémicos; como el de asegurar la viabilidad del sistema ante subidas o bajadas repentinas en el uso del sistema que requerían fondos de estabilidad y mecanismos de contención que los emisores no tenían.
- Factores especulativos: como el de fijar la cotización de la moneda virtual en relación a las restantes divisas de cambio logrando una estabilidad en el cambio.
- Factores institucionales: en concreto la personalidad del emisor y el alcance de las garantías que podía ofrecer al sistema. La mayor parte de estas monedas digitales fueron emitidas por compañías que carecían de recursos para poder actuar como un regulador-emisor monetario con garantías y que por ello se vieron desbordados por la evolución del sistema. Otras fueron finalmente abordadas como un sistema ilícito de encubrimiento y blanqueo de capitales.[28]

Tener presente estos factores es útil para valorar los pluses y las debilidades que ofrecen las criptomonedas en sistema blokchain.

La base tecnológica de los Blockchain reside en la combinación de los sistemas de comunicación Peer to Peer (puerto a puerto) con los sistemas de firma o acreditación por mutua confianza que aparecen con el sistema PGP (*Pretty Good Privacy*) en los años noventa. [29] La propuesta de usar un sistema de acreditación mutua basada en el consenso y en la computación criptológica para crear un instrumento de pago no oficial se atribuye a Satoshi Nakamoto (que es un pseudónimo) en 2009[30]. La propuesta de Nakamoto fue polémica y genero tanto entusiasmo en la red como perplejidad y rechazo en el sistema financiero.[31] El

27 Mateo Hernández, J. L., El dinero electrónico en Internet Aspectos técnicos y jurídicos. Granada, Comares, 2005. FATF. Guidance for a risk-based approach, Virtual Currencies, 2015

28 FATF. *Guidance for a risk-based approach, Virtual Currencies*, 2015.

29 Creado por Phil Zimmerman en 1991 utilizando los sistema de criptografía asimétrica o de clave pública. Véase https://es.wikipedia.org/wiki/Pretty_Good_Privacy

30 Nakamoto Satoshi, (pseudonimo), Bitcoin: "A Peer-to-peer Electronic Cash System", 2008, https://bitcoin.org/bitcoin.pdf

31 European Central Bank, Virtual Currency Schemes, Report, october 2012, in www.ecb.europa.eu/pub/
pdf/other/virtualcurrencyschemes201210en.pdf (e informes posteriores año por año).
febbraio 2015, in www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf;

desarrollo temprano del sistema ahondo en la polémica, máxime tras la desaparición de varios millones de dólares del sistema y la detención en Tokio de un programador alemán del que se sospechaba como posible personalidad de Nakamoto. A día de hoy y tras varios años de instrucción no se ha sabido determinar con claridad si fue un fraude por un ataque de computación, una apropiación indebida del procesado o el fallo de un sistema que entonces todavía estaba en rodaje inicial. Lo cierto es que este y otros escándalos no han impedido el desarrollo y progresión de la plataforma de pago bitcoin y el nacimiento de otras alternativas basadas en la misma tecnología, ni que, con el paso del tiempo, el sistema haya demostrado ser viable y computacionalmente resistente.

Bitcoin propiamente es un protocolo o programa descargable en cualquier ordenador que crea una plataforma descentralizada y sin intermediarios ni autoridad de supervisión, para la conclusión y gestión de transacciones de cambio (bitcoins) creando un ecosistema digital. El objetivo del protocolo Bitcoin es la transmisión de bitcoins; "moneda digital" creada por el propio sistema al que se atribuye valor de cambio por aceptación de terceros que se afilian al sistema contable bitcoin. El sistema contable bitcoin resultó ser rápido y computacionalmente confiable desde el momento en que no ha habido un numero de errores de sistema que lo hayan puesto en riesgo, o al menos no lo bastante como para provocar la huida del sistema. En la actualidad bitcoin supera los noventa mil millones de dólares en valor y crece diariamente:[32] Bitcoin, además ha resultado ser no sólo un medio de pago electrónico automatizable sino también un instrumento de inversión especulativa[33], un instrumento de evasión fiscal, blanqueo de dinero y facilitación de operaciones en negro[34], lo que aumenta su carácter polémico exponencialmente. Sin embargo, para hacer un juicio ecuánime del sistema es necesario analizar con más profundidad su funcionamiento, sus virtudes y sus riesgos.

Banco central Europeo: Opinion on virtual currencies, Report, 4.7.2014, in www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+ Opinion+ on+ Virtual+ Currencies.pdf asi como advertencias de prácticamente todos los bancos centrales europeos. Un resumen de posiciones en informe FATF. *Guidance for a risk-based approach, Virtual Currencies*, 2015.

32 https://blockchain.info/en/charts/market-cap

33 Instrumento especulativo altamente volátil según los estudios: Polasik-Piotrowska-Wisniewski-Kotkowski-Lightfoot, "Price Fluctuation and the use of Bitcoin", en *International Journal of Electronic Commerce*, Vol. 20, n. 1, 2016, 9.

34 FATF. *Guidance for a risk-based approach, Virtual Currencies*, 2015

2.2.1. La Tecnología de la cadena de bloques: funcionamiento de bases de datos descentralizadas o distributive ledger

Desde la aparición del dinero contable o dinero bancario,[35] todo sistema de contabilidad se ha orientado a impedir el doble cómputo o doble pago de una anotación. En una transacción ordinaria el dinero sólo existe en una ubicación, o en nuestro bolsillo o en el del vendedor. Ni podemos gastar el mismo billete dos veces ni podemos tenerlo en dos sitios. Los bancos en sus sistemas contables emulan este mismo comportamiento, las retiradas de dinero se emulan contablemente mediante un sistema de anotación-desanotación contable en debe y haber. La compensación automática previene del doble gasto o del doble apunte. [36]

