Cadenas de bloques y Registros de derechos

Block chains and rights registers

por

LUIS ANTONIO GALLEGO FERNÁNDEZ*

Registrador de la Propiedad

RESUMEN: La atención mediática que en los últimos tiempos está recibiendo la tecnología de la cadena de bloques ha motivado que se haya propuesto su extensión a otros sectores más allá de su ámbito inicial: Bitcoin.

En este artículo, tras una primera parte en la que se expone su funcionamiento, en su aplicación concreta a Bitcoin, se analiza si podría llegar a sustituir a los registros de derechos, pero proporcionando sus mismos efectos. La conclusión, sin embargo, es que esta tecnología, aplicada sin modificaciones, produciría una radical reducción de la calidad de la seguridad jurídica preventiva que proporcionan este tipo de registros y, en todo caso, sería necesario aceptar profundas modificaciones legislativas y una fuerte restricción a la libertad de contratación.

Es posible, no obstante, el establecimiento de cadenas de bloques privadas con versiones modificadas de su protocolo de funcionamiento, que eliminarían alguno de aquellos problemas, pero que lo desnaturalizan, aproximándolo a otro tipo de soluciones que ya se aplican con éxito en algunos países y, como ejemplo de ello, se analiza brevemente el sistema español.

* Vocal director del Servicio de Sistemas de Información del Colegio de Registradores de la Propiedad y Mercantiles de España e Ingeniero de Telecomunicación.

ABSTRACT: The media attention being given to blockchain technology has recently led to a call for its use to be extended to other sectors beyond the field in which it was initially applied: Bitcoin.

This article, after first describing how it operates, in its specific application to Bitcoin, looks at whether it could be used to replace rights registers, but provide the same effects. The conclusion, however, is that this technology, applied without modification, would radically reduce the quality of the preventive legal certainty provided by registers of this kind and would, in any case, require major legislative changes and considerable restrictions on freedom of contract.

Private blockchains with modified versions of the operating protocol could however be established, and this would eliminate some of those problems, but they would change its character, making it more like other types of solution that are already being applied successfully in some countries. An example isthe Spanish system, which is analysed briefly.

PALABRAS CLAVE: Blockhain. Cadenas de bloques. Registros jurídicos. Registros de derechos. Bitcoin.

KEY WORDS: Blockchain. Block chains. Legal records. Rights registers. Bitcoin.

I. INTRODUCCIÓN

A finales de octubre del año 2008, en plena crisis financiera, SATOSHI NAKAMOTO[1] publica, a través de la Cryptography Mailing List (cryptography@metzdowd.com)[2] y de la página: http://www.bitcoin.org[3], su artículo: «Bitcoin: A Peer-to-Peer Electronic Cash System» en el que el autor exponía su diseño para un sistema electrónico de pagos sin terceros de confianza: el sistema Bitcoin. Más tarde, en 2009, haría pública la primera versión del primer programa cliente de Bitcoin.

Bitcoin[4] se caracteriza por la privacidad, su volatilidad, su naturaleza esencialmente descentralizada, la ausencia de una autoridad central que lo controle y el uso extensivo de la criptografía como medio para asegurar las transacciones. Estas características, junto con la reacción y desconfianza que se suscitó frente a los bancos centrales y privados durante la crisis de 2008, explican el desarrollo exponencial que ha experimentado esta criptomoneda desde sus inicios.

A la fecha de este artículo[5] la capitalización del mercado[6] de bitcoins es superior a los diecinueve mil cien millones de dólares y existen más de dieciséis millones de bitcoins en circulación con un precio medio de mercado, cada una de ellas, de alrededor de 1.175 dólares.

Por otro lado, en la actualidad son muchas las empresas que admiten el pago de sus productos o servicios en bitcoins (WordPress, Microsoft, Virgin, Dell, etc.) o su compra y cambio a monedas reales (Bitstamp[7], Coinbase[8], Kraken[9], Bitfinex[10], BTC-e[11], LocalBitcoins[12], OKCoin[13], etc.). Además, tras la estela de bitcoin, han comenzado a surgir nuevas monedas virtuales (Litecoin[14], Ripple[15], Primecoin[16], Dogecoin[17], Zcash[18], etc.) que utilizan la misma tecnología de base: las cadenas de bloques.

Son precisamente, las cadenas de bloques, la base tecnológica sobre la que se asienta el éxito de Bitcoin. Realmente, dichas cadenas de bloques, son una combinación de diferentes tecnologías (redes Peer-to-Peer, criptografía asimétrica, etc.) que ya eran conocidas desde hace tiempo. Lo verdaderamente novedoso es la forma en que se han combinado todas ellas.

Tal ha sido la atención mediática que ha recibido esta tecnología que recientemente se han buscado y señalado otros campos en los que podría tener aplicación. Entre estos campos se ha propuesto la contratación inmobiliaria, argumentando la mayor seguridad y transparencia que ofrece el sistema de cadenas de bloques frente a los sistemas actuales, así como el ahorro de costes que podría suponer su adopción en este campo, al permitir la eliminación de los intermediarios que tradicionalmente han venido interviniendo en este sector.

En este artículo se analizarán estas afirmaciones en relación con los Registros de la Propiedad y, más concretamente, en relación con los Registros de derechos, como lo son los Registros de la Propiedad españoles. No obstante, y como paso previo, se expondrá sucintamente el funcionamiento de las cadenas de bloques mediante el estudio de su implementación en el sistema Bitcoin.

II. FUNCIONAMIENTO DE LAS CADENAS DE BLOQUES. BITCOIN

1. Primero pasos

Bitcoin trata de implementar un sistema seguro para llevar a cabo transacciones sin la intervención de un tercero de confianza (por ejemplo, una entidad

bancaria). Trata, por tanto, de establecer un sistema mediante el que puedan realizarse transferencias monetarias y que funcione de forma segura aun cuando sus usuarios no se conozcan y desconfíen unos de otros.

Como inciso, señalar que una consecuencia de lo anterior, y a diferencia del sistema bancario tradicional, es que en el supuesto de que ocurra cualquier problema, no existe ninguna persona, entidad o corporación ante la que plantear la oportuna reclamación, sino tan solo usuarios que no se conocen entre sí, por lo que no habrá nadie que responda por aquel mal funcionamiento.

En términos simplificados para lograr el objetivo expuesto en el primer párrafo de este epígrafe se establece un fichero digital en el que se hacen constar todas las transacciones que se van realizando entre dichos usuarios, a modo de libro de contabilidad. Una copia de este archivo se mantiene en cada uno de los equipos que se conectan a la red Bitcoin. Por tanto, cualquier usuario puede conocer las transacciones realizadas por los demás.

Es, precisamente, este grado de total distribución de la información lo que caracteriza al sistema Bitcoin y a la tecnología de cadena de bloques que lo sustenta. Ningún nodo de la red, por sí solo, es determinante ni imprescindible para el correcto funcionamiento del sistema; si alguno de dichos nodos se pierde, ello no supone pérdida de información alguna puesto que todos tienen una copia completa de la misma y, por tanto, teóricamente ninguna persona o entidad individual podría hacerse con el control del sistema.

En Bitcoin existen distintos tipos de nodos o, dicho de otra forma, nodos que llevan a cabo diferentes funciones:

— En primer lugar, nodos que solo emiten transacciones *(broadcast node):* Son aplicaciones monedero que únicamente permiten enviar o recibir monedas a través de la red Bitcoin. Las hay para todo tipo de dispositivos y también existen plataformas web que ofrecen este servicio.
— Nodos que propagan transacciones *(relay node):* Su función es, principalmente, recibir transacciones y retransmitirlas a otros nodos, aunque también comprueban que tienen el formato correcto, que las firmas criptográficas que contienen son válidas y también verifican, en la cadena de bloques, que el dinero que se transfiere existe en la cuenta de origen de la transacción.
— Y, por último, nodos que emiten, transmiten y minan transacciones *(mining node):* Además de poder llevar a cabo las mismas tareas que los anteriores tipos, su principal cometido es validar y añadir las transacciones a la cadena de bloques, en la forma que luego se verá.

La anterior clasificación está ordenada de menor a mayor complejidad, de tal forma que los nodos del primer grupo son los más simples y los que menos capacidad computacional requieren, mientras que los últimos son los más com-

plejos, suelen contar con un hardware específico para poder realizar las labores de minado a la mayor velocidad posible y son, además, imprescindibles para garantizar la seguridad del sistema.

De forma muy resumida, para realizar una transferencia a favor de otro usuario no hay más que difundir un mensaje en la red Bitcoin indicando la cantidad a transferir y el destinatario. Con cada una de estas transacciones se realizan una serie de operaciones de verificación y, una vez superadas, se anotan en la copia del archivo contable del nodo que las hubiera verificado y se difunden a otros nodos, de tal forma que el *libro* de transacciones es mantenido por la totalidad de los usuarios.

Para comenzar a operar en la red Bitcoin lo primero que debe hacerse es crear nuestro propio monedero en el que almacenar las monedas virtuales y que también nos permitirá realizar transacciones. Como antes se ha indicado, existen numerosas páginas web que permiten crear estos monederos o bien podemos optar por la instalación en nuestro equipo de la correspondiente aplicación cliente. En este último caso también existe una gran variedad de programas entre los que elegir, para todo tipo de dispositivos (ordenadores personales, dispositivos móviles, etc.) o sistemas operativos e, incluso, es posible encontrar librerías para programar nuestro propio programa cliente[19]. Una de las aplicaciones cliente más populares es Bitcoin Core[20].

Estos clientes, una vez instalados, descargan la totalidad de la cadena de bloques, convirtiéndose así nuestro dispositivo en un nodo más de la red Bitcoin, en el que se almacenará y, posteriormente, se actualizará una copia de la cadena de bloques.

En la actualidad la cadena de bloques completa ocupa, aproximadamente, unos 100 Gb. La primera vez que se ejecute el programa cliente instalado, tratará de descargar, construir índices y validar la totalidad de la cadena de bloques existente en ese momento lo que, debido a su volumen, podrá demorarse varios días dependiendo de la velocidad de nuestra conexión y de la capacidad de procesamiento de nuestro dispositivo. Una vez completado este proceso la copia de la cadena de bloques descargada se irá sincronizando automáticamente.

Existen, no obstante, clientes ligeros (MultiBit[21], Electrum[22], etc.) que solamente descargan las cabeceras de los bloques disponibles en la cadena, lo que reduce los tiempos anteriores y, a la vez, es suficiente para determinar si una transacción pertenece, o no, a un bloque sin necesidad de descargar la cadena completa.

Como antes se ha señalado, para realizar transacciones no hay más que enviar un mensaje a la red Bitcoin utilizando para ello nuestra aplicación cliente e indicando, al menos, el remitente, el destinatario y la cantidad de bitcoins a transferir. Para asegurar que el mensaje es auténtico e íntegro, es decir, para acreditar la identidad del remitente y que el mensaje enviado no ha sido modi-

ficado, se utilizan técnicas de firma electrónica mediante criptografía asimétrica o criptografía de dos claves.

Para ello, las aplicaciones cliente generan pares de claves criptográficas compuestos, cada uno de ellos, por una clave pública y una clave privada, las cuales no son independientes, sino que se encuentran ligadas matemáticamente. Las claves públicas son cadenas alfanuméricas de 26 a 35 caracteres que comienzan por un '1' o un '3', un ejemplo de clave pública sería: 1Hg7wA7JMuMtpXbPMLi6XXh1XwrKK4fwUC y la clave privada que le correspondería sería: 5J1D73SKtkgjtBGUKPL6EASDbGCKJ226prTAPmnhkyByvpU5deC.

Si la aplicación cliente utilizada está correctamente implementada, los métodos criptográficos utilizados garantizan que cada pareja de claves solo se puede generar una vez, de modo que se puede asumir que no es posible que dos personas tengan una misma pareja de claves. Por otra parte, una misma persona puede tener más de una pareja de claves, lo que puede ser útil, por ejemplo, para separar y distinguir entre monedas virtuales con orígenes y propósitos distintos.

La clave privada debe mantenerse secreta, puede considerarse como nuestra firma personal, permite encriptar y firmar electrónicamente los mensajes que se envíen a la red Bitcoin, y es el único medio que permite acceder y gestionar las monedas virtuales asociadas a la misma. Por tanto, su pérdida supone la pérdida definitiva de estas monedas y, del mismo modo, si un tercero hace uso de nuestra clave privada podrá disponer de nuestros bitcoins como quisiera.

La clave pública, por el contrario, puede darse a conocer libremente, es el único medio que nos permitirá descifrar los mensajes encriptados o firmados con la clave privada asociada a ella pero, además, en el protocolo Bitcoin, es lo que permite identificar a un usuario[23], es decir, actúa de modo semejante a un nombre de usuario o dirección de correo electrónico.

De esta forma, cuando mediante la aplicación cliente, se vaya a realizar una transferencia de bitcoins a otro usuario, en el campo destinatario habrá de introducirse la clave pública de este. Si dicha clave se introduce erróneamente (por ejemplo, si se especifica la de un usuario distinto a aquel a quien queremos enviar la transferencia), y dado que en Bitcoin las transacciones son irreversibles, es decir, una vez realizadas estas no se pueden volver atrás, se habrá perdido la cantidad transferida.

Por tanto, para evitar las pérdidas de monedas, por alguno de los motivos expuestos anteriormente, será necesario ser especialmente cuidadoso tanto en la custodia de las claves privadas como en la especificación de las claves públicas de los destinatarios de una transferencia ya que, como se ha dicho, en el sistema Bitcoin no hay nadie ante quien presentar una reclamación y el resto de usuarios, en principio, nos son desconocidos.

2. Privacidad

Con ello llegamos a la cuestión de la anonimacidad o privacidad de Bitcoin. Cuando se instala una aplicación cliente no es necesario introducir ningún dato personal y si, en vez de utilizar alguna de estas aplicaciones se opta por usar alguna de las webs que permiten operar en dicha red, a lo sumo se deberá especificar una dirección de correo electrónico que, no obstante, puede ser una dirección creada al efecto en alguno de los muchos servicios de correo gratuitos en los que tampoco es necesario introducir nuestros datos personales reales.