La actividad de control frente al doble pago es relativamente fácil cuando hay una autoridad central supervisora del sistema y es responsable de la emisión de la moneda contable, es decir, un sistema público de respaldo que cumple con las funciones de supervisión y garantía del sistema. La novedad, y dificultad que presenta bitcoin y los sistemas similares, es la de que no existe dicho intermediario-supervisor: son los propios usuarios del sistema los que supervisan y admiten las operaciones, cada operación, a través de un sistema difuso de acreditación mutua. El control es posible gracias a la existencia de una base de datos única, de construcción colectiva, compartida por todos los nodos (o "mineros")[37] que utilizan el sistema. Así, los usuarios autorizados introducen cada operación usando un protocolo común y respetando una línea temporal de marcado que evita la retroactividad y exige la coherencia de cada operación con las anteriores. El protocolo busca acreditar la certeza de la operación, su unidad y su inmutabilidad mediante una prueba de trabajo computacional que consiste en la resolución de complejos algoritmos y que debe ser confirmada a su vez por otros operadores del sistema. Las operaciones confirmadas por el sistema se integran en un bloque de computación que son base de las siguientes y van quedando sepultadas por las posteriores en una cadena interminable de operaciones superpuestas (cadena de bloques o blockchain). El resultado es tal que, alterar la base de datos retroactivamente, exigiría una capacidad computacional casi imposible de obtener, hoy por hoy, pues supone la necesidad de superar como mínimo el 51% del poder computacional de todos los miembros del sistema. El conjunto genera así una estructura de control, sin gobierno, que minimiza el riesgo de manipulación por uno o varios usuarios, pues las modificaciones exigen una operación idéntica de sentido contrario que exigiría el consentimiento de todos los partícipes. La totalidad de la red puede supervisar y comprobar el sistema y controlar la coherencia contable de la cadena, por lo que no cabe una intervención directa que altere sus términos.

El sistema se basa pues en la mutua acreditación de confianza. Es el consenso mayoritario de los usuarios el que acredita la legitimidad de una operación y la última versión del **registro blockchain**. Registro blockchain en el

35 Bonet Correa, J. *Las deudas de dinero*… Cit.

36 https://www.oroyfinanzas.com/2013/10/bitcoin-block-chain/

37 Se llama mineros al individuo o entidad que participa en una red descentralizada de divisas virtuales utilizando un software especial para resolver complicados algoritmos en una prueba de trabajo distribuida o sistema distribuido de prueba/verificación usado para validar las transacciones y anotaciones contables del sistema de moneda virtual. FATF *Virtual Currencies key definitions*… 2014.

que los sucesivos bloques de computación que se añaden por los "mineros" de datos (nodos) a la cadena se refresca cada 10 minutos gratuitamente y sin interrupción. Así cualquier elemento del sistema puede introducir un dato-transacción en el mismo, pero la existencia y veracidad de la transacción no está aún verificada. La veracidad de la operación en un sistema descentralizado se constata cuando la transacción se inserta en un blockchain y luego se crean nuevos bloques sobre este, que van confirmando la transacción que hemos realizado. Una operación no es refrendada hasta que al menos seis nodos o mineros la refrendan. Al conseguir ser verificado por más elementos del sistema e incorporarse a la cadena la estructura del sistema asume como "verdaderos" aquellos bloques de la cadena más larga que tengan 5 o más bloques encima del mismo. Un bloque que se haya extendido con 5 bloques más muestra un total de seis confirmaciones como mínimo. Una bolsa de cambio de valor, como es Bitcoin, no se puede exponer al riesgo del doble gasto. Por eso solo puede transferir los bitcoins a la cuenta de un cliente cuando se haya confirmado como "verdadera" y, es precisamente por eso, que ignorará los bloques hasta que no sean parte de la cadena más larga y tengan más de seis confirmaciones. Una copia completa de la blockchain (registro blockchain) contiene todas las transacciones ejecutadas en la divisa y con esa información uno puede saber qué valor ha sido propiedad de cualquier dirección en cualquier momento desde la existencia de la base de datos. [38] Bitcoin, pues se basa en la trazabilidad de la divisa electrónica desde su origen para asegurar su valor. Cada bloque tiene un hash o huella electrónica desde el génesis hasta la actualidad y permite un orden cronológico que impide el doble pago (tendrías que modificar todos los bloques anteriores). El sistema prima la generación honesta en la que la cadena más larga, por su dificultad combinada, [39] y por su mayor respaldo computacional, es más fiable. Una cadena es válida si todos sus bloques previos son confiables y permiten el acceso hasta el génesis. Para cualquier bloque de la cadena solo hay un camino al génesis block.

Este sistema de refrendo colectivo resulta ser sorprendentemente fiable, pero aquí hay que señalar un riesgo del sistema: En un momento dado puede haber dos o más bloques al mismo nivel, con contenido contradictorio y compitiendo por procesar la misma transacción y convertirse en el próximo bloque de la Blockchain, son los llamados **forks** bifurcaciones u orquillas[40] que se crean cuando dos bloques son creados con solo unos pocos segundos de diferencia. Este fenómeno no debe confundirse con el de la aparición de plataformas falsas (Scrum) que simulan la computación de bitcoins para recabar inversiones fraudulentamente. [41] En este caso nos referimos a la aparición de una orquilla que pone un valor bitcoin en conflicto entre dos potenciales titulares. Cuando pasa eso, los nodos siguen construyendo la cadena sobre el bloque que hayan recibido primero. Los bloques de cadenas más cortas no serán validadas y finalmente serán desestimadas: todas las transacciones que forman parte de la

38 https://www.youtube.com/watch?v= 8zgvzmKZ5vo

39 https://www.youtube.com/watch?v= 9V1bipPkCTU

40 https://www.youtube.com/watch?v= Lx9zgZCMqXE

41 Como ejemplo local la moneda virtual unite de Unetenet que resultó ser un fraude de mas de 50 millones. véase www.bolsamania.com/noticias/tecnología/que-es-el-unete-una-estafa-de-50-millones-de-euros-a-partir-del-bitcoin-de-jose-manuel-ramirez--771685.html
www.noticiasespanolas.es/index.php/483471/prision-para-los-dos-fundadores-de-unete-la-estafa-de-la-moneda-virtual-espana/
www.lasexta.com/noticias/sociedad/detienen-responsables-estafa-piramidal-unetenet_2015102657245f4d6584a81fd882a0f7.html

cadena corta se reagrupan en las transacciones pendientes y se incluyen en otro bloque. La recompensa para los bloques en la cadena más corta no estarán en la cadena más larga, por lo que estarán perdidos en una lista RPCCall[42].

Esta es la razón por la que la red obliga un "tiempo de maduración" de 100 bloques para la generación de bitcoins que remunera la labor computacional de los "mineros". El tiempo de maduración de un bloque se aplica para los bloques nuevos generados por los mineros de Bitcoin como medida de seguridad para evitar el doble uso de bitcoins: un nodo minero de datos no podrá gastar o pagar nada con sus bitcoins generados, hasta que su bloque esté a 101 bloques del bloque de más reciente creación.