Como consecuencia de todo ello, en principio, no es posible conocer la identidad real de la persona que está detrás de una concreta clave pública.

Sin embargo, existen medios indirectos para tratar de obtener indicios sobre la identidad de un usuario determinado o, al menos, el terminal desde el que accede habitualmente a la red, mediante técnicas de análisis de tráfico, identificación de ip, etc., aunque estos mecanismos también pueden burlarse utilizando herramientas que permiten ocultar o enmascarar las direcciones ip como, por ejemplo, la red TOR.

Tampoco el análisis de los flujos monetarios a favor de una determinada persona garantiza ningún resultado en esta materia en cuanto que, como se ha dicho, dicha persona puede crear tantas parejas de claves, o usuarios del sistema, como quiera y, por tanto, podrá crear una pareja de claves para cada una de las transacciones que se hagan a su favor o, incluso, varias para cada una de ellas.

De esta forma la única vía de investigación, frente a los usuarios que tratan de preservar su identidad por los anteriores medios u otros semejantes, es el análisis de los vínculos entre las transacciones[24], que es información pública. No obstante, existen otras criptomonedas que incluso permiten eludir estas líneas de investigación, como Zcash[25], que oculta las direcciones de emisor y receptor, así como la cuantía de las transacciones, de tal forma que solo quienes tengan una clave de visualización podrán ver el contenido de las operaciones.

Todas estas dificultades, han hecho que gobiernos y organizaciones internacionales hayan comenzado a concienciarse del peligro que representan las monedas virtuales para la lucha contra el blanqueo de capitales. Así, por ejemplo, la Comisión Europea aprobó, el pasado 7 de julio, la propuesta de Directiva COM (2016) 450 final 2016/0208 (COD)[26], de modificación de la Directiva de Prevención de Blanqueo de Capitales (EU) 2015/849 y en la que ya se incluye a las agencias o plataformas de cambio de monedas virtuales bajo la regulación de prevención de blanqueo de capitales y la financiación del terrorismo, de tal forma que, dichas agencias y plataformas, deberán aplicar controles e identificar a quienes soliciten el cambio entre monedas virtuales y reales, así como denunciar cualquier operación sospechosa. Conforme al texto anterior, los Estados miembro deberían haber modificado sus respectivas normativas sobre blanqueo de capitales, en dicho sentido, antes del pasado 1 de enero de 2017.

3. TRANSACCIONES

3.1. Funcionamiento de los procesos de firma electrónica en los sistemas de criptografía asimétrica

El proceso de firma electrónica en este tipo de sistemas, se lleva a cabo del siguiente modo:

— En primer lugar, al mensaje se le aplica una función hash criptográfica con el fin de obtener su huella digital o código hash. Por tanto, las funciones hash devuelven, para el elemento que se les haya pasado como entrada (texto, imágenes, video, etc.), un resumen cifrado consistente en una cadena alfanumérica de longitud fija.

Existen numerosas funciones o algoritmos de hash, como las familias MD (MD2, MD4, MD5), SHA (SHA-0, SHA-1, SHA-2, SHA-3), RIPEMD (RIPEMD-128, RIPEMD-160, RIPEMD-256, RIPEMD-320), etc. El sistema Bitcoin hace un amplio uso de este tipo de algoritmos, no solo para la firma de mensajes sino también para otro tipo de tareas como la generación de direcciones, la minería de bitcoins, etc.; siendo uno de los más utilizados el algoritmo SHA-256, perteneciente a la familia SHA-2. Por ejemplo, el código md5 del párrafo primero del artículo 1 de la Ley Hipotecaria de España[27] que dice: «*El Registro de la Propiedad tiene por objeto la inscripción o anotación de los actos y contratos relativos al dominio y demás derechos reales sobre bienes inmuebles*.» es: 7fc58fd522e15898ccf8e65ddf80697f, mientras que su código SHA-1 es: f1a5cb06a5cae6425a34ec11cc1314112192811d y su código SHA-256: d6c59ecaa6f1cd80cb1ff044d67134a16e23e83d3c47335af18ff7226a72957b.

Las funciones hash criptográficas tienen varias características importantes:

- Su cálculo es muy sencillo, en términos de tiempo y de capacidad de cálculo necesaria, pero, inversamente, la obtención de una entrada a partir de su código hash es prácticamente imposible.
- Entradas iguales siempre producen códigos hash iguales y entradas diferentes siempre producen códigos hash diferentes, por lo que un determinado código hash identificará inequívocamente la entrada de la que proviene. Así, por ejemplo, los códigos md5, SHA-1 y SHA-256 para el mismo texto de antes pero sin el punto final, es decir: «*El Registro de la Propiedad tiene por objeto la inscripción o anotación de los actos y contratos relativos al dominio y demás derechos reales sobre bienes inmuebles*» serían, respectivamente: a2be77b72247e97489ea6a743c203579, f9653976b98cbd788dcd138ae84ff1e8846522d6 y 7eb3efbbebe731b13df4a8fe678256e0161d7afd1ec696d0eb77a4782a20c9df.
- Y, por último, es imposible predecir cualquier código hash a partir de otros previamente capturados. En relación con ello, en los ejemplos ante-

riores se puede comprobar la gran disparidad que existe entre los distintos resultados por el simple hecho de quitar un punto final.

— En segundo lugar, a la huella digital del mensaje, así obtenida, se le aplica una segunda función criptográfica para firmarla con la clave privada del usuario remitente. El resultado obtenido es la firma electrónica del mensaje.

Esta segunda función criptográfica, por tanto, tiene dos entradas: la huella digital del mensaje y la clave privada del usuario y se caracteriza porque su resultado solo puede descifrarse (y así obtener nuevamente la huella digital del mensaje enviado) mediante la clave pública de dicho usuario.

— A continuación, se encapsula en un solo fichero tanto el mensaje original, como la clave pública del remitente y la firma electrónica del mensaje y se envía al destinatario.

— Por último, el destinatario, al recibir dicho fichero encapsulado usará la clave pública del remitente para descifrar la firma electrónica, incluida en el fichero, y obtener la huella digital o código hash del mensaje que calculó el remitente.

El destinatario también calculará la huella digital del mensaje original, aplicándole el mismo algoritmo que el remitente, y si esta última huella coincide con la obtenida al descifrar la firma electrónica, se habrá garantizado que el mensaje no ha sido modificado y que ha sido emitido por el titular de la clave privada que se ha utilizado para firmar electrónicamente el mensaje.

3.2. Operativa de las transacciones

Hasta ahora se ha visto cómo se utilizan los sistemas de criptografía asimétrica para garantizar la autenticidad e integridad de la mensajería utilizada para realizar una transacción, no obstante, es necesario detenerse no solamente en este aspecto sino también en cómo se determinan las monedas virtuales que un usuario tiene disponibles en un momento dado y como se almacenan las transacciones realizadas.

A este respecto, cabe señalar que en el sistema Bitcoin no se mantiene una tabla de saldos en la que se van actualizando la cantidad de monedas que cada uno de los usuarios tiene disponibles en un momento dado. Por el contrario, el sistema lo que hace es guardar la totalidad de las transacciones que se van realizando, estableciendo enlaces entre ellas que relacionan las transacciones actuales con las anteriores.

De esta forma, para que un usuario: *X* pueda transferir una cantidad: *z* a otro usuario: *Y*, *X* debe tener a su favor, es decir, apuntando a su identificador o clave pública, un número de transacciones sin usar cuyo importe total sea, al menos, la cantidad *z*.

A las transacciones que apuntan al usuario *X*, y que van a ser utilizadas por este para hacer la transferencia al usuario *Y*, se les denominan entradas de esta última transacción y a las direcciones del usuario o usuarios a cuyo favor se hace la transferencia, en este caso la del usuario *Y*, se les denomina salidas.

Toda transacción, por tanto, habrá de estar compuesta por una serie de elementos que, al menos, serán: entradas, salidas, la cantidad a transferir y su identificador de transacción, que no es más que el código hash que se calcula a partir de todo el conjunto de información que compone la propia transacción.

En la figura 1 se puede ver una representación gráfica de la implementación de este *árbol de transacciones* para una transacción concreta, cuyo identificador es: 9844f73174f4dcf249fb1c8c640b505962c3d6eeacf684b7e-808da752c68cb1d y que fue realizada por el usuario con clave pública: 1DpkGipzLb32KcqYbwCDbQNmJgrr6oMyip para transferir un total de 1,71835096 BTC en favor del usuario con identificador: 1Lnt32vFqwz7WkqS1KXN2xwX-2DZ4Nj4j1m.

En dicha figura únicamente se muestran los tres primeros caracteres de los identificadores de las diversas transacciones y usuarios involucrados. En ella se pueden ver las transacciones pasadas, o entradas de la transacción actual, que apuntaban al usuario: 1DpkGipzLb32KcqYbwCDbQNmJgrr6oMyip, y que fueron utilizadas por este para realizar el pago a favor del destinatario antes indicado.

Dichas entradas sumaban un total de 1,72951046 BTC que se desglosan en las siguientes salidas: una comisión de 0,00112312 BTC a satisfacer al minero que mine el bloque en el que se incluya la transacción (en la forma que luego se verá), los 1,71835096 BTC a pagar a favor del usuario: 1Lnt32vFqwz7WkqS-1KXN2xwX2DZ4Nj4j1m y el cambio que se devuelve al pagador, el usuario: 1DpkGipzLb32KcqYbwCDbQNmJgrr6oMyip, lo que también genera una salida en la transacción.

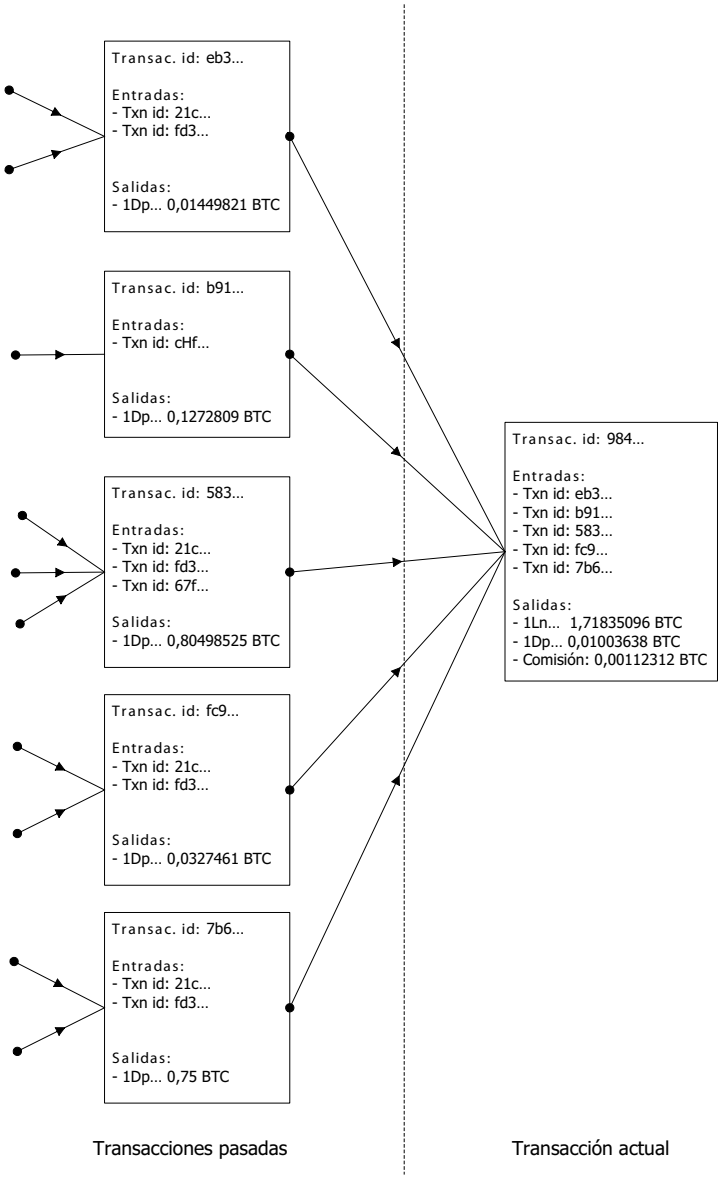
En la figura 2 se muestra la salida que proporciona la página web blockexplorer.com si se consulta en ella esta transacción y en la que, entre otros elementos, se ha resaltado el bloque de entradas, para las que esta página muestra, no los identificadores de transacción, sino los códigos de los usuarios que las realizaron a favor del que ahora dispone de los fondos.

Una vez verificada y realizada una transacción por un nodo, se difunde por el resto de la red para que sea nuevamente verificada, confirmada e incluida en la cadena de bloques por los mineros y almacenada en la copia local de cada nodo.

Resumiendo lo hasta ahora visto se puede concluir que Bitcoin, mediante el establecimiento de una red Peer-to-Peer y el uso de criptografía asimétrica, implementa un sistema que:

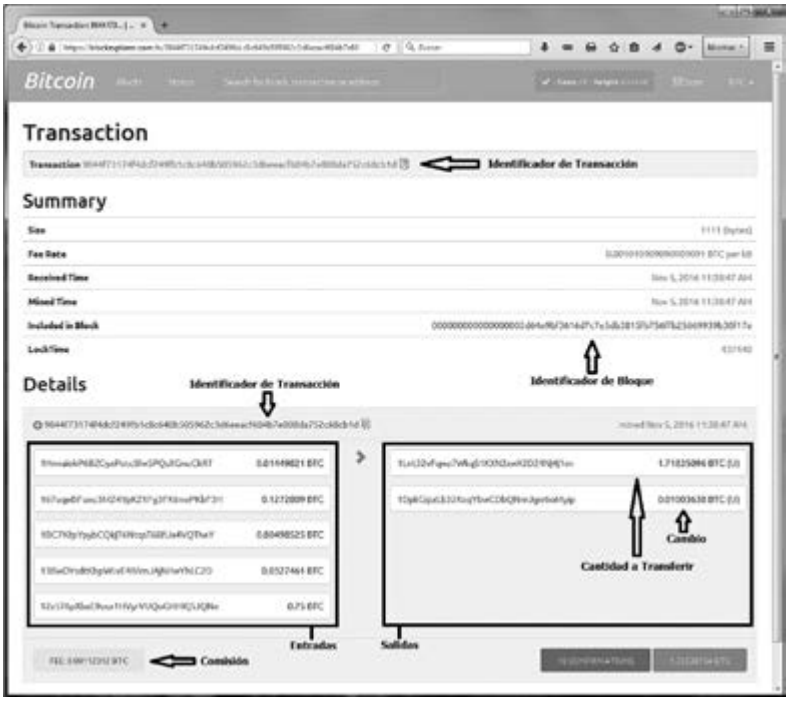
— Permite el envío de mensajes de transacción entre sus usuarios.
— Teóricamente, y mediante la utilización de los mecanismos de verificación de firma digital explicados, puede asegurar que el titular del

Figura 1



Transacción: 9844f73174f4dcf249fb1c8c640b505962c3d6eeacf684b7e808da752c68cb1d

Figura 2



Datos proporcionados por la página web blockexplorer.com para la transacción: 9844f73174f4dcf249fb1c8c640b505962c3d6eeacf684b7e808da752c68cb1d

correspondiente par de claves pública y privada es el remitente de un determinado mensaje de transacción.

— Gestiona un registro contable en el que lo que se almacena no son los saldos a favor de cada usuario sino el historial completo de todas las transacciones realizadas, así como las relaciones entre ellas.

— Y en el que la posibilidad de llevar a cabo una nueva transacción depende de la validez de las anteriores. Esta validez se comprueba por cada nodo de la red, para todo el histórico de transacciones, al instalar la aplicación cliente y descargar la cadena de bloques completa existente en ese momento y, para cada nueva transacción, en el momento de realizar esta y respecto de las transacciones anteriores, o entradas, involucradas en la misma.

Otras características de las transacciones son las siguientes:

— Cada bitcoin se divide en cien millones de partes que no reciben el nombre de céntimos ni de peniques sino de *satoshis* (en honor al creador del sistema), siendo la transferencia mínima, que se puede realizar, de: 546 *satoshis* o 0,00000546 BTC.
— Cada entrada, de una nueva transacción, ha de usarse por completo, de tal forma que, si el número de bitcoins asociado a esa entrada es superior a la cantidad que se quiere transferir, dicha transacción tendrá una salida de *vuelta* o *cambio* mediante la que se devolverá al pagador, o a otro usuario que este especifique, la diferencia.
— Cada transacción puede tener una o más entradas e, igualmente, una o más salidas. A su vez, las entradas pueden ser de uno solo o de varios usuarios, en cuyo caso se requerirá que todos ellos firmen la transacción, y las salidas también pueden dirigirse a un único o a varios destinatarios.
— En la actualidad, no es obligatorio el pago de una comisión al realizar una transacción (ya que todavía existen mineros que validan este tipo de transacciones), no obstante, si se paga, la confirmación de dicha transacción se obtendrá con mayor rapidez. La cuantía de estas comisiones dependerá, no de la cantidad a trasferir, sino del número de entradas y salidas de la transacción de que se trate.
— Una vez que se firma y se envía un mensaje de transacción, este llegará a su destinatario en segundos, no obstante, se tratará de una transacción no confirmada, es decir, una transacción que todavía no forma parte de ningún bloque en la cadena de bloques. Por tanto, cuando una transacción recibe la primera confirmación significará que se ha integrado en un bloque para formar parte de la cadena de bloques.
— Una transacción, a pesar de no estar confirmada, se puede utilizar como entrada en una nueva transacción, aunque esto no es recomendable. Las confirmaciones proporcionan seguridad a los destinatarios de las transacciones, al asegurar su titularidad sobre las monedas recibidas y les protegen frente a los ataques de doble gasto y frente a los ataques del 51%, que luego se verán.
— Bitcoin soporta un lenguaje de programación: el Bitcoin Scripting, que es el lenguaje que utiliza internamente el sistema para sus operaciones como el envío de transacciones, el intercambio de información entre nodos, etc., pero que también permite introducir código en las transacciones que se ejecutará con estas, aunque la mayor parte de las aplicaciones cliente ocultan esta posibilidad a los usuarios.
— Por último, debe recordarse que las transacciones no pueden revertirse. Si, por ejemplo, se realiza una transacción indebida, se transfiere una cantidad superior a la necesaria, se envía a un destinatario erróneo,

etc., no habrá forma de volver atrás estas operaciones, salvo que se tenga algún medio para contactar con sus destinatarios, estos acepten la reclamación y realicen la correspondiente devolución a nuestro favor.

4. La cadena de bloques

Hasta ahora se ha descrito el protocolo que Bitcoin establece para la realización de transacciones entre los distintos usuarios, pero no se han mencionado, más que incidentalmente, las cadenas de bloques, por lo que el lector que haya llegado hasta este punto probablemente se estará preguntando si, después de todo, estas cadenas tienen algún papel en el sistema, a pesar de la importancia que, en la introducción de este artículo, se ha dicho que tenían.

Como se recordará, los creadores de Bitcoin trataron de establecer un sistema totalmente distribuido que permitiera el intercambio de dinero y en el que era imperativo prescindir de cualquier elemento que fuese necesario para su funcionamiento pero que pudiera estar controlado por una o por unas pocas manos.

Ello implica que no existe, por ejemplo, una única señal horaria que sea suministrada a los distintos usuarios y nodos para establecer el momento exacto en el que se realiza una transacción y, por otro lado, tampoco se puede tener en cuenta el sellado de tiempo que cada usuario pudiera haber puesto en el momento de firmar y enviar sus transacciones, ya que aquella marca horaria podría ser fácilmente manipulable.

En esta situación y teniendo en cuenta la arquitectura general del sistema, en el que como se ha visto las transacciones se comunican progresivamente de nodo a nodo, no puede garantizarse que el orden en el que un nodo de la red recibe dichas transacciones es el mismo en el que fueron realizadas.

Como consecuencia de lo anterior se abriría la puerta al fraude y, en concreto, a la posibilidad de llevar a cabo ataques de doble gasto.

Efectivamente, un usuario malintencionado podría realizar una transacción y a continuación, antes de que esta fuese validada, desde otro dispositivo realizar una nueva transacción utilizando las mismas entradas que en la anterior. Debido a los diferentes tiempos de propagación en la red habrá nodos que recibirán la segunda transacción antes que la primera —y por ello considerarán esta última como inválida— y viceversa, con lo que no habría acuerdo en cuanto a que operaciones deben considerarse válidas.

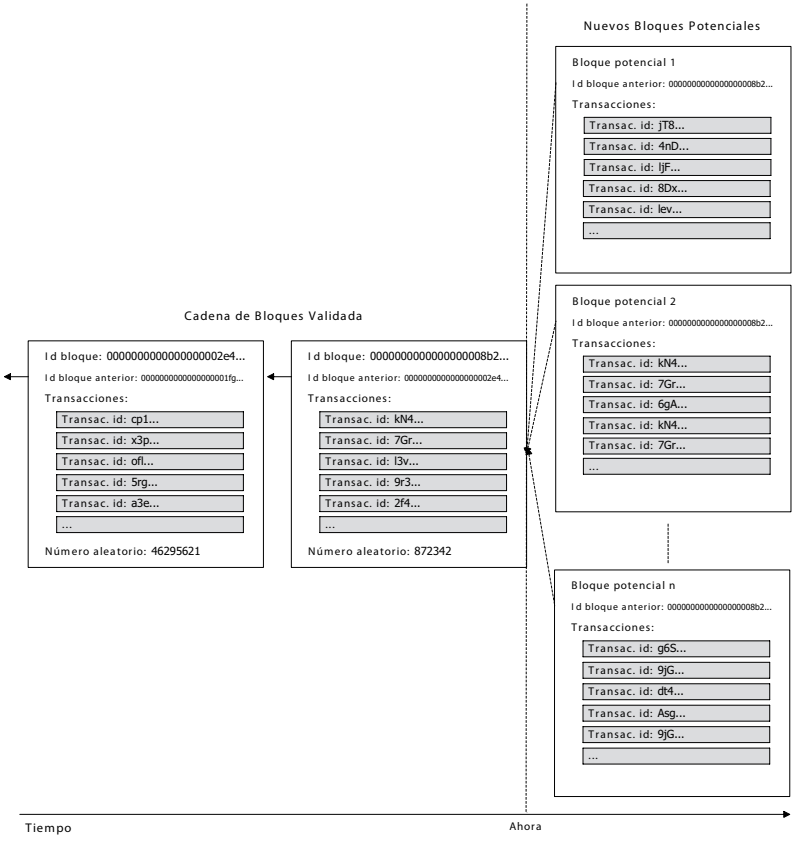
La solución que se ha implementado en Bitcoin para dar solución al anterior problema es, precisamente, la cadena de bloques que no es, por tanto, más que un mecanismo para ordenar las transacciones.

De esta forma las transacciones se agrupan en bloques y estos se enlazan entre sí, formando la cadena de bloques. En la figura 3 puede verse una representación de la cadena de bloques y de sus distintos componentes.

Cada bloque tiene una estructura definida en la que, al menos, se habrá de incluir el identificador de bloque, el identificador o referencia al bloque anterior[28], el conjunto de transacciones que se agrupan en el propio bloque (cada una de las cuales incluirá, al menos, los datos que se han visto anteriormente, es decir: entradas, salidas, importe, identificador de transacción, etc.) y un número aleatorio (que recibe el nombre de *nonce*) cuya función se verá más adelante.

Por tanto, en Bitcoin se gestionan dos estructuras paralelas y con funciones diferentes. En primer lugar, el árbol de transacciones cuya función es determinar la titularidad de las monedas y, en segundo lugar, la cadena de bloques que tiene por objeto ordenar dichas transacciones.

Figura 3
Representación esquemática de la cadena de bloques



Las transacciones incluidas en un mismo bloque se considera que se han producido al mismo tiempo, mientras que la referencia que cada bloque contiene al anterior permite ordenarlos uno tras otro en el tiempo.

Cualquier nodo puede agrupar transacciones que todavía no forman parte de ningún bloque —es decir, transacciones no confirmadas—, formar un nuevo bloque potencial y difundirlo al resto de nodos como propuesta de siguiente bloque en la cadena.

Dado que los distintos nodos de la red pueden realizar diferentes propuestas de nuevos bloques potenciales, es necesario establecer un criterio que permita decidir cuál de estos nuevos bloques potenciales debe ser considerado el siguiente bloque de la cadena.

Este criterio no puede ser el orden de recepción de las nuevas propuestas de bloques ya que, como se ha visto para el caso de las transacciones y como consecuencia de las diferentes velocidades de propagación de la información entre los nodos de la red, ello podría dar lugar a decisiones contradictorias entre dichos nodos.

Al contrario, el criterio por el que se opta en Bitcoin es considerar válido el nuevo bloque propuesto que incluya la solución a una búsqueda matemática. Esta solución es el número aleatorio, que se ha mencionado anteriormente al exponer la estructura de los bloques, y que aparece en cada uno de los bloques validados de la figura 3.

Estas búsquedas matemáticas son realizadas por los nodos de la red que actúan como mineros y consisten, una vez más, en el cálculo de un hash. En este caso, el hash se calcula a partir de los datos que conforman cada nuevo bloque propuesto[29].

En concreto, dicho cálculo, se lleva a cabo sobre la estructura del siguiente conjunto de datos: identificador del último bloque de la cadena, el conjunto de transacciones que se integran en el nuevo bloque propuesto sobre el que se realiza el cálculo y un número aleatorio o *nonce*[30].

Para que el nuevo bloque sea considerado válido y, por tanto, el siguiente bloque de la cadena de bloques, el hash calculado debe estar por debajo de un determinado valor o, dicho de otra forma, debe tener un número determinado de ceros al principio (como ejemplo se puede ver el identificador de bloque que se muestra en la figura 2).

Si el hash no cumple las anteriores condiciones se cambia el número aleatorio utilizado por otro distinto y se vuelve a realizar el cálculo del hash y así sucesivamente hasta que se obtiene el código hash con las condiciones requeridas.

Teóricamente, de media serían necesarias miles de millones de operaciones de cálculo de hash como las anteriores para dar con la solución que valide una concreta propuesta de bloque, lo que, a un solo ordenador, le llevaría años. No obstante, el propio sistema se autorregula, teniendo en cuenta la potencia de cálculo de todos los nodos de la red Bitcoin que actúan como mineros, ajustando

cada dos semanas la dificultad de la búsqueda para que el tiempo medio de validación de bloque se mantenga alrededor de los 10 minutos.

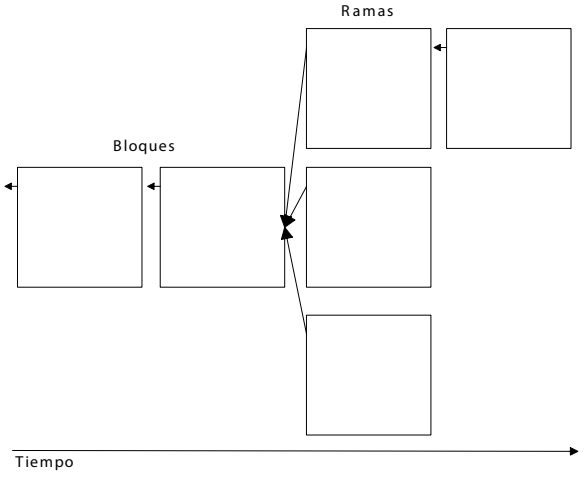
Este periodo de 10 minutos es un compromiso entre el tiempo de confirmación y la probabilidad de que se produzcan ramas o bifurcaciones en la cadena (que se verán a continuación). Un intervalo de tiempo más corto en la confirmación de los bloques, haría que las transacciones se ejecutaran más rápidamente, pero aumentaría la probabilidad de que se produjeran ramas en la cadena de bloques y viceversa.