Para aquellos supuestos en los que surge disputa sobre la titularidad del valor o la validez de una transacción, sin embargo, se ha creado un sistema de resolución de conflicto que resulta igualmente eficaz y coherente con el sistema. En la última versión del protocolo se introdujo el sistema multifirma (*multi signature*), que sustituye al primitivo sistema de resolución de conflictos por vía judicial o por un árbitro externo al sistema.[43] Así, si aparece un conflicto sobre un fondo (titularidad de un bitcoin) con el sistema multi-sig, este quedará bloqueado en manos de un tercero que hará las funciones de árbitro en caso de controversia. La operación finamente aprobada puede quedar con ello subordinada a la acreditación de la misma por un número pre establecido de sujetos interesados/involucrados. El sistema, en definitiva, otorga en caso de controversia sobre la titularidad de un bitcoin entre a y b, a quien C o más acreditadores apoyen como parte vencedora del litigio, sin que ninguna de las partes, árbitro/s incluidos, puedan disponer del fondo hasta que se produzca dicho consenso.

Y dicho esto, el sistema arbitral puede dirimir la cuestión de la titularidad sobre un bitcoin, o sobre la legitimidad de una cadena, si se prefiere así, pero eso no impide que los titulares de la cadena más corta, la desestimada, puedan ver defraudados sus intereses, planteando un problema de responsabilidad.

Por completar la visión del sistema: para solucionar los posibles problemas de obsolescencia y asegurar la evolución del sistema la evolución del software y la supervisión técnica del sistema se encomienda a una fundación, sin ánimo de lucro, la bitcoin fundation.[44] La importancia de esta fundación en la adaptación e innovación del sistema es esencial, pero en modo alguno es un órgano rector o un supervisor del sistema como tal.

2.2.2. Secreto y criptografía de seguridad en bitcoin:

Conforme a lo expuesto, todo el mundo puede comprobar la cadena de bloques y ver el momento y circunstancias de una transacción. Esta trasparencia permite el contraste con los datos aportados por los usuarios, pero el sistema permite el seudónimo y por ello no identifica necesariamente al usuario de cada transacción. Comprobar una operación no es lo mismo que comprobar la autoría de la misma. Blockchain no exige la identificación previa de un usuario, lo

42 https://en.bitcoin.it/wiki/API_reference_%28JSON-RPC%29

43 Oermann-Töllner, The Evolution of Governance Structure in Cryptocurrencies and the Emergence of Code-Based Arbitration, https://cyber.harvard.edu/publications/2014/internet_governance in Bitcoin

44 https://bitcoinfoundation.org/

identifica por una serie de códigos y una copia criptográfica con un sistema de criptografía publica de doble clave, por lo que cada usuario tiene sus claves almacenadas en un portafolio independiente que debe controlar, pues el único medio de identificación de la titularidad de la operación, con el inconveniente de que la apropiación o la perdida de las claves harían imposible acceder al bitcoin. Es cierto que se pueden usar mecanismos de identificación indirectos; Ip del proveedor de servicios, adjuntado de correos, vinculación de la operación a CC bancaria…. por lo que el sistema se califica como pseudo secreto, pero el sistema en si permite y facilita el anonimato del titular, y la combinación del sistema con mecanismos como los de navegación anónima, uso de la red TOR y similares pueden hacer imposible la identificación del titular, motivo por el cual se ha convertido en una panacea para quienes buscan su uso en transacciones ilícitas o en el blanqueo de capitales.

2.2.3. Riesgos particulares y riesgos sistémicos del Bitcoin

De hecho y abundando en lo ya indicado, bitcoin presenta diversos riesgos particulares y algunos riesgos sistémicos que conviene exponer para valorar el sistema.

2.2.3.1. Riesgos individuales en bitcoin

Entre los riesgos particulares está el de que alguien se haga con nuestra clave privada para usar el sistema de criptografía de clave pública: por ejemplo, asaltan nuestra wallet, copian el archivo 'wallet.dat'. Si usamos clave personal estas son bastante accesibles frente a asaltos de computación basados en el diccionario las palabras de uso frecuente o de claves numéricas vinculadas al usuario… Lo habitual en estos casos es usar un ataque usando cuatro millones de palabras básicas de las que destacan unos pocos miles.[45]

Finalmente, si no dispones de copia y te olvidas o pierdes la clave, pierdes para siempre el acceso al bitcoin, que queda perdido en el ciber espacio. Se calcula que una cantidad superior a los 22 millones de euros navega por el ciber espacio en esta condición de limbo.

¿En qué cartera de almacenamiento confiar? ¿En una depositada en la nube (Hotwallet)?, ¿en tu ordenador o en dispositivos de almacenamiento? (coldwallet)[46] La utilización de plataformas de intercambio interpuestas añade, además, un factor de riesgo, ya que algunas son muy vulnerables en el acceso.

El segundo riesgo de seguridad personal deriva de la propia dinámica de funcionamiento: si se te estafa para realizar un pago no hay vuelta atrás, la cadena es irreversible y los nodos no responden de la introducción de los datos en el bloque, por lo que sólo cabría una compensación por quien nos ha estafado como forma de reversión, lo que por definición es improbable. En sentido parecido, si

---

45 http://www.eldiario.es/hojaderouter/seguridad/seguridad-carteras-bitcoin-hackers-criptomonedas_0_363264145.html

46 http://www.technologyreview.es/informatica/44368/escribe-la-clave-de-tus-bitcoins-en-un-papel-si/

alguien nos "coloca" en una cadena insegura, en un fork destinado a fracasar, descubriremos que, en propiedad, nadie dentro del sistema responde por ello.

2.2.3.2. Riesgos sistémicos de bitcoin

Pero lo que en realidad debe preocuparnos más, es si el propio sistema presenta riesgos que lo hagan inhábil para los fines funcionales que aquí se pretenden. Siguiendo el listado de riesgos utilizado al comienzo de este apartado, diríamos:

Bitcoin parece un sistema resistente frente al **riesgo tecnológico**. El sistema de hoja contable compartida o base de registro única compartida que se crea es computacionalmente resistente. Un ataque computacional contra la cadena implicaría utilizar una capacidad de computación que supere al menos al 51% del sistema distribuido, lo que es harto difícil y aún más teniendo en cuenta la existencia de registros previos y la descentralización del sistema. Con excepción de un incidente en el momento incipiente del nacimiento de la cadena, que no quedo nunca bien aclarado, el sistema ha resultado ser confiable. Ello no obstante, no es impensable un riesgo de colapso derivado de la propia dinámica del sistema, que no admite más de tres transacciones por segundo, lo que puede ser insuficiente ante el crecimiento exponencial del uso de la red.[47] Peor es la respuesta frente al **riesgo sistémico**: ni los nodos o mineros de bitcoin ni los diversos agentes intermediarios e inversores que operan en el sistema se someten en realidad a norma de garantía alguna ni responden de la introducción de datos en el sistema. Diversas compañías especulativas en bitcoin han quebrado, y esto causa trastornos y pérdidas a los usuarios, pero lo más inquietante es lo que esto supone por cuanto indica que no hay mecanismos de contención frente a un hundimiento generalizado de los agentes. Bitcoin protagoniza constantemente fluctuaciones de su cotización que mayormente se resuelven al alza,[48] pero un abandono repentino y generalizado del sistema hundiría su cotización y podría provocar un crack del sistema en su conjunto sin que hubiera mecanismos de control como los existentes en el sistema target, el sistema de pago interbancario o en cualquier otro sistema de compensación financiera supervisado. En los sistemas de compensación de pagos europeos se establecen mecanismos de control de concentración de riesgo, de paralización temporal de operaciones ante caídas repentinas o acumulaciones inusuales de movimientos de caja que actúan como colchón del sistema y que podrían haber protegido a múltiples usuarios ante el hackeo de operadores en bitcoin o ante quiebras de dichos operadores. De hecho uno de los mayores riesgos de bitcon es el **riesgo institucional**; que sean las propias autoridades bancarias las que coordinen un ataque en forma de prohibición de operación, como la decretada por la autoridad bancaria china, pues si finalmente las criptomoneda virtual tiene problemas para su conversión en divisa ordinaria o para realizar operaciones de pago, los usuarios forzarían la

47 Una de las razones alegadas para la producción del hard fork (vid infra) fue el cuasi colapso del sistema en 2016 cuando las transacciones llegaron a completarse en plazos de 43 minutos y se llegó a rechazar operaciones por bloqueo del sistema. www.gurusblog.com/archives/bitcoin-al-borde-del-colapso-tecnico/06/03/2016/

48 Polasik-Piotrowska-Wisniewski-Kotkowski-Lightfoot, "Price Fluctuation and the use of Bitcoin", en *International Journal of Electronic Commerce*, Vol. 20, n. 1, 2016, 9.

desinversión masiva y esto podría provocar el colapso del sistema.[49] Sorprendentemente, sin embargo, es necesario aclarar que aunque la prohibición de China supuso bajadas de un 16 a un 22% en las criptodivisas, éstas se recuperaron en menos de una semana y han continuado subiendo en la cotización.

Hay, por otro lado, una lección a aprender del **riesgo mutualista o de coherencia** evidenciado por los llamados "**hard forks**" [50] o con más propiedad de la división del sistema que se produce cuando es la comunidad de mineros la que se divide y duplica la cadena entera creando dos líneas separadas de desarrollo por modificación del protocolo asumido, como cuando bitcoin se separó en bitcoin cahs y bitcoin gold.

Al dividirse la cadena de nodos en el uso de dos protocolos, ambos tomando la cadena de bloques original como base, lo que ocurre es que los titulares de posiciones en la cadena vieron duplicadas sus anotaciones, aunque eso sí, la división afectó a la valoración de ambos nominales devaluando (inicialmente) la cotización previa. Esta multiplicación es, desde el punto de vista contable inadmisible y aunque el sistema obviamente resistió la operación, dio lugar a movimientos especulativos con los nuevos y los viejos nominales[51] y demostró que un sistema basado en el consenso estructural puede morir si dicho consenso estructural se pierde, pues realmente nadie dirimió la titularidad de la cadena y un sistema monetario no puede duplicar sus activos, sin base real, indefinidamente. Detrás de una divisa o de un valor de cambio, necesariamente ha de existir una base de capìtal real (PIB de las naciones, bienes) o de capital Monetario (divisas). Un sistema que duplica el valor residente, aunque sea nominalmente, carece de estabilidad y credibilidad a largo plazo. Al menos como moneda, otra cosa es, ciertamente, como valor especulativo. Tras la división de la cadena Bitcoin, de hecho su cotización se ha revalorizado a niveles nunca vistos, en lo que reproduce un sistema de hiperinflación virtual altamente arriesgado, Pero esto implica que, juegos de inversión aparte, las criptomonedas o introducen sistemas de control del riesgo sistémico o terminarán por no ser instrumentos aptos para la contratación regular y masiva del Business to Business, pues nadie puede un articular un sistema de intercambios regular sobre una divisa hiperinflacionaria o hiperdeflacionaria en el que se desconoce finalmente cuál es el valor comprometido en la transacción. Bitcoin, por desgracia, se ha convertido más en un valor que en una moneda. No es de extrañar que el Banco de España

49 https://cincodias.elpais.com/cincodias/2017/09/04/mercados/1504518523_957352.html
http://www.abc.es/economia/abci-prohibicion-china-pone-fiesta-monedas-digitales-201709100129_noticia.html
https://urbantecno.com/tecnologia/bitcoin-ethereum-china

50 https://elbitcoin.org/escenarios-posibles-partir-del-fork/
https://www.forbes.com/sites/laurashin/2017/10/31/what-will-happen-at-the-time-of-the-bitcoin-hard-fork/#a742865337d4
https://www.xataka.com/empresas-y-economia/mas-forks-de-bitcoin-mas-incertidumbre-a-bitcoin-cash-se-le-suman-bitcoin-gold-y-el-segwit2x
https://criptotendencia.com/2017/09/29/primero-cash-ahora-gold-otro-hard-fork-de-bitcoin-esta-en-camino/
https://es.cointelegraph.com/news/hard-fork-y-soft-fork-en-qu%C3%A9-consisten-y-cu%C3%A1les-son-sus-diferencias
https://www.coindesk.com/bitcoin-cash-developers-set-date-november-hard-fork/

51 Chernukka, V., "Como influencia el hard fork al precio del bitcoin" https://blog.iqoption.com/como-influencia-el-hard-fork-al-precio-del-bitcoin/ 30-10-2017

considere las transacciones en bitcoins como más cercanas a una operación OTC en un mercado descentralizado que al mercado monetario.[52]

2.2.4. Régimen jurídico de las operaciones en Bitcoin y demás cripto monedas virtuales

2.2.4.1. Régimen jurídico de los operadores Blockchain:

La tecnología blockchain ha sido identificada como tecnología disruptiva[53] en contraposición a la llamada tecnología de sustentación al crear sistemas horizontales y descentralizados sin una autoridad rectora o supervisora, momento en el que aparece un riesgo de gobernabilidad y de definición del estatus jurídicos (ley y foro aplicable),[54] así como una clara dificultad para identificar a los sujetos responsables. El estatus jurídico de los operadores en bitcoin es, a día de hoy, ciertamente confuso.