Una vez que se encuentra el número aleatorio o *nonce* que produce el hash con las características mencionadas, se considera que se ha validado la propuesta de bloque y el minero que ha resuelto la búsqueda lo difunde por la red para que sea verificado por el resto de nodos y aceptado como siguiente bloque de la lista. En el nuevo bloque se incluirá el hash calculado, que será el identificador del propio bloque, el hash del bloque anterior, el conjunto de transacciones que conforman el nuevo bloque, así como el número aleatorio que resuelve la búsqueda matemática expuesta.

Con esta configuración, sin embargo, no se resuelven todos los problemas ya que es posible que dos o más mineros validen simultáneamente propuestas de nuevos bloques diferentes, dando lugar a varias ramas posibles en la cadena.

En este tipo de situaciones cabe preguntarse cuál de los distintos primeros bloques, de las diferentes ramas existentes, habrá de ser considerado como bloque anterior al intentar validar un nuevo bloque o, en otras palabras, en que

Figura 4
Ramas en la cadena de bloques



rama deben integrarse los nuevos bloques. La regla es que, si todas las ramas tienen el mismo número de bloques, cada minero seguirá validando bloques considerando como anterior el último de los bloques de la primera de las ramas que hubiera recibido. No obstante, en el momento en el que una rama sea más larga que las demás automáticamente se comenzará a minar sobre esta lo que, además, provocará que el resto de ramas se eliminen y que todas las transacciones que estaban incluidas en los bloques que integraban estas ramas más cortas y que, por tanto, eran consideradas transacciones confirmadas, pasarán a formar parte, nuevamente, del conjunto de transacciones no confirmadas y tendrán que ser incluidas en un bloque posterior que, a su vez, habrá de ser minado para poder integrarse otra vez en la cadena de bloques.

Desafortunadamente, esta última circunstancia abre la posibilidad a que un usuario malintencionado pueda llevar a cabo dobles gastos (que era precisamente lo que se trataba de evitar mediante la cadena de bloques) por medio de los ataques del 51%.

Efectivamente, imaginemos que un usuario *X* realiza una transacción a favor de otro usuario *Y*. Este usuario *Y*, por su parte, espera a que dicha transacción sea confirmada para prestar el servicio o enviar el producto adquirido por *X*. Mientras tanto, *X* mina su propia rama de bloques en la que incluirá una nueva transacción a partir de la misma entrada que utilizó para realizar el pago a favor de Y, pero para usarla en favor de un usuario diferente.

Cuando la transacción original a favor de Y se haya validado y dicho usuario Y, en consecuencia, realice el servicio contratado por *X*, este último envía a la red la rama minada por él, la cual, si es de mayor longitud que la rama que contenía la transacción original, sustituirá a esta y, por tanto, se producirá la desconfirmación de, entre otras, la transacción original a favor de *Y*.

Con ello, *Y* habrá perdido su dinero ya que cuando se trate de confirmar/minar nuevamente la transacción a su favor, el sistema detectará que la entrada utilizada por X para pagarle ya se ha gastado en otra operación y se invalidará.

Dado que X no puede modificar un bloque de la cadena sustituyendo una transacción por otra, ya que ello se detectaría inmediatamente mediante la verificación de hashes, la única vía que le queda es competir con el resto de nodos en una carrera matemática por construir una rama de mayor longitud que la construida por estos. Por ello se suele decir que, para tener éxito en este tipo de ataques, X debería controlar, al menos, más del 50% de la totalidad de la potencia de cálculo de todos los nodos/mineros que integran la red, de ahí el nombre de ataques del 51%.

Usualmente se considera que la probabilidad de que un ataque del 51% pueda tener éxito es despreciable, dado el elevado número de mineros que integran la red Bitcoin, pero que, en todo caso, se recomienda esperar a que una transacción sea confirmada al menos por seis nodos antes de realizar la correspondiente contraprestación.

La realidad, sin embargo, es que es posible demostrar[31] que:

— No es necesario controlar más de la mitad de la potencia de cálculo de la red Bitcoin, sino que, al contrario, es posible realizar con éxito, y con una probabilidad no nula, los ataques anteriormente descritos cualquiera que sea la potencia de cálculo de la que dispone un atacante.
— Cuanto mayor sea el número de confirmaciones que reciba una transacción más disminuye la probabilidad de éxito de un ataque de doble gasto. La velocidad en la disminución de dicha probabilidad dependerá de la potencia de cálculo de la que disponga el atacante.

  No obstante, ningún número de confirmaciones disminuirá la probabilidad de éxito a cero. Por el contrario, si el atacante dispone de más potencia de cálculo que el resto de la red (es decir, más del 50% de la totalidad de la misma), ningún número de confirmaciones reducirá la tasa de éxito por debajo del 100%. En realidad, un usuario malintencionado de este último tipo no solo podrá llevar a cabo un ataque de doble gasto respecto de cualquier transacción, sino que también podrá forzar que cualquier bloque no minado por él sea rechazado.
— La recomendación de esperar 6 confirmaciones, a la que me he referido anteriormente, está basada en la asunción de que es improbable que un atacante pueda controlar más del 10%[32] de la capacidad de cálculo de la red y de que una probabilidad de éxito en los ataques del 0,1 es aceptable. No obstante, si bien el criterio de las seis confirmaciones puede desincentivar al atacante ocasional no supone ningún obstáculo insalvable para un atacante que efectivamente disponga de más de aquel 10% de la potencia de cálculo.

5. El problema del tamaño de los bloques

Con el fin de dificultar los ataques de denegación del servicio, en el momento de diseñar el protocolo Bitcoin, se fijó un tamaño máximo de bloque relativamente bajo, concretamente en un máximo de 1 MB[33]. La consecuencia de esto es que la capacidad máxima de procesado de transacciones por unidad de tiempo se reduce a, aproximadamente, 7 transacciones por segundo dado que un bloque se mina cada 10 minutos y el tamaño de cada transacción es alrededor de 250 bytes, con lo que en cada bloque se pueden agrupar, como máximo, unas 4000 transacciones[34].

Comparativamente, los operadores financieros ordinarios tienen velocidades de procesamiento mucho mayores (VISA, por ejemplo, puede procesar más de 56.000 transacciones por segundo[35]) lo que dificulta que Bitcoin, en su configuración actual, pueda llegar a ser adoptado como un sistema de

pagos global, dados los problemas de escalabilidad que podrían presentarse en el futuro.

Ello ha provocado que el tamaño de los bloques se haya convertido en una de las preocupaciones principales dentro de la comunidad Bitcoin y, además, ha producido una fuerte división, enfrentamientos y abandonos entre el núcleo de desarrolladores principales, los mineros y las empresas que prestan servicios alrededor de Bitcoin y respecto de si, efectivamente, la limitación en el tamaño de los bloques es un problema y, en su caso, cual es la solución que se le debe dar.

A este respecto se han dado diferentes argumentos a favor y en contra de aumentar el tamaño de bloque:

- A favor:
  - La ya apuntada necesidad de aumentar la velocidad de procesamiento de las transacciones para poder competir con otros sistemas de pagos ya establecidos.
  - Si no se aumenta la velocidad de procesamiento indicada las comisiones que los usuarios han de pagar a los mineros para que estos validen y minen sus transacciones lo antes posible, irán aumentando progresivamente, lo que desincentivará la utilización del sistema.
  - Se crearía espacio para la implementación de extensiones del protocolo Bitcoin como, por ejemplo, las llamadas *metacoins, metachains o blockchain apps* (Colored Coins, Mastercoin, Counterparty, etc.). Estas extensiones se caracterizan por compartir la cadena de bloques de Bitcoin, pero añaden nuevas capas al protocolo que permiten incluir datos adicionales en las transacciones.

- En contra:
  - Unas comisiones más altas, o simplemente la necesidad de pagar algún tipo de comisión, permitirá eliminar las transacciones spam e incentivar económicamente a los mineros para que no abandonen el sistema, sobre todo teniendo en cuenta que la recompensa que reciben por minar bloques se reducirá progresivamente, como se expone en el epígrafe siguiente.
  - Aumentará la probabilidad de que se produzcan ramas en la cadena y, por tanto, una mayor probabilidad de que se puedan dar situaciones de doble gasto, ya que el mayor tamaño de los bloques implicará una velocidad de propagación más lenta y también requerirá una mayor capacidad de procesamiento en los nodos.
  - Esta menor velocidad de propagación y la necesidad de una mayor capacidad de procesamiento provocará una mayor centralización de la red Bitcoin ya que se reducirá el número de mineros, como consecuencia de

los aumentos de costes, y, por tanto, la seguridad del sistema también disminuirá.

— Dado que habría más transacciones en cada bloque, el número de bloques a minar sería menor y como quiera que los mineros reciben una recompensa por bloque minado, su retribución disminuiría, lo que agravaría el problema señalado en el punto anterior.

— El aumento del tamaño de los bloques sería, en todo caso, una medida transitoria ya que ningún tamaño específico asegurará que no se puedan presentar problemas de escalabilidad en el futuro.

— Sería necesaria una bifurcación dura u obligatoria (hard fork) de la cadena de bloques ya que se implementaría una nueva versión del sistema que no sería totalmente compatible con la anterior.

Se trataría, por tanto, de una bifurcación planificada que supondría el abandono de la antigua cadena de bloques lo que requeriría la aceptación unánime de la nueva versión por todos los actores del sistema, así como su migración a la nueva cadena.

No obstante, dado su número y los fuertes intereses contrapuestos de los distintos tipos de usuarios, tal unanimidad se estima prácticamente imposible y la realización de esta bifurcación dura traería consecuencias catastróficas para la reputación y el precio de las bitcoins.

En cualquier caso, lo cierto es que se han publicado diversas propuestas para la ampliación del tamaño de los bloques (Bitcoin Improvement Proporsal o BIP)[36], siendo algunas de las más conocidas: Bitcoin Classic, Bitcoin Unlimited o Bitcoin XT. Esta última, por ejemplo, fue publicada en agosto de 2015 por Gavin Andresen y Mike Hearn (ambos habían sido anteriormente desarrolladores principales de Bitcoin) y consiste en una variante de la propuesta BIP 101, es decir, se trataría de aumentar el tamaño de los bloques, a partir del pasado 11 de enero de 2016, de 1 Mb a 8 Mb, duplicándolo nuevamente cada dos años, hasta alcanzar los 8192 MB, pero añadiendo, además, mejoras en el protocolo para dificultar el doble gasto, los ataques DDoS, mejorar la identificación de los nodos, etc. Los proponentes, además, defendían que Bitcoin XT debía ser adoptado obligatoriamente por todos los nodos, una vez que fuese aceptada, e instalada, por el 75% de los nodos mineros.

Sin embargo, su acogida entre la comunidad bitcoin no fue la esperada por sus autores (en la dirección: http://xtnodes.com/#all_nodes, se puede consultar el número de nodos que utilizan Bitcoin XT, y también Bitcoin Core o tradicional, Bitcoin Classic y Bitcoin Unlimited, frente al total de la red) ya que Bitcoin XT apenas se encuentra instalada en poco más del 1% de los nodos y, sin embargo, lo que si se ha producido, es una fuerte lucha interna, una suerte de guerra civil, en la comunidad bitcoin, empezando por el propio grupo de los cinco desarrolladores principales en el que dos de ellos (Gavin Andresen y

Jeff Garzik) defendían la realización de la bifurcación dura, antes mencionada, pero los otros tres la rechazaban totalmente.

Igualmente se han producido conflictos entre los mineros acompañados de ataques informáticos para colapsar los nodos que implementaban Bitcoin XT y también las empresas que prestan servicios alrededor de Bitcoin se han involucrado en este problema del tamaño de los bloques, así como en los conflictos descritos. Por ejemplo, algunas entidades como Blockstream han sido acusadas de oponerse frontalmente al aumento del tamaño de bloque exclusivamente por razones de lucro empresarial ya que, de esta forma, dichas empresas podían imponer la utilización de sus propias soluciones técnicas a los problemas derivados de mantener el tamaño actual[37] (en el caso de Blockstream su solución se denomina Lightning Network[38]), cobrando las correspondientes comisiones por su uso a los usuarios.

Todo esto provocó, finalmente, que en enero de 2016 Mike Hearn, comunicara su retirada en un amargo artículo[39] en el que anunciaba la venta de todos sus bitcoins, consideraba a Bitcoin como un experimento fallido y muerto y señalaba sus, a su juicio, numerosos problemas, entre los que mencionaba la ya indicada falta de capacidad para procesar el incremento futuro de transacciones, lo que producirá el consiguiente colapso y abandono del sistema; la monopolización de la práctica totalidad de la capacidad de minado por unos pocos grupos, que se oponen a cualquier modificación que pueda alterar su status actual lo que supone, además, la pérdida de control de Bitcoin por parte de los usuarios que era, precisamente, uno de los objetivos iniciales; también la falta de claridad respecto de la cuantía de las comisiones a pagar por la realización de las transacciones y su previsible rápido crecimiento en el futuro; la falta de democracia en la comunidad Bitcoin; etc.

En cualquier caso, el problema del tamaño de los bloques, y su consecuencia de la reducida capacidad de procesamiento de transacciones por unidad de tiempo, es, a día de hoy, un problema pendiente de solución.

6. Mineros

Como se ha visto una de las principales funciones de los nodos de la red que actúan como mineros es la construcción de la cadena de bloques. No obstante, también son el medio para la generación y distribución de nuevas monedas en el sistema ya que cada vez que un minero construye un bloque válido, recibe una recompensa en forma de bitcoins de nueva creación aunque, antes de recibirla, tendrá que esperar a que se hayan minado otros 99 bloques.