Hacienda Pública:

Así, sabemos por diversas consultas vinculantes a la **Hacienda pública** (V3625-16, V 1028-15, 1029-15, V2846-15) que los mineros de bitcoin están obligados a darse de alta en hacienda y a pagar en su caso la cuota de autónomos. En concreto, que la actividad de minado en sí misma no está sujeta al IVA; la generación de la criptomoneda, para que fuera gravable por el impuesto, tendría que responder a una relación directa entre el servicio prestado y la contraprestación recibida, como señaló el TJUE (Sala Segunda) en su sentencia de 5 de febrero de 1981, asunto 154/80. [55] La creación de bitcoins no presupone una relación entre el proveedor y el destinatario del servicio "de tal forma que en la actividad de minado no puede identificarse un destinatario o cliente efectivo de la misma, en la medida que los nuevos Bitcoins son automáticamente generados por la red" (V3625-16) Por ello, el minado de criptomonedas que genera nuevos bloques en la red no estará sujeto al IVA, pero, ¡cuidado¡ el cobro de comisiones que no aumenta la masa monetaria, si estaría sujeto a tributación del IVA. Y minar bitcoins tampoco daría derecho a desgravarse las cuotas de IVA soportadas (art. 94 LIVA).

Del mismo modo, la primera transmisión de bitcoins estaría sujeta al IVA pero sería una operación exenta.[56] Por otro lado, minar, se tenga beneficios o no es una actividad económica y el titular de la actividad está obligado a darse de alta

52 Gorjón, S., Banco de España, Eurosistema, Dirección General de Operaciones, Mercados y Sistemas de Pago," Divisas o Monedas Virtual: El caso de Bitcoin" enero 2014, pág. 4/13.

53 Bower-Christensen, Disrupting Technologies: Catching the Wave, in *Harvard Business Review*, I, 1995, 43. Swartz, Lana, "El sueño del Blockchain. Imaginando alternativas tecnoeconómicas mas allá del bitcoin" en Castells, M. et al. Otra economía es posible. Cultura y economía en tiempos de crisis. Alianza editorial, Madrid, 2017, págs. 123-155

54 Böhme-Christin-Edelman-Moore, "Bitcoin: Economics, Technology and Governance", in *Journal of Economic Perspectives*, Vol. 29, n. 2, 2015, 213.

55 https://www.abanlex.com/2016/09/los-mineros-de-bitcoins-estan-obligados-a-darse-de-alta-en-hacienda-y-pagar-la-cuota-de-autonomo/
https://www.abanlex.com/wp-content/uploads/2016/09/V3625-16_anonimizada.pdf

56 V1029-15 y V2846-15 y TJUE en su Sentencia del asunto C-461/12 y asunto C-264/14 sobre la fiscalidad en el IVA de las transmisiones en bitcoins: https://www.abanlex.com/wp-content/uploads/2016/09/TJUE_C-264-14.pdf

en el Impuesto de Actividades económicas como "Otros servicios financieros no comprendidos en otras partes".[57] El minero individual debería darse de alta en la Seguridad social, incluso si no llegara a generar bloques, y debería reflejar sus ventas de Bitcoins en el IRPF o en el Impuesto de Sociedades. De manera incoherente con el tratamiento IVA del bitcoin, sin embargo, para el ICAC, las monedas virtuales deberán calificarse como inmovilizados intangibles en la medida que cumplan con los requisitos expuestos en la NRV 5ª del PGC.[58]

Obviamente, la mayoría de los cientos de pequeños mineros no profesionales raramente cumplen con estos deberes.

Normativa de prevención del blanqueo de capitales:

Por un lado, sabemos que en países como Los EEUU, desde marzo de 2013 el Financial Crimes Enforcement Network (FinCEN) del Departamento de Estado Norteamericano, extendió el alcance de la normativa BSA, tanto a las casas de cambio que efectuaban operaciones de compra/venta de las divisas virtuales por dinero de curso legal, como a quienes actuasen como "mineros" de bitcoins, obligándoles a ambos a registrarse como empresas prestatarias de servicios monetarios y cumplir con la normativa de blanqueo de capitales y financiación del terrorismo por considerar que en su actividad existía una transferencia de valor. No obstante, los usuarios que emplean bitcoins exclusivamente como un medio de pago de bienes o servicios no se ven afectados por esta medida. La FINcen Norteamericana, de hecho, ya ha impuesto graves sanciones a operadores de Bitcoin por no cumplir con los planes de prevención del blanqueo de capitales.[59] La postura contrasta con la sostenida hasta el momento por el FATF europeo que aunque considera que bitcoins no pueden considerarse moneda corriente, dinero electrónico o instrumento financiero y por tanto no sujeta directamente estas operaciones a la normativa anti blanqueo (FATF informe 2014) aunque recomienda a las autoridades nacionales y europeas que utilicen los marcos legislativos actuales de regulación y supervisión para que sean aplicables a las monedas virtuales y que si no fuere posible procedan a su modificación y adaptación (Informe 2015). El plan europeo de lucha contra el terrorismo (Com 2016 50 final) ya propone abiertamente la modificación de la directiva de prevención del blanqueo de capitales para incluir las agencias y plataformas de moneda digital en el ámbito de supervisión, y ya existe una primera jurisprudencia en la que se ha aplicado a agentes de bitcoin el art. 7.3 de la LPBC (SAP Asturias 6 febrero 2015).[60]

Normativa de servicios de pago:

Mientras en los USA los transmisores de Bitcoins se consideran transmisores de dinero y como tal deben obtener la correspondiente licencia estatal y someterse a la normativa de secreto bancario, en Europa ni la directiva de dinero electrónico ni la directiva de servicios de pago es directamente aplicable

---

57 Art. 78 TR LHRL epígrafe 831-9 de la sección primera de tarifas, "Otros servicios financieros no comprendidos en otras partes"

58 Contestación a Consulta del Instituto de Contabilidad y Auditoría de Cuentas (ICAC). Rfa: rmr/38-14.

59 Véase Ramos Suárez, F. (Presentación) La regulación jurídica de las monedas virtuales y la tecnología blockchain, Fide DPO it Law, mayo 2016 (Disponible en red)