Cada 210.000 bloques minados, lo que, a la velocidad de minado de 10 minutos por bloque, ocurre aproximadamente cada cuatro años, la recompensa se reduce a la mitad y, precisamente, 2016 ha sido uno de los años en los que

dicha reducción ha tenido lugar y, así, mientras que hasta el pasado 9 de julio la cantidad pagada a los mineros por cada bloque minado era de 25 bitcoins, a partir de dicha fecha, se ha reducido a 12,5 bitcoins. Con esta progresión, el número total de bitcoins que se crearán será de, aproximadamente, 21 millones[40].

Además de la anterior, otra fuente de ingresos de los mineros, como ya se ha indicado, es el cobro de las comisiones que los usuarios hayan pagado para acelerar la confirmación de sus transacciones. En la actualidad, el pago de estas comisiones, si no se quiere ganar prioridad para confirmar la transacción, no es obligatorio, pero en el futuro, cuando cese el sistema de recompensas o cuando estas dejen de ser rentables, las comisiones serán la única fuente de ingresos de los mineros, por lo que la realización de transacciones dejará de ser gratuita y, probablemente, la cuantía de dichas comisiones crecerá de forma significativa.

En los primeros días del sistema los mineros tenían un carácter principalmente doméstico, utilizando sus propios ordenadores personales para llevar a cabo el minado de bitcoins. Este era el sueño libertario de Satoshi Nakamoto, dinero *cultivado* domésticamente. No obstante, conforme el valor de la moneda subía, los mineros comenzaron a profesionalizarse y a asociarse para repartirse las ganancias.

Paralelamente a todo ello, se comenzó a diseñar y construir hardware y procesadores a medida para el minado de bitcoins[41] (ASIC's: application-specific integrated circuits), que han venido doblando su capacidad de procesamiento, aproximadamente, cada 6 meses, alcanzando, en la actualidad, alguna de estas máquinas una capacidad de decenas de tera-hashes por segundo. Igualmente, surgieron startups que ofrecían la posibilidad de contratar capacidad de minado en la nube[42].

Todo ello ha conducido a la aparición de grandes *granjas* con miles de máquinas especializadas dedicadas exclusivamente al minado de bitcoins que, prácticamente, han eliminado la posibilidad de que los mineros domésticos u ocasionales puedan conseguir minar algún bloque. De esta forma cada vez es mayor la complejidad técnica y los recursos necesarios para el minado de bloques. Además, el minado es una actividad con un alto consumo energético, uno de los principales costes (alrededor del 90%) que deben afrontar los mineros es, precisamente, el coste de la electricidad y, como cualquier industria con un consumo intensivo de energía, la industria del minado de bitcoins ha terminado localizándose en lugares en los que los costes de la energía eléctrica son bajos, como por ejemplo: China, Georgia, Mongolia, Malasia, etc. —en los que la energía se genera principalmente a partir del carbón y las normas medioambientales no demasiado estrictas— o, también, en Islandia —que cuenta con abundante energía renovable y barata—.

Los mineros son imprescindibles para la seguridad de Bitcoin. Efectivamente, cuanto mayor sea la capacidad total de minado del sistema mayor será la

dificultad de la búsqueda matemática mediante la que se minan los bloques y, por tanto, menor será la probabilidad de que un minero, o un grupo de mineros, puedan llevar a cabo un ataque del 51%.

Si la capacidad total de minado es reducida, el sistema se autorregulará bajando la dificultad de la búsqueda matemática, para que el tiempo medio de minado por bloque se mantenga en 10 minutos, con lo que aumenta la probabilidad de que un agente externo con suficiente capacidad de minado se incorpore al sistema y pueda llevar a cabo los mencionados ataques del 51%. Además, debe tenerse en cuenta que, como se ha visto anteriormente, con una capacidad de cálculo significativa, aunque sea menor al 51% del total, la probabilidad de llevar a cabo ataques con éxito es muy elevada.

Por tanto, desde el punto de vista de la seguridad, la situación ideal sería que existiera una gran capacidad total de computación, pero distribuida entre un elevado número de mineros, de tal forma que ninguno de ellos por sí solo, o asociado con otros, pudieran atacar el sistema y, precisamente, con estas premisas se había diseñado Bitcoin.

Sin embargo, la creciente complejidad técnica y, también, los crecientes recursos financieros, materiales y humanos necesarios para minar las monedas favorecen la aparición de superestructuras o grupos de mineros. Así, por ejemplo, durante el pasado mes de abril más del 70% del total de transacciones fueron minadas por grupos chinos de minado y, más del 70% de aquel porcentaje por solo dos de estos grupos. En tiempos más recientes y, en concreto, en los cuatro días anteriores a la fecha de este artículo, el 50,1% de la capacidad de minado mundial estaba en manos de únicamente 4 de estos grupos y, solamente una docena de ellos, reunía más del 87% de la capacidad total de minado[43]. Todos estos datos demuestran que, en realidad, Bitcoin no es tan descentralizada como se quiere hacer ver y, también, que, como apuntaba Mike Hearn, sus usuarios han perdido el control del sistema.

Estas agrupaciones mineras también han sido señaladas como culpables de la progresiva obsolescencia técnica de Bitcoin, que no ha experimentado ningún cambio significativo en los últimos años, dado que estos deben ser aceptados por los mineros, mediante la instalación de las nuevas versiones en sus sistemas, las cuales no serán aceptadas si suponen una alteración del *status quo* que les pueda producir algún tipo de perjuicio o detrimento económico.

En cualquier caso, el futuro de los mineros es incierto ya que conforme vaya disminuyendo la recompensa que obtienen por el minado de bloques y esta actividad deje de ser rentable, se producirá la expulsión de muchos de ellos, lo que reducirá la seguridad del sistema y, con ello, la pérdida de usuarios y la pérdida de valor de la moneda por la desconfianza que se generaría.

En esta situación la única alternativa que tendrían sería el cobro de comisiones por transacción que pasarían a ser obligatorias y más elevadas que en la actualidad, lo que igualmente podría producir el abandono de usuarios.

En realidad, lo que Bitcoin hace no es eliminar los intermediarios sino sustituir unos por otros, es decir, sustituye a los operadores bancarios tradicionales por los mineros.

Como argumento a favor de Bitcoin se suele señalar que sus costes y comisiones son mucho más reducidas que las de la banca tradicional, lo que ocurre, sin embargo, es que, en la actualidad, la razón de que sus comisiones sean muy reducidas o inexistentes es que los mineros son retribuidos por el propio sistema, pero, como se ha visto, esto no será así en el futuro. Por otra parte, en el negocio bancario tradicional, además de existir una relación contractual donde se recogen los derechos y obligaciones para ambas partes, sus operadores están sujetos a las normas sobre transparencia y defensa de los consumidores, cuya aplicación se les puede reclamar; sin embargo, nada de esto existe en Bitcoin.

7. Cadenas de bloques públicas y privadas

Lo hasta ahora expuesto se refiere al funcionamiento de un sistema (Bitcoin) que implementa el protocolo de funcionamiento de una cadena de bloques con respecto a un problema concreto: un sistema de pagos global.

Desde el punto de vista de las credenciales o privilegios necesarios para el acceso, Bitcoin puede ser considerada como una cadena de bloques pública, en el sentido de que se diseñó para que fuera libremente accesible por cualquiera sin más requisitos que disponer de un dispositivo adecuado y una simple conexión a internet.

De esta forma cualquier persona puede consultar la información almacenada en la cadena de bloques, también puede incorporar nueva información realizando transacciones e incluso participar en la construcción de la propia cadena mediante el minado de bloques.

Las ventajas que aporta la tecnología de las cadenas de bloques son principalmente dos: en primer lugar, permiten validar y detectar fácilmente la modificación o la corrupción de la información y, en segundo lugar, que la totalidad de la información se encuentra replicada en cada uno de los nodos de la red, todo lo cual permite prescindir de los llamados *terceros de confianza*. Efectivamente, en las cadenas de bloques públicas cualquier usuario puede, no solo consultar la información almacenada en ella, sino que también puede verificar su integridad y autenticidad, en el caso de Bitcoin mediante la comprobación de firmas y el recálculo de hashes, y, en el caso de que alguna de estas comprobaciones falle, se puede acudir a la copia de la información que se almacene en cualquier otro nodo, hasta obtener alguna que supere todas las comprobaciones y pueda ser considerada correcta.

No obstante, pueden existir situaciones en que no sea conveniente que la información sea de libre acceso; situaciones en que deban exigirse determinados

privilegios para la incorporación de la información o supuestos en que deban establecerse ambas restricciones.

Es en este tipo de casos en los que las cadenas de bloques privadas tendrían aplicación. Dentro de esta categoría, por otra parte, se puede distinguir entre las cadenas completamente privadas y las consorciales[44]. Las primeras son aquellas en las que los permisos de escritura están centralizados en una sola organización mientras que los de lectura pueden ser igualmente centralizados, públicos o bien parte de la información es libremente accesible y parte no. Las consorciales, por su parte, son aquellas otras que son operadas por unas pocas organizaciones cada una de las cuales puede gestionar uno o varios nodos preseleccionados y en los que se confía para llevar a cabo las labores de minado.

Entre las ventajas de las cadenas de bloques privadas se encuentran:

— Se puede llevar a cabo adaptaciones a medida del protocolo.
— Aumenta la velocidad de procesamiento de transacciones al reducirse el número de nodos en los que, además, se confía, por lo que no es necesario que cada nodo verifique cada una de las transacciones y tampoco es necesario que el mecanismo de minado de bloques sea una búsqueda matemática, como la expuesta anteriormente para el caso de Bitcoin, pudiendo sustituirse por otros mecanismos más rápidos.
— Tampoco sería necesario el establecimiento de un testigo o token (como las bitcoins) ya que estos son usados en las criptomonedas para retribuir a los mineros y, en el caso de las cadenas de bloques privadas, la retribución suele obtenerse por otros medios.
— Como consecuencia de lo anterior el coste por transacción puede reducirse y las comisiones pueden establecerse y regularizarse para que sean previamente conocidas por todos.
— La confidencialidad de la información se refuerza si se restringen los permisos de acceso.

Sin embargo, las cadenas de bloques privadas contradicen algunos de los principios que inspiraron originalmente la tecnología. Recordemos que el objetivo de las cadenas de bloques era implementar un sistema con el que realizar transacciones de forma segura eliminando el factor humano, es decir, sin que fuese necesario ningún intermediario, tercero de confianza o entidad central, y sin que sus usuarios tuviesen que confiar, o incluso conocerse, entre sí.

Evidentemente, con las cadenas de bloques privadas una o unas pocas personas o entidades serán las que definan el funcionamiento general del sistema, las características de los nodos, formas de validación, etc. e, igualmente, se reduce el nivel de redundancia de la información por lo que no solamente se estaría volviendo a la centralización, sino que, desde el momento en el que se establezcan restricciones en el acceso a la información, también sería necesario confiar en los gestores del sistema.

Con ello se pierde cierta justificación en cuanto al recurso a la tecnología de las cadenas de bloques, pudiendo utilizarse otras diferentes para alcanzar los mismos objetivos.

III. CADENAS DE BLOQUES Y REGISTROS DE DERECHOS

1. Introducción

El principal objetivo de cualquier sistema jurídico, relacionado con los ámbitos inmobiliario y mercantil, es garantizar la seguridad jurídica de las transacciones que se producen en ellos y, en definitiva, servir de medio para alcanzar la seguridad económica y el fomento de la inversión y la riqueza. Por tanto, la seguridad jurídica, la confianza en el tráfico, la defensa de la propiedad, y el fomento del crédito fueron los factores determinantes en el nacimiento de los Registros de la Propiedad y Mercantiles.

En este sentido, instituciones, como el Banco Mundial, consideran los registros jurídicos de la Propiedad y Mercantiles fundamentales y esenciales para el desarrollo de una economía de mercado que funcione ya que mejoran la seguridad de la propiedad, disminuyen los costes de las transacciones y proporcionan un mecanismo de bajo coste para resolver las eventuales disputas sobre estas materias.

Efectivamente, el aseguramiento de los derechos y expectativas jurídicas a través de un sistema de publicidad registral es básico para el desarrollo económico de un país; dicho sistema se inserta en el principio de seguridad jurídica, sobre la que descansa la confianza en una determinada economía, soporta los flujos financieros de los que depende la inversión y el crecimiento económico e igualmente reduce el riesgo asociado a cualquier operación financiera, lo que se traduce en una disminución de los tipos de interés.

De esta forma, el Registro de la Propiedad publicita las titularidades sobre los inmuebles y las cargas que recaen sobre ellos, constituyendo, así, un catalizador esencial de la actividad económica, pues estimula la inversión, facilita el comercio y abarata el crédito. Al asegurar la propiedad, da a los propietarios confianza para invertir, pues ya no necesitan gastar recursos en proteger la posesión de sus bienes y hacer valer sus derechos. Asimismo, al clarificar quién ostenta los diversos derechos sobre cada propiedad, elimina los costes de transacción que, en forma de asimetrías o desigualdades informativas, aparecen entre las partes a la hora de contratarlos. Por último, al establecer quién es propietario de cada inmueble y qué cargas lo gravan, hace posible que los inmuebles se usen como garantía, lo que elimina el riesgo de insolvencia y abarata el crédito. De este modo, los recursos productivos se mueven fácilmente hacia quienes más los valoran, y pueden agotarse las oportunidades de especialización y desarrollo.

Igualmente, los Registros Mercantiles también desempeñan esta función de facilitadores de la actividad económica en cuanto que permiten la rápida identificación de operadores y patrimonios societarios y, al mismo tiempo, sus asientos protegen al que opera en el tráfico económico, de buena fe y confiando en sus pronunciamientos, reduciendo, así, los costes para hacer efectivos sus derechos.

Por ello, todo lo que contribuya a reforzar e incrementar los efectos del sistema registral redundará en beneficios para el sistema de seguridad jurídica preventiva, y en definitiva para la seguridad económica y para el desarrollo económico y social de los países, sus ciudadanos y empresas.

Indudablemente, en la tarea de maximizar dichos objetivos y, también, en la de acercar los servicios registrales a los ciudadanos, la tecnología es una poderosa herramienta y, de acuerdo con ello, por ejemplo, los registradores españoles, desde hace más de quince años, han venido realizando continuos desarrollos tecnológicos, demostrando así su compromiso y disposición para abordar toda clase de proyectos y servicios que permitan una mejor relación con el registro haciendo un uso efectivo de las nuevas tecnologías, pero sin reducir en modo alguno los objetivos finales de aquel, que no son sino el de proporcionar seguridad al tráfico, favorecer el desarrollo económico y la igualdad social.

A este respecto, debe tenerse en cuenta que el funcionamiento satisfactorio de una determinada institución depende, en gran medida, de la calidad de su arquitectura institucional y el uso de la tecnología puede ser de una gran utilidad para que un concreto modelo institucional funcione más eficiente y eficazmente. Pero para ello es necesario que el principal objetivo en la utilización de la tecnología sea, no una finalidad en sí misma, sino el eficiente funcionamiento de dicha arquitectura institucional.

Efectivamente, los sistemas registrales que se integran en los diversos diseños institucionales que sirven al principio de seguridad jurídica preventiva, son algo más que simples bases de datos o meros repositorios de información y, en este sentido, debe distinguirse entre la seguridad técnica o informática de la información registral —que desde luego es imprescindible para que aquel principio pueda ser efectivo— y la propia seguridad jurídica que se deriva de los pronunciamientos registrales, como consecuencia de los efectos *erga omnes* que, en los sistemas de registros de derechos, les reconoce el ordenamiento jurídico, y que es distinta de aquella seguridad técnica.

2. Breve idea de los principales tipos de Registros de la Propiedad[45]

En relación con lo anterior, y por lo que respecta a los Registros de la Propiedad, es necesario tener en cuenta los diferentes niveles de efectividad que proporcionan los principales modelos registrales que históricamente se han venido aplicando. Dichos modelos varían, fundamentalmente, en cuanto al modo

y el momento en que se depuran las posibles contradicciones con los derechos de terceros y la legalidad. Desde este punto de vista los dos principales diseños organizativos propuestos han sido los registros de documentos y los registros de derechos[46].

Los registros de documentos acreditativos de las transacciones sobre bienes inmuebles (compraventas e hipotecas, principalmente), que es el sistema que aún se utiliza en Francia e Italia, se limitan a datar y conservar pruebas de las escrituras o contratos en las que eventualmente se basarán los tribunales para adjudicar los derechos en litigio.

Sin embargo, los registros de derechos, como el Registro de la Propiedad español, el Grundbuch alemán o el Land Register inglés, van más allá de la mera publicidad de los documentos potencialmente acreditativos de los contratos, pues acreditan el reconocimiento por el Estado de las titularidades sobre los derechos y los propios derechos. No olvidemos que, en estos sistemas, los contratos no son traslativos, sino que son contratos con finalidad traslativa. Para que esta se produzca efectivamente, es decir, con vinculación *erga omnes,* se requiere la inscripción. Para conseguirlo, los documentos son calificados por el registrador, con el fin de detectar posibles ilegalidades, así como cualquier conflicto que pueda perjudicar otros derechos reales. Como consecuencia de todo ello, la información del Registro está siempre depurada y es capaz de proporcionar titularidades definitivas e irrevocables, en el sentido de que el tercero de buena fe, que adquiera sobre la base de la información suministrada por el Registro, adquiere un derecho real, inatacable.

La superioridad de los registros de derechos, por tanto, es clara en cuanto a la calidad de sus productos: no solo asegura perfectamente la propiedad del titular, sino que reduce de forma drástica el coste de las transacciones futuras. El propietario tiene entonces mejores incentivos para invertir y, cuando transmite su derecho, esa transacción ya no requiere un costoso análisis jurídico de los antecedentes, sino que el Registro certifica con exactitud quién es el propietario. Además, estos beneficios no se refieren solo a las compraventas de inmuebles, sino también al abaratamiento del crédito mediante el uso de los inmuebles como garantía. Efectivamente, se puede concluir que[47]:

— En los países que cuentan con registros de derechos los precios (tipos de interés) de las hipotecas son apreciablemente inferiores, una vez ajustados dichos precios por las diferencias que existen entre países en cuanto a la mezcla de productos, el riesgo de tipo de interés, y el riesgo de insolvencia y prepago, de modo que tales precios ajustados representen precios comparables para el deudor.
— Este menor precio obedece a un menor coste operativo para las entidades financieras, en buena medida causado por el hecho de que la ejecución hipotecaria es notablemente más costosa y lenta en países con registros

de documentos. El registro de derechos facilita la ejecución porque proporciona una información ya depurada sobre cuáles son los derechos vigentes y su prioridad. Entre otros, facilita el cálculo de lo adeudado, establece de forma fidedigna la prioridad de las distintas hipotecas, y evita posibles litigios relacionados con la titularidad, los poderes y la capacidad de los contratantes. En otros términos: hace posible que las causas de oposición estén muy tasadas.

— Adicionalmente, cabe señalar que en los países con registros de derechos tanto el plazo medio de los préstamos hipotecarios como la relación entre la cuantía del préstamo y el valor del inmueble son notablemente superiores a las magnitudes que exhiben estas variables en los países con registros de documentos.

3. Cadenas de bloques y registros de derechos

En los sistemas con registros de derechos, los Registros de la Propiedad y Mercantiles tienen por objeto dar publicidad, eliminando así las asimetrías informativas, a los actos y contratos civiles y mercantiles que acceden a ellos, pero rechazando, y por tanto evitando que gocen de publicidad registral, los actos anulables, ineficaces, incompletos, irregulares o claudicantes. Esta labor se lleva a cabo a través del control de legalidad que los registradores llevan a cabo con independencia y bajo su responsabilidad personal y directa. Con ello se trata de evitar la posible litigiosidad futura sobre los derechos inscritos para lo cual los registradores han de verificar la adecuación a la legalidad del negocio jurídico celebrado, así como su compatibilidad con otros derechos preexistentes.

Este exhaustivo control de legalidad, por medio del cual el registrador ha de decidir si inscribe o rechaza una transacción jurídica, es indispensable, por tanto, para que el Registro pueda producir los efectos de protección de terceros in rem que son propios de los registros de derechos. Si el registrador practica la inscripción, esta pasa a ser reconocida por el Estado y el que en ella aparezca como titular del derecho que recoge, será considerado como titular *erga omnes* con la extensión y límites que resulten de la propia inscripción.

Frente al anterior modelo, que obsérvese que es un modelo exclusivamente institucional sin perjuicio que pueda ser apoyado por una infraestructura tecnológica que, en todo caso, tendrá un carácter meramente instrumental, es necesario analizar si se puede alcanzar un nivel igual o mayor de seguridad jurídica preventiva con un modelo, exclusivamente técnico-informático, basado en la tecnología de las cadenas de bloques.

A su vez, dentro de estos modelos basados en las cadenas de bloques y aplicados al ámbito de los registros deben distinguirse dos versiones:

— La que podría denominarse versión dura que consistiría, básicamente, en una cadena de bloques pública y autogestionada, con el mismo funcionamiento que Bitcoin pero en la que, en lugar de monedas, se almacenarían los contratos inteligentes enviados por los otorgantes, una vez suscritos, y mediante los que se llevaría a cabo la constitución y transmisión de derechos y cargas sobre bienes inmuebles. Esta cadena de bloques se encontraría replicada en los nodos una red Peer-to-Peer a la que se podría acceder libremente, en la que existirían los mismos tipos de nodos que en Bitcoin y en la que los mineros validarían las transacciones mediante búsquedas matemáticas semejantes a las antes descritas y se les retribuiría con algún tipo de moneda virtual.
— Y una versión blanda que consistiría en una cadena de bloques privada que se utilizaría, únicamente, como un mecanismo para proporcionar seguridad de carácter técnico a los asientos registrales, pero manteniendo el modelo institucional propio de los registros de derechos descrito al principio de este epígrafe.

Como veremos, los sistemas basados en la versión dura no solo no aumentan, sino que disminuyen drásticamente el nivel de seguridad jurídica preventiva que proporcionan los registros de derechos; mientras que los basados en la versión blanda no dejan de ser una alternativa técnica más, frente a otras también existentes, para el almacenamiento y securización de la información.

Efectivamente existen determinadas características del protocolo de funcionamiento de las cadenas de bloques, al menos en la versión dura, que son incompatibles con los objetivos que persiguen los sistemas registrales y con el principio de seguridad jurídica al que sirven.

En primer lugar, está la cuestión de la privacidad. Como hemos visto, en un sistema de cadenas de bloques a los usuarios únicamente se les identifica mediante su clave pública, sin que exista ni se almacene ningún otro dato que permita conocer la identidad real de cada uno de ellos.

Sin embargo, esto no es conforme con el funcionamiento de los registros que son, precisamente, un mecanismo de transparencia, de publicidad, que tienen por objeto, entre otros extremos, publicar las titularidades sobre los bienes y sobre los derechos y cargas constituidos sobre ellos, así como eliminar las cargas ocultas que les afecten y, todo ello, con el fin de dar confianza a los operadores económicos, para, de esta forma, facilitar el crédito territorial y, en definitiva, contribuir a la seguridad económica.

Por otro lado, con la identificación de los titulares de los derechos inscritos se facilita su transmisibilidad ya que esta no puede quedar supeditada a que su titular conserve o no su clave privada o a que, por ejemplo, en caso de su fallecimiento, sus herederos tengan o no acceso a la misma.

Además, los Registros también son un potente mecanismo para contribuir a la satisfacción de diversos intereses generales como, por ejemplo, la persecución del delito: corrupción, blanqueo de capitales, etc., lo que exige, igualmente, que sean conocidas las identidades reales de los titulares registrales.

Otra incompatibilidad es la protección de datos personales. Efectivamente, aunque los Registros son un sistema de publicidad y transparencia, ello no quiere decir que toda la información que pueda estar recogida en un asiento registral pueda ser libremente accesible por el público, ya que también es necesario respetar las normas relativas a la protección de datos personales y la intimidad de las personas. Por contra, como se ha explicado, toda la información almacenada en las cadenas de bloques es libremente accesible por cualquier persona, se refiera o no a transacciones por ella realizadas.

En el ámbito europeo esta es una materia especialmente sensible y, así, se ha tratado profusamente en una gran cantidad de normas comunitarias[48] y que en España se contempla tanto en su Constitución[49] (CE), como en leyes y reglamentos, principalmente la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal[50] (LOPD) y el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba su Reglamento de desarrollo[51].

Se trata esta de una materia directamente relacionada con derechos fundamentales constitucionalmente protegidos que, al encontrarse recogidos en la Sección 1.ª del Capítulo II del Título I de nuestra Constitución, están sometidos a reserva de ley orgánica (art. 81 CE), que en todo caso deberá respetar su contenido esencial, que vinculan a todos los poderes públicos (art. 53.1 CE) y, respecto de sus garantías jurisdiccionales, podrá recabarse la tutela de los tribunales ordinarios mediante un procedimiento basado en los principios de preferencia y sumariedad y, subsidiariamente, la tutela del Tribunal Constitucional mediante el recurso de amparo (art. 53.2 CE).

El propio Tribunal Constitucional configura este derecho como un derecho independiente pero íntimamente relacionado con el derecho a la intimidad reconocido en el artículo 10 de la Constitución Española (SSTC 254/1993, de 20 de julio y 290/2000, de 30 de noviembre) y directamente vinculante para los poderes públicos sin necesidad de desarrollo normativo (STC 254/1993) e, igualmente, como un derecho estrechamente vinculado con la libertad ideológica, consagrada en el artículo 16 de la Constitución, pues evidentemente el almacenamiento y la utilización de datos informáticos puede suponer un riesgo para aquella, no solamente por lo que se refiere a «datos sensibles», entre los que se encuentran los de carácter ideológico o religioso sobre los cuales según indica el artículo 16 de la Constitución nadie estará obligado a declarar, sino también por su posible utilización ajena a las finalidades para los que fueron recabados (entre otras, SSTC 11/98, de 13 de enero; 44 y 45/1999, de 22 de marzo), por la inclusión de datos sin conocimiento del afectado (STC 202/1999, de 8 de noviembre) o por efectuarse accesos indebidos (STC 144/1999, de 22 de julio).

En España, además, la protección de los datos personales que puedan constar en los Registros de la Propiedad, Mercantiles o de Bienes Muebles es una tarea que se impone expresamente a los registradores en el artículo 222.6 de la Ley Hipotecaria (LH): «*Los Registradores, al calificar el contenido de los asientos registrales, informarán y velarán por el cumplimiento de las normas aplicables sobre la protección de datos de carácter personal*» y, también, la propia Dirección General de los Registros y del Notariado en numerosas instrucciones (29 de octubre de 1996, 17 de febrero de 1998, y 27 de enero de 1999) y resoluciones (11 de septiembre de 2009, 29 de julio y 3 de diciembre de 2010, 16 de septiembre de 2011, 14 de septiembre, y 12 de diciembre de 2012) ha señalado que el registrador debe calificar que datos debe incluir o excluir en la publicidad registral, teniendo en cuenta la legislación y jurisprudencia sobre protección de datos.

Todo ello hace que el acceso al contenido de los asientos registrales no puede ser directo y libre, sino que el consultante ha de acreditar un interés legítimo (art. 221.1 LH: «*Los Registros serán públicos para quienes tengan interés conocido en averiguar el estado de los bienes inmuebles o derechos reales inscritos*») y, al emitir publicidad registral, es necesario un previo tratamiento profesional por el registrador (art. 222.2 LH: «*La manifestación, que debe realizar el Registrador, del contenido de los asientos registrales tendrá lugar por nota simple informativa o por certificación, mediante el tratamiento profesional de los mismos…*») y la información que finalmente se proporcione no puede extenderse más allá de lo que sea necesario para satisfacer aquel legítimo interés[52].