60 Un comentario en https://www.oroyfinanzas.com/2015/04/aplica-ley-prevencion-blanqueo-capitales-bitcoin-espana/

al supuesto. Bitcoin no es una moneda en sentido técnico y por ello no estaría en el ámbito de dichas regulaciones,[61] pero nuevamente se recomienda a las autoridades nacionales la aplicación del marco de supervisión en lo que sea admisible y la modificación del marco regulatorio en su caso a fin de someter a los mismos a un régimen de garantía. En concreto, los mineros de bitcoin no son entidades de pago a los efectos de la LSP española ni en los términos de la Directiva 2007/64 o en la más reciente DSP2 de 2015. Tampoco pueden considerarse como las más recientes Entidades de Servicios de iniciación de pago.[62] Y dicho esto, sin embargo, buena parte de los operadores de compra y venta de bitcoins son perfectamente incluibles en la categoría, puesto que trafican con otras divisas, del mismo modo que algunas de las compañías de iniciación de servicios de pago han incluido en su cartera de servicios operaciones de pago en bitcoin con grandes compañías como Apple o Microsoft, momento en el cual entrarían bajo el paraguas regulatorio. Conviene pues diferenciar entre el mercado primario o de emisión de bitcoins y el mercado secundario o derivado de negociación de los mismos, que ocasionalmente si es susceptible de encuadramiento. Por otro lado, si bien no cabe definir a los mineros de bitcoin como entidades de pago, las operaciones de pago en bitcoin no están explícitamente excluidas del ámbito de la directiva y las transacciones en bitcoin organizadas por agentes de bitcoins son encuadrables en la definición de operación de pago y sistema de pago de la DSP2 (art. 4 nº 5 y 7). Del mismo modo, la función de bitcoin como instrumento de pago es perfectamente coherente con la definición del art. 4.14 DSP2 por la que instrumento de pago es "cualquier dispositivo personalizado y/o conjunto de procedimientos acordados entre el usuario de servicios de pago y el proveedor de servicios de pago y utilizados para iniciar una orden de pago". A mi juicio, la futura trasposición de la directiva de servicios de pago 2015, previsiblemente establecerá algún mecanismo expreso de incorporación al régimen tutelar, no a los mineros de bitcoin, que ciertamente no son incluibles en el tipo, pero si a las compañías que trafican con el cambio de divisas y bitcoins o que actúan como pasarelas de pago o de iniciación de servicios de pago, admitiendo el pago en bitcoins. Esto supondrá una extensión de la seguridad jurídica de los usuarios del sistema, que podrán acogerse al régimen tutelar comunitario de los art 38 y ss. de la DSP2 (trasparencia informativa, gastos de información, carga de la prueba, información precontractual y condiciones generales, plazos de ejecución, etc.) pero también nos lleva al previsible contexto de diferenciación entre las compañías de pago en bitcoins que regularicen su estatus jurídico y las que previsiblemente no lo harán o no estarán sujetas a dicha carga por no ser de ningún estado comunitario. El panorama del uso del bitcoin en los próximos años se prevé confuso porque, además, hemos de recordar que buena parte de la normativa cautelar choca frontalmente con el planteamiento de privacidad y anonimato de las redes blockchain y en concreto del bitcoin. Y sin embargo, en mi opinión, las criptomonedas están destinadas a incorporarse al sistema de pagos oficial y a poder funcionar normalmente como sistema de pago por más que previsiblemente queden reductos de operaciones

61 Banco Central Europeo, Informe sobre monedas virtuales febrero 2015 y opinión de 4 de julio 2014.

62 Alvarado Herrera, L. "El servicio de iniciación de pagos en la Directiva 2015/2366 sobre servicios de pago en el mercado interior" en *La Ley mercantil nº 34*,2893 2017

opacas en la red. Lo mismo que ocurre a fin de cuentas con el dinero ordinario, que siempre ha tenido su mercado negro de transacciones no registradas.

2.2.4.2. Régimen jurídico de los pagos en criptomonedas virtuales

Por otro lado, dejando al margen la calificación del pago en criptomoneda como instrumento de pago en sentido propio, con el pago en divisa virtual propiamente estamos ante una permuta de valor de un bien fungible (art. 337 C.C.) representación digital de un valor de cambio aceptable como medio de pago mediando consentimiento y aceptación de las partes (art. 1166 C.C.) y con sometimiento al art. 1170.2 del C.C. (medio de pago pro solvendo "salvo buen fin"). Y por ello, lo que es más importante de resaltar, ante un pago perfectamente legal y eficaz en términos jurídicos (ex art. 1170.2 C.C.)

3. CONCLUSIONES

Desde que se introdujo la logística en la distribución, hemos asistido a un creciente proceso de automatización en las funciones distributivas (almacenes robotizados, documentos de trazabilidad[63], sistemas de producción just in time)…[64] Era un corolario lógico de todo este proceso que terminara afectando a la propia forma de la contratación, pues un proceso que busca la maximización de la eficiencia y el máximo ahorro en costes, no podía quedar subordinado a lentos procesos de conclusión y formalización contractual y al albur de volátiles voluntades de cumplir con el proceso de ejecución automatizado. La aparición de los Smart contracts o contratos en formato electrónico autoejecutable era por ello una necesidad para dar respuesta a esa creciente búsqueda de eficacia en operaciones en masa, a la multiplicación en el ámbito electrónico de micro operaciones y a la creciente demanda de estructuración de las operaciones en el internet de las cosas.

Los contratos en formato electrónico con mecanismos de ejecución pre programada no presentan en principio ningún problema reseñable de validez o de determinación de régimen jurídico, una vez salvado el trámite del consentimiento inicial del contrato marco expresado en lenguaje humano a los efectos del art. 1261 del C.C. Ciertamente, la creciente globalización de las operaciones mercantiles introducirá como factor de cierta incertidumbre el de la compleja normativa de fijación del foro de competencia y ley aplicable, pero, aun en esto, no hay novedad respecto a cualquier otro contrato electrónico o no.

Las dificultades para la expansión y normalización de los Smart contracts, sin embargo, son de pura operativa y se centran mayormente en la dificultad de articular sistemas de pago en red, automatizados y no susceptibles de desistimiento una vez que se cumplen y justifican por vía electrónica los eventos

63 Véase "La carta de porte emitida electrónicamente" en Comentarios a la ley de transporte terrestre, Duque Domínguez,J/Martínez Sanz, F. (Dir.) Aranzadi Thomson-Reuters, Pamplona 2010, ISBN 978-84-9903-629-8, págs. 185-212.

64 Echebarría Sáenz, J.A., Voz "Distribución comercial" en *Diccionario de derecho de la competencia*, Velasco San Pedro, L. A. (Director), Madrid, Iustel, 2006, (Págs. 323-331), "El comercio electrónico entre empresarios" en El comercio electrónico…, 2001, págs. 81-144

desencadenantes del pago. Dos son los instrumentos que por su adecuación cumplen con esta posible función, a saber, los instrumentos de dinero electrónico y las monedas virtuales o criptodivisas creadas en red usando las tecnologías blockchain como pueden ser bitcoin, ethereum y otras.

El dinero electrónico, por su régimen de plena convertibilidad en divisa ordinaria y su inclusión en el sistema europeo de pagos es en principio el instrumento aparentemente más adecuado para este tipo de operaciones. Ofrece la misma estabilidad que la divisa representada digitalmente, plena convertibilidad, efectos de pago pro soluto y sus operadores ofrecen un régimen de garantía operativa y garantía sistémica muy apreciable. Sin embargo, la poca disposición de las compañías a articular una oferta comercial en este campo, ha dejado paso a la introducción de las criptodivisas que nacen de la misma filosofía y de la misma tecnología (blockchain) que los propios Smart contracts.

Detrás de los Smart contracts, lo mismo que detrás de las criptodivisas se encuentran los llamados mutualistas infraestructurales[65] y tecnologías de contabilidad distributiva (distributive ledger) que permiten un gigantesco registro de datos de transacciones monetarias o contractuales con bajo coste, alta fiabilidad, resistencia computacional, acceso público y, todo ello, sin necesidad de crear una estructura jerárquica en lo que es un sistema descentralizado, horizontal y autoregulado. Ciertamente, esto último es una opción. Mientras la mayoría de los sistemas blockchain reúnen las características de crear entes descentralizados (DAOs)[66] también es posible crear sistemas de contabilidad compartida bajo el control y dirección de un operador tradicional (sistemas GDS).[67] En todo caso, en la actualidad, muchas de las operaciones de pago automatizado se canalizan por sistemas de criptodivisa virtual que, hoy por hoy, carecen de un estatus legal reconocido y dotado de seguridad jurídica, pero que, en un análisis detallado, son perfectamente legales y admisibles en Derecho. A este respecto hemos de señalar que desde el punto operativo, las monedas virtuales han demostrado ser perfectamente eficaces, abaratar costes, y ofrecer una funcionalidad con niveles de seguridad perfectamente aceptables. Nada nos permite denunciar ilegalidad en sí misma de las operaciones de pago en criptodivisa, por el contrario, son perfectamente encuadrables como medio de pago y surten plenos efectos, aunque sus operadores aun no formen parte del sistema regulado. El conflicto aparece cuando comprobamos que los pagos en criptomoneda carecen de mecanismos contra el riesgo sistémico financiero o riesgo de hundimiento o que su propia alegalidad les coloca en un riesgo institucional que es quizás el más grave. Asistimos a un proceso de incorporación creciente de los operadores de bitcoin al sistema de supervisión cautelar. Ya disponen de un régimen fiscal, se les aplica la normativa de prevención del terrorismo y blanqueo de capitales, aun sin una declaración formal al efecto, y es cuestión de poco tiempo que se les aplique determinadas normas cautelares de la regulación de servicios de pago, si bien esta última etapa, recién iniciada, aun es incierta en su ejecución y previsiblemente tropezara tanto con la filosofía de estas redes, como con su estructuración como sistema anónimo, que entra por ello en contradicción con la normativa de

65 Swartz, "El sueño del Blockchain…. págs.127.

66 Swartz, "El sueño del Blockchain…. Págs. 129 y ss

67 Caso de la *distributive ledger iniciative* 2015 fomentada por los 15 bancos principales del mundo en ordena crear un sistema de moneda virtual propia y un sistema de compensación y liquidación de operaciones globalizado basado en tecnología blockchain. SWARTZ, "El sueño del Blockchain…. Págs.. 129 y ss

supervisión comunitaria. En todo caso, y con independencia de cómo llegue a solucionarse este encuadramiento, el principal problema de las divisas virtuales para articular sistemas de contratación fiables, estandarizados y continuados en el tiempo, es su propia volatilidad, el hecho de que actúen simultáneamente como unidad de valor y como valor especulativo, al punto de que ningún sistema de contratación automatizada puede articularse sobre una unidad de cuenta cuyo valor es indeterminable por su rápida fluctuación. Esto limita la funcionalidad de la divisa virtual a operaciones aisladas y la aleja de posibles contratos marco para operaciones en serie.

Finalizo con una reflexión de Anthony Giddens, animémonos a "ocupar el futuro" e imaginar sistemas innovadores. Solucionemos razonablemente los problemas y abramos nuevos sectores económicos, pues de otro modo ya llegará quien nos escriba el futuro según sus intereses.

4. Notas bibliográficas y Referencias web:

AA.VV. (1995): Bower-Christensen, Disrupting Technologies: Catching the Wave, in *Harvard Business Review*, I, 43.

AA.VV. Calvo Caravaca, A./Carrascosa González, J. "problemas de extraterritorialidad en la contratación electrónica" en Echebarría Sáenz, J. (Dir) *El comercio electrónico*, págs. 145-217.

AA.VV. (2017): "Collaboration or business? From value for users to a society with values", Madrid, OCU, Creative Commons.

AA.VV. (2015): Böhme-Christin-Edelman-Moore, "Bitcoin: Economics, Technology and Governance", in *Journal of Economic Perspectives*, Vol. 29, n. 2, 213.

AA.VV. (2007): Mata Martín, R./Javato Martín, A. *Los medios electrónicos de pago*, Granada Comares,

AA.VV. (2016): Polasik-Piotrowska-Wisniewski-Kotkowski-Lightfoot, "Price Fluctuation and the use of Bitcoin", en *International Journal of Electronic Commerce*, Vol. 20, n. 1, 9.

AA.VV., Velasco, Echebarría, Herrero (Dir) (2014): Acuerdos horizontales, mercados electrónico y otras cuestione actuales de competencia y distribución, Valladolid, Lex Nova Thomsom-Reuters.

AAVV., Pereira de Araújo, H./Arambasic Rebelo da Silva, R.B. (2017): "A tecnologia digital blockchain: análise evolutiva e pragmática", en REFAS v3, nº 4, junio (ISSSN 2359-182X).

Alvarado Herrera, L. (2017): "El servicio de iniciación de pagos en la Directiva 2015/2366 sobre servicios de pago en el mercado interior" en *La Ley mercantil nº 34,*2893 2017

BBVA Research, (2017): "Smart Contracts: ¿lo último en automatización de la confianza" en CASTELLS, M. et al. Otra economía es posible. Cultura y economía en tiempos de crisis. Alianza editorial, Madrid.

Bitcoin. https://elbitcoin.org/escenarios-posibles-partir-del-fork/

Bitcoin. www.bitcoinfoundation.org

Blockchain. https://blockchain.info/en/charts/market-cap

Bolsamania. www.bolsamania.com/noticias/tecnología/que-es-el-unete-una-estafa-de-50-millones-de-euros-a-partir-del-bitcoin-de-jose-manuel-ramirez--771685.html

Bonet Correa, J. (1981): Las deudas de dinero, Madrid, Civitas.