Otro punto de fricción entre el funcionamiento de las cadenas de bloques y el de un registro de derechos, es la determinación de la prioridad entre los derechos que acceden a cada uno de dichos sistemas.

En las cadenas de bloques la ordenación de las transacciones no depende del instante en que estas se realizan y envían, sino de un hecho que es totalmente aleatorio y ajeno a las partes intervinientes en ellas, y es la resolución de las búsquedas matemáticas que realizan los mineros para el minado de bloques y la validación de transacciones e, incluso, puede ocurrir que una transacción inicialmente confirmada e integrada en un bloque minado sea «desconfirmada» si se encontraba en un bloque situado en una rama más corta que las otras que pudieran existir en un momento dado en la cadena.

En un registro de derechos, como por ejemplo en España, el momento de la presentación de los documentos en el registro (ya se haga presencial o telemáticamente) determina la prioridad de los derechos a que se refieren, aplicando el correspondiente sellado temporal. De esta forma el titular de uno de dichos derechos, teniendo en cuenta la situación tabular de la finca en el momento de la presentación, puede saber con exactitud el rango hipotecario, con el que se va a inscribir el suyo, frente a otros que se puedan presentar.

Si se aplicase a los registros el protocolo seguido en las cadenas de bloques, ante una presentación sucesiva con relación a una misma finca, los presentantes no podrían conocer con que rango o prioridad se van a inscribir sus derechos, pudiendo ocurrir que el derecho constituido y presentado en último lugar se inscriba con preferencia al presentado en primer lugar, dado que por una mera cuestión aleatoria —el minado de bloques— o monetaria —el último presentante pagó una comisión superior a los demás— se minó antes el bloque en el que se incluyó la última transacción y todavía podría ser peor, si un derecho inicialmente inscrito, posteriormente se «desinscribe» por encontrarse en una rama corta.

Es evidente que esto crea, no seguridad, sino inseguridad jurídica y dificulta el tráfico ya que los operadores económicos, en el momento de suscribir los contratos inscribibles, no podrán tener la completa seguridad de que en dicho instante la situación de los derechos inscritos que figuran en el registro es la definitiva, ni de la prioridad que su derecho, una vez presentado en el registro, tendrá frente a otros que se presenten coetáneamente con él, de tal forma que será posible, por ejemplo, que la ejecución de un derecho constituido y presentado posteriormente a otro, pero inscrito con un rango anterior a este por la aleatoriedad del funcionamiento de la cadena de bloques, provoque la cancelación de este último.

Con todo, el principal problema para que los sistemas que implementen la versión dura de las cadenas de bloques puedan producir los mismos efectos que se derivan de un registro de derechos es la ausencia, en aquellos, de todo control de legalidad y calificación.

La importancia que la contratación inmobiliaria tiene para los mercados, el crédito y la economía de un país hace que dichos contratos se rodeen de especiales cautelas y solemnidades, sobre todo en aquellos países en los que existen registros de derechos, que, como se ha explicado, tratan de eliminar toda litigiosidad futura respecto de los derechos inscritos como medio para dar seguridad y confianza al tráfico.

Estas fueron las razones[53] por las que, en España, la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico[54], que incorpora a nuestro ordenamiento la Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio, relativa a determinados aspectos de los servicios de la sociedad de la información y, en particular, el comercio electrónico en el mercado interior, señala en el apartado a del número primero de su artículo 5, que: «*1. Se regirán por su normativa específica las siguientes actividades y servicios de la sociedad de la información: a) Los servicios prestados por notarios y registradores de la propiedad y mercantiles en el ejercicio de sus respectivas funciones públicas*» mientras que el párrafo segundo de su artículo 23.4 también establece que: «*Los contratos, negocios o actos jurídicos en los que la Ley determine para su validez o para la producción de determinados*

efectos la forma documental pública, o que requieran por Ley la intervención de órganos jurisdiccionales, notarios, registradores de la propiedad y mercantiles o autoridades públicas, se regirán por su legislación específica».

Efectivamente, no basta con que las partes suscriban un contrato. Al contrario, es necesario verificar que no concurren ninguno de los supuestos que puedan determinar su nulidad o ineficacia y, así, entre otros extremos, habrá de determinarse, no solo que se ha prestado el consentimiento, que quienes lo han prestado son quienes dicen ser, que lo han hecho libremente, que no se encuentran incapacitados ni tienen sus facultades de disposición limitadas, que en el momento de dicha prestación los otorgantes estaban en pleno uso de sus facultades y, en caso de que se actúe por medio de un representante, que este cuente realmente con dicho poder de representación y que las facultades que se le han delegado son suficientes para llevar a cabo el negocio jurídico a que se refiere el contrato suscrito, etc., sino también que las diferentes circunstancias que conforman dicho negocio se ajustan a la legalidad y no afectan a los derechos preexistentes de terceros. Ninguna de estas cuestiones se resuelve mediante las cadenas de bloques

Se podría decir que lo expuesto en el anterior párrafo se podría solventar, al menos parcialmente, mediante la estandarización de los contratos inscribibles. De esta forma solo serían admisibles, o inscribibles, los derechos contenidos en modelos de contratos preestablecidos, una vez suscritos por las partes.

Ello, no obstante, choca con la libertad de empresa y de contratación, propia de una economía de mercado moderna, y que, por ejemplo, en el ordenamiento jurídico español no solamente se reconoce en la Constitución (art. 38: «*Se reconoce la libertad de empresa en el marco de la economía de mercado. Los poderes públicos garantizan y protegen su ejercicio…*») y en el propio Código Civil (art. 1.255: «*Los contratantes pueden establecer los pactos, cláusulas y condiciones que tengan por conveniente, siempre que no sean contrarios a las leyes, a la moral, ni al orden público*») sino también en la legislación hipotecaria que se establece un sistema de libre constitución de derechos reales y, así, el artículo 2.2 de la Ley Hipotecaria establece que: «*En los registros expresados en el artículo anterior se inscribirán: … 2.º. Los títulos en que se constituyan, reconozcan, transmitan, modifiquen o extingan derechos de usufructo, uso, habitación, enfiteusis, hipoteca, censos, servidumbre y otros cualesquiera reales*» y en el artículo 7 de su reglamento que: «*Conforme al artículo 2.º de la Ley no solo deberán inscribirse los títulos en que se declare, reconozca, transmita, modifique o extinga el dominio o los derechos reales que en dichos párrafos se mencionan, sino cualesquiera otros relativos a derechos de la misma naturaleza, así como cualquier otro pacto o contrato de trascendencia real que, sin tener nombre propio en derecho, modifique, desde luego o en lo futuro, algunas de las facultades del dominio sobre bienes inmuebles o inherentes a derechos reales*».

No parecería lógico, por tanto, optar por una concreta solución técnica que suponga o que obligue a reducir las libertades de las que disfrutan los ciudadanos y que el ordenamiento jurídico les reconoce, sobre todo cuando existen otras opciones que permiten preservarlas. Parecería con ello, que la tecnología constituiría el elemento esencial, y no accesorio o instrumental, lo que conduciría, finalmente, a que solamente se pudiesen establecer aquellas relaciones contractuales que fuesen posibles técnicamente y en el modo y forma que la tecnología determinase, lo cual es inaceptable.

Por otra parte, debe tenerse en cuenta que a los registros acceden, no solamente contratos, sino también resoluciones judiciales o administrativas que pueden suponer la modalización de los derechos inscritos, su cancelación, la inscripción de nuevos bienes o derechos, el establecimiento de limitaciones a su transmisibilidad, etc., sin que sea factible, por ejemplo, limitar la independencia de los órganos judiciales en cuanto al contenido de sus decisiones, preestableciendo dichos contenidos.

En otro orden de cosas, debe tenerse en cuenta que el registrador no solamente lleva a cabo un juicio independiente de control de adecuación a la legalidad y de respeto a los derechos de terceros —actuando como una especie de defensor de los ausentes— sino que también actúa en defensa de los otorgantes mediante la aplicación de la legislación de protección de consumidores y usuarios.

Piénsese que, en la versión dura de contratación inmobiliaria con cadena de bloques, en que los contratos, una vez celebrados, se remiten a la cadena para su «inscripción», casi todos los contratos acabarían siendo contratos de adhesión en los que las partes no predisponentes, en ausencia del control de legalidad que realiza el registrador, podrían verse perjudicadas.

Para evitar esto, en el ordenamiento español, el artículo 258.2 LH señala que: «*El Registrador denegará la inscripción de aquellas cláusulas declaradas nulas de conformidad con lo dispuesto en el párrafo segundo del artículo 10 bis de la Ley 26/1984, de 19 de julio, General para la Defensa de los Consumidores y Usuarios*». También el Real Decreto Legislativo 1/2007[55], de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios, señala en su artículo 84 los Registradores no inscribirán aquellos contratos o negocios jurídicos en los que se pretenda la inclusión de cláusulas declaradas nulas por abusivas en sentencia inscrita en el Registro de Condiciones Generales de la Contratación.

Los usuarios de las cadenas de bloques, además, podrían verse todavía más perjudicados por la ausencia de asesoramiento legal, personal y directo que el sistema no les prestaría, por lo que tendrían que recurrir al consejo legal externo, satisfaciendo el coste correspondiente. Por el contrario, los registradores hemos de prestar este asesoramiento y, además, de forma gratuita. Así, una vez más en España, el artículo 222.7 de la Ley Hipotecaria establece que: «*Los Registradores en el ejercicio profesional de su función pública deberán informar a cualquier persona que lo solicite en materias relacionadas con el Registro.*

La información versará sobre los medios registrales más adecuados para el logro de los fines lícitos que se propongan quienes la soliciten» y, también, su artículo 258.1 señala que: «*El Registrador, sin perjuicio de los servicios prestados a los consumidores por los centros de información creados por su colegio profesional, garantizará a cualquier persona interesada la información que le sea requerida, durante el horario habilitado al efecto, en orden a la inscripción de derechos sobre bienes inmuebles, los requisitos registrales, los recursos contra la calificación y la minuta de inscripción*».

Podría defenderse que algunos de los anteriores inconvenientes desaparecen optando por la versión blanda de la cadena de bloques, es decir, estableciendo un sistema de cadena de bloques privada con calificación registral anterior a la introducción de la información en la cadena. Efectivamente ello es así, pero también supone que se perderían algunas de sus principales características configuradoras como la eliminación de la privacidad, las búsquedas matemáticas para la ordenación de las transacciones, etc. asemejándose así, cada vez más, a otras opciones técnicas que prestan las mismas garantías como, por ejemplo, las utilizadas en el modelo español, que se describen en el epígrafe siguiente, y en el que se utilizan técnicas de firma electrónica de documentos y asientos, con sellado temporal electrónico y replicación de datos en cluster.

4. Actualidad de los Registros en España

Como se decía anteriormente, la consecución eficaz y eficiente de los objetivos que persiguen los registros jurídicos, como los de la propiedad y mercantiles, no pueden alcanzarse con soluciones exclusivamente tecnológicas, sino que, al contrario, solo una adecuada organización jurídica e institucional, apoyada por los medios técnicos más ajustados a cada situación, permiten obtenerlos.

En España, desde el punto de vista jurídico, como se ha expuesto, el Registro de la Propiedad se configura como un registro de derechos con las características ya vistas y, desde el punto de vista organizativo, al frente de cada oficina registral se encuentra un registrador, al que se le retribuye mediante el saldo neto obtenido después de afrontar todos los gastos de la oficina (inversión, personal, etc.) con los aranceles satisfechos por los usuarios del sistema, y que asume tanto el riesgo jurídico como económico de la actividad de su Registro.

Se siguen así, las recomendaciones de diversos organismos internacionales, como Naciones Unidas, que recomiendan que los sistemas registrales se autofinancien y que, por tanto, el coste del servicio sea pagado por los usuarios[56]. De igual modo, la Dirección General del Mercado Interior de la Comisión Europea recomienda que los funcionarios encargados de los registros sean directamente responsables por sus errores[57], lo que no parece viable sin alguna modalidad de arancel.

Esta arquitectura organizativa se adapta, igualmente, a las exigencias de la moderna gestión pública, también, con las recomendaciones de buena praxis de organizaciones como la OCDE[58] y garantiza la concurrencia de tres características esenciales en todo modelo registral eficaz:

— Elevada productividad y costes reducidos, ya que tanto el registrador como los empleados, que también tienen cierta participación en los beneficios, son los primeros interesados en que los asuntos se despachen rápidamente y los costes sean lo más ajustados posible.
— Sirve para atraer profesionales altamente cualificados, al proporcionar confianza para que invertir en la propia formación, tanto antes de entrar en la profesión como durante su ejercicio.
— Y garantiza la calidad jurídica de los productos registrales al responsabilizar personalmente al registrador por sus decisiones.

Y, desde el punto de vista tecnológico, los registradores españoles hemos venido realizando continuos desarrollos tecnológicos dirigidos a la mejora y modernización del Registro y para su adaptación a los cambios sociales, económicos y tecnológicos, pero todo ello sin menoscabo de los principios y fines esenciales de la seguridad jurídica, el desarrollo económico y la igualdad social a los que debe responder.

Estos desarrollos comenzaron, a iniciativa de los propios registradores, en la década de los años 1990, con las primeras aplicaciones de gestión registral, para, más tarde, imponerse por medio de disposiciones legales. Así, en el año 2001[59] se establecieron diversas obligaciones de carácter tecnológico a cargo de los registradores, entre las que destacaban la de trasladar el contenido de los asientos de los libros de todos los Registros de la Propiedad y Mercantiles de España a soporte informático, la de dotarse de una red segura y privada de comunicaciones que interconectase todos los registros del estado entre sí y estos con los sistemas corporativos del Colegio de Registradores y, también, imponía a cada registrador la utilización de certificados reconocidos —hoy cualificados— de firma electrónica para la firma de documentos electrónicos (con técnicas de criptografía asimétrica semejantes a las vistas para el caso de Bitcoin) con sellado temporal mediante la señal horaria oficial y también obligaba al Colegio de Registradores a constituirse en prestador de servicios de certificación.

Estos y otros desarrollos normativos y tecnológicos posteriores, permiten que, en España, hoy en día y desde hace más de 15 años, la totalidad del procedimiento registral se pueda tramitar de forma electrónica, tanto por lo que se refiere a sus aspectos internos —es decir, los relacionados con el despacho de documentos en la oficina registral—, como a los externos —los concernientes a los usuarios de los servicios registrales—.

Así por ejemplo, y en cuanto a los aspectos internos, es posible recibir telemáticamente, en cualquier Registro de la Propiedad, Mercantil o de Bienes Muebles, todo tipo de documentos electrónicos notariales, judiciales, administrativos o privados firmados electrónicamente; también se pueden remitir por la misma vía la notificación de la práctica de los correspondientes asientos de presentación, notas de calificación, notas de despacho, notas simples, certificaciones, minutas, etc., todo ello con la firma electrónica del registrador y, finalmente, elaborar y firmar electrónicamente los asientos registrales a que den lugar los documentos presentados, así como las representaciones georreferenciadas de las fincas.

Por lo que respecta a los aspectos externos del procedimiento registral, y complementariamente a lo señalado en el párrafo anterior, los usuarios del Registro pueden presentar telemáticamente cualquier clase de documento, consultar su estado de tramitación y recibir la resolución del expediente (nota de calificación o de despacho), así como solicitar y recibir telemáticamente, desde cualquier punto del planeta, alertas, notas simples o certificaciones electrónicas.

La eficacia y eficiencia, resultantes de la combinación de los anteriores factores jurídicos, organizativos y tecnológicos, quedan de relieve al comparar la productividad de nuestros Registros de la Propiedad y Mercantiles, tanto con registros extranjeros como con aquellos otros registros españoles que están organizados sobre bases diferentes.

Por un lado, nuestro nivel de seguridad jurídica es de los más altos del mundo, a juicio de los principales operadores internacionales. Efectivamente, en opinión del Banco Mundial, nuestros registros logran esta máxima seguridad a unos costes reducidos y en unos tiempos de procesamiento muy cortos[60]. En el mismo sentido, el índice «Registering Property» del IPRI 2016 (International Property Rights Index), que mide la facilidad para registrar una propiedad en términos de número de días y procedimientos necesarios, ha puntuado a los registros españoles con 9,6 puntos[61], de los 10 posibles.

Ello hace posible, por ejemplo, que en España los tiempos para formalizar y eventualmente ejecutar los préstamos hipotecarios sean muy cortos, lo que redunda en menores costes para el prestatario. Coinciden en esta apreciación de forma rotunda los principales usuarios del sistema registral español, como resulta del informe final del grupo de trabajo creado por la Comisión Europea en 2003 para el análisis del mercado hipotecario europeo[62] y que valora muy positivamente el funcionamiento de nuestros registros[63].

Coincide también el informe sobre el Conveyancing Services Market, elaborado para la Comisión Europea por el Centre of European Law and Politics de la Universidad de Bremen[64] y, más recientemente, la Federación Hipotecaria Europea, que situaba a España como uno de los dos países europeos cuyas operaciones inmobiliarias disfrutaban costes de transacción de naturaleza jurídica más bajos[65].

CONCLUSIONES

I. La aplicación directa y sin modificaciones de la tecnología de las cadenas de bloques, conforme al esquema en que esta opera en el ámbito de Bitcoin, a un sistema registral de derechos, como el español, supondría no solo la lesión de derechos fundamentales de los ciudadanos, así como de su libertad de empresa y contratación o la independencia de los órganos judiciales sino que también iría en contra de importantes principios hipotecarios, consagrados en nuestro ordenamiento jurídico, como el de prioridad, la libre constitución de derechos reales, el asesoramiento gratuito por el registrador, etc. y también se vería perjudicada la propia seguridad jurídica preventiva, y por tanto la seguridad económica y el desarrollo económico y social del país, al no existir ningún tipo de control de legalidad o calificación registral.

II. No es admisible sacrificar todo lo anterior simplemente porque se quiera implantar una determinada solución tecnológica como las cadenas de bloques, sobre todo cuando existen otras opciones que permiten preservar los derechos y libertades de los ciudadanos. En este sentido debe recordarse el carácter accesorio, instrumental, no esencial, de la tecnología y, por ello, es esta la que debe adaptarse a las normas y procedimientos del ordenamiento jurídico y no a la inversa.

III. Sería, por tanto, necesario introducir importantes modificaciones en el protocolo de las cadenas de bloques para evitar los perjuicios indicados que, no obstante, lo desnaturalizarían, reduciéndolo a un mero sistema de archivo digital que se asemejaría a otras opciones técnicas existentes en el mercado, ya probadas y que pueden ofrecer las mismas garantías.

BIBLIOGRAFÍA

ANTONOPOULOS A., *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*, California (EEUU), O'Reilly. 2014.

ARRUÑADA, B., Property Enforcement as Organized Consent, *Journal of Law, Economics, and Organization,* volumen 19, número 2, 2003.

— Institutional Support of the Firm: A Theory of Business Registries, *The Journal of Legal Analysis,* volumen 2, número 2, 2010.

BECKER, G., *Merkle Signature Schemes, Merkle Trees and Their Cryptanalysis*, Ruhr-Universität Bochum, 2008.

BONNEAU, J., CLARK, J., FELTEN, E. W., GOLDFEDER, S., MILLER, A. Y NARAYANAN, A., *Bitcoin and Cryptocurrency Technologies*, New Jersey (EEUU), Princeton University Press, 2016.

CASEY, M.J. y VIGNA, P., *The Age of Cryptocurrency*, Nueva York (EEUU), St. Martin's Press. 2015.

DÍAZ FRAILE, J.M., Comentarios a la Directiva y al Proyecto de Ley español de comercio electrónico de 2000. Contenido y proceso de elaboración, *Revista Crítica de Derecho Inmobiliario*. Año LXXVII; número 663; enero-febrero de 2001.

GARCÍA GARCÍA, J.M., *Derecho inmobiliario registral e hipotecario*, Madrid: Civitas, 1988.
MÉNDEZ GONZÁLEZ, F.P., *Fundamentación Económica del Derecho de Propiedad*, Madrid, Civitas, 2011.
ROSENFELD, M., *Analysis of hashrate-based double-spending*, disponible en: https://arxiv.org/pdf/1402.2009v1, 2014.
MERKLE, R., *Secrecy, authentication and public key systems. A certified digital signature*, Stanford University, 1979.
NAKAMOTO, S., *Bitcoin: A Peer-to-Peer Electronic Cash System*, disponible en: http://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html, 2008.
POPPER, N., *Digital Gold*. Nueva York (EEUU), Harper Collins, 2015.
RON, D. Y SHAMIR, A., *Quantitative Analysis of the Full Bitcoin Transaction Graph*, disponible en: http://eprint.iacr.org/2012/584.pdf, 2012.
SWAN, M., *Blockchain: Blueprint for a New Economy*. California (EEUU), O'Reilly. 2015.
TAPSCOTT, A. y TAPSCOTT, D., *Blockchain Revolution*, Nueva York (EEUU), Portfolio Penguin, 2016.

NOTAS:

[1] Mucho se ha especulado sobre la verdadera identidad o identidades que se esconden bajo el seudónimo de SATOSHI NAKAMOTO. En mayo de este año se produjo uno de los anuncios más prometedores sobre este asunto cuando el informático australiano CRAIG WRIGHT, tras diversas filtraciones previas por parte de terceros, aseguró ser dicha persona presentando una serie de pruebas de su autoría, que sin embargo fueron cuestionadas por algunos expertos. Craig WRIGHT prometió, entonces, difundir la prueba definitiva, que consistiría en transferir bitcoins de uno de los bloques de transacción iniciales, algo que supuestamente solo podría hacer el verdadero fundador mediante su clave privada. Finalmente, sin embargo, acabaría retractándose, alegando el acoso mediático y policial al que, a su juicio, se le estaba sometiendo, lo que mantiene vigente el interrogante sobre la autoría del sistema Bitcoin.

[2] Véase: Satoshi NAKAMOTO, *Bitcoin: A Peer-to-Peer Electronic Cash System*, (octubre de 2008). http://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html

[3] Véase: https://bitcoin.org/bitcoin.pdf

[4] En el resto de este documento, cuando el término bitcoin aparezca como: Bitcoin, con la inicial en mayúscula, se estará haciendo referencia a la red o sistema Bitcoin y, a la moneda en caso contrario, al igual que cuando se utilicen las siglas BTC.

[5] 25 de febrero de 2017.

[6] Véase: https://blockchain.info/es/charts

[7] Véase: https://www.bitstamp.net

[8] Véase: https://www.coinbase.com

[9] Véase: https://www.kraken.com

[10] Véase: https://www.bitfinex.com

[11] Véase: https://btc-e.com

[12] Véase: https://localbitcoins.com

[13] Véase: https://www.okcoin.com

[14] Véase: https://litecoin.org

[15] Véase: https://ripple.com

[16] Véase: http://primecoin.io

[17] Véase: http://dogecoin.com

[18] Véase: https://z.cash

[19] En la siguiente página se puede encontrar una relación de las distintas posibilidades: https://es.bitcoin.it/wiki/Software.

[20] Véase: https://bitcoin.org/es/descargar

[21] Véase: https://multibit.org

[22] Véase: https://electrum.org

[23] El número de direcciones posibles es de: $1{,}46 \cdot 10^{48}$.

[24] Véase: Dorit RON and Adi SHAMIR, *Quantitative Analysis of the Full Bitcoin Transaction Graph,* (octubre de 2012). http://eprint.iacr.org/2012/584.pdf

[25] Véase: https://z.cash/

[26] Véase: http://ec.europa.eu/justice/criminal/document/files/aml-directive_en.pdf

[27] Véase: https://www.boe.es/buscar/pdf/1946/BOE-A-1946-2453-consolidado.pdf

[28] Todos los bloques, por tanto, hacen referencia al bloque anterior salvo, obviamente, el primer bloque de la cadena. Como curiosidad, dicho primer bloque fue minado el 4 de enero de 2009 y su hash o identificador es: 000000000019d6689c085ae165831e934ff763ae46a-2a6c172b3f1b60a8ce26f.

[29] Este hash en particular se calcula por medio de la técnica de los árboles de Merkle:

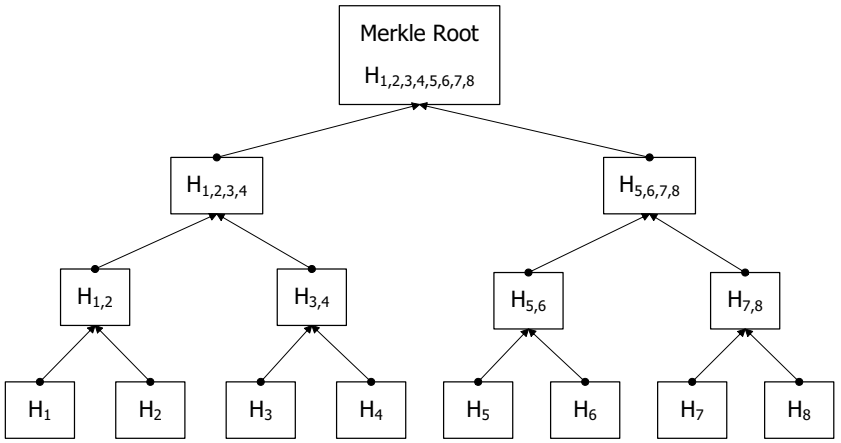
— RALPH MERKLE. *Secrecy, authentication and public key systems. A certified digital signature*. Stanford University, 1979.

— GEORG BECKER. *Merkle Signature Schemes, Merkle Trees and Their Cryptanalysis*. Ruhr-Universität Bochum, 2008.

[30] En realidad, el hash de cada bloque es el hash de la cabecera de dicho bloque que es un campo en el que, entre otros datos, se almacenan el hash del bloque previo, el *nonce* y el llamado *merkle root*. Este *merkle root* no es más que un nuevo código hash que se calcula a partir de los hashes de las transacciones incluidas en el propio bloque mediante el algoritmo de Merkle.

Considerando, por ejemplo, un conjunto de 8 transacciones, en la siguiente figura se muestra el árbol de Merkle para el cálculo del *mekle root* de dicho conjunto. Como se puede ver en ella, las transacciones se agrupan por pares y se calcula un nuevo hash (el algoritmo criptográfico que Bitcoin utiliza para esta operación es el double-SHA-256) a partir de los hashes de cada par, dando lugar a los hashes: H1,2, H3,4, H5,6 y H7,8, a su vez estos nuevos hashes también se agrupan por pares y se calculan otros nuevos a partir de ellos, obteniendo los identificados como: H1,2,3,4 y H5,6,7,8 y, finalmente, el proceso se vuelve a repetir para obtener el *merkle root* del conjunto.

Árbol de Merkle



Este algoritmo permite obtener una huella digital que resume todas las transacciones comprendidas en un bloque y que, a su vez, facilita la comprobación de si una concreta

transacción se encuentra incluida en un bloque, ya que el número máximo de operaciones de hash necesarias para llevar a cabo dicha comprobación con esta estructura, dado un conjunto de N transacciones a 2*log2(N).

[31] Véase: Meni ROSENFELD, *Analysis of hashrate-based double-spending*, (última versión: febrero de 2014). https://arxiv.org/pdf/1402.2009v1.

[32] En realidad, esto es más frecuente de lo que en principio pudiera creerse. Así, por ejemplo, durante los primeros meses de 2014 la empresa de minado Ghash.IO (https://ghash.io) estuvo muy cerca de llegar al 50%; en la actualidad, diversos grupos de mineros (AntPool, F2Pool y BitFury, etc.) superan, cada uno de ellos y de forma sostenida, el 10% de la capacidad de cálculo