Chernukka, V., "Como influencia el hard fork al precio del bitcoin" https://blog.iqoption.com/como-influencia-el-hard-fork-al-precio-del-bitcoin/ 30-10-2017

Coindesk.https://www.coindesk.com/bitcoin-cash-developers-set-date-november-hard-fork/

Cointelegraph. https://es.cointelegraph.com/news/hard-fork-y-soft-fork-en-qu%C3%A9-consisten-y-cu%C3%A1les-son-sus-diferencias

Comisión Europea. Libro Verde, "Hacia un mercado europeo integrado de pagos mediante tarjeta, pagos por internet o pagos móviles" 11 de enero de 2012.

Criptotendencia. https://criptotendencia.com/2017/09/29/primero-cash-ahora-gold-otro-hard-fork-de-bitcoin-esta-en-camino/

Cuccuru, Pierluigi. (2016): "Blockchain ed Automazione contrattuale. Riflessioni sugli smart contract" WOLTERS Kluwer Italia.

EBA. European Central Bank, Opinion on virtual currencies, Report, 4.7.2014, in www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+ Opinion+

EBA. European Central Bank, Virtual Currency Schemes, Report, ottobre 2012, in www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf

Echebarría Sáenz, J. A. (2010): "La carta de porte emitida electrónicamente" en Comentarios a la ley de transporte terrestre, Duque Domínguez,J/Martínez Sanz, F. (Dir.) Aranzadi Thomson-Reuters, Pamplona, ISBN 978-84-9903-629-8, págs. 185-212

Echebarría Sáenz, J. A. (2001): (Dir) *El comercio electrónico*, Madrid, Edisofer.

Echebarría Sáenz, J. A., (2007): "El dinero electrónico; construcción del régimen jurídico emisor-portador" en Mata/Javato, Los medios electrónicos de pago, Granada, Comares, págs. 219-267.

Echebarría Sáenz, J. A., (2006): Voz "Distribución comercial" en Diccionario de derecho de la competencia, Velasco San Pedro, L. A. (Director), Madrid, Iustel, Págs. 323-331.

El Diario. http://www.eldiario.es/hojaderouter/seguridad/seguridad-carteras-bitcoin-hackers-criptomonedas_0_363264145.html

European Banking Authority, Opinion on "virtual currencies", 4th July 2014

FATF (GAFI). (2015): *Guidance for a risk-based approach, Virtual Currencies*.

Financial Action Task Force (FATF-GAFI), Virtual currencies – key definitions and potential aml/cft risks, 2014

FORBES. https://www.forbes.com/sites/laurashin/2017/10/31/what-will-happen-at-the-time-of-the-bitcoin-hard-fork/#a742865337d4

García, R./Vasquez, C., (2016) "Supercalifragilisticoespialidoso… perdón, quería decir Blockchain", en Espacio Actuarial, nº 39, otoño.

Gorjón, S., (2017): Banco de España, Eurosistema, Dirección General de Operaciones, Mercados y Sistemas de Pago," Divisas o Monedas Virtual: El caso de Bitcoin" ENERO 2014, Pág. 4/13

Gurusblog. www.gurusblog.com/archives/bitcoin-al-borde-del-colapso-tecnico/06/03/2016/

López Lérida J., (2017): "Las tecnologías Blockchain", en Agenda de la empresa, junio.

Nakamoto Satoshi, (2009): "Bitcoin: a peer to peer electronic cash system", www.bitcoinfoundation.org

Nussbaum, (1929): *Teoría jurídica del dinero*, Madrid, (Traducción Sancho Seral).

O´Reily, Blockchain (2015): blue print for a new economy, Swan.

Oermann-Töllner, The Evolution of Governance Structure in Cryptocurrencies and the Emergence of Code-Based Arbitration, https://cyber.harvard.edu/publications/2014/internet_governance in Bitcoin on+ Virtual+ Currencies.pdf

Open Transactions. http://opentransactions.org/wiki/index.php/Voting_Pools

Oro y Finanzas. https://www.oroyfinanzas.com/2014/11/definicion-bitcoin-2-0-que-es-bitcoin-2-0/

Oro y Finanzas. https://www.oroyfinanzas.com/2015/07/ethereum-proyecto-bitcoin-2-0-mas-ambicioso-lanza-plataforma-descentralizada-frontier/

Oro y Finanzas. https://www.oroyfinanzas.com/2015/10/rootstock-contratos-inteligentes-smart-contracts-ethereum-bitcoin/

Oro y Finanzas. https://www.oroyfinanzas.com/2015/11/que-son-contratos-inteligentes-smart-contracts/

Oro y Finanzas. https://www.oroyfinanzas.com/2015/04/aplica-ley-prevencion-blanqueo-capitales-bitcoin-espana/

Ramos Suárez, F. (Presentación) (2016) La Regulación Jurídica De Las Monedas Virtuales Y La Tecnología Blockchain, Fide DPO it Law, mayo.

Regulation of bitcoin in selected jurisdictions: http://www.loc.gov/law/help/bitcoin-survey/

Situación Economía Digital, Octubre 2015.

Swartz, Lana, (2017) "El sueño del Blockchain. Imaginando alternativas tecnoeconómicas mas allá del bitcoin" en Castells, M. et al. Otra economía es posible. Cultura y economía en tiempos de crisis. Alianza editorial, Madrid, págs. 123-155.

Technology review. http://www.technologyreview.es/informatica/44368/escribe-la-clave-de-tus-bitcoins-en-un-papel-si/

U.S. Congress, Bitcoin: Questions, Answers, and Analysis of Legal Issues: ttps://fas.org/sgp/crs/misc/

UK Treasury, Digital Currencies: Response to the Call of Information, Report, marzo 2015: www.gov.uk/government/uploads/system/uploads/attachment_data/file/414040/digital_currencies_response_to_call_for_information_final_changes.pdf

Vicente Blanco, D. J. (2007) "Medios electrónicos de pago y jurisdicción competente en supuesto de contratos transfronterizos en Europa", en Mata Martín, R./Javato Martín, A. *Los medios electrónicos de pago*, Granada, Comares, págs. 270-319.

Vicente Blanco, D. J. (2014): "Problemas de jurisdicción competente y ley aplicable en los mercados electrónicos" en Velasco, Echebarría, Herrero (Dir) Acuerdos horizontales, mercados electrónico y otras cuestione actuales de competencia y distribución, Valladolid, Lex Nova Thomsom-Reuters, págs. 644-666.

Xataka. https://www.xataka.com/empresas-y-economia/mas-forks-de-bitcoin-mas-incertidumbre-a-bitcoin-cash-se-le-suman-bitcoin-gold-y-el-segwit2x

Yuan, L., (2015): "forget bitcoin, Long live Blockchain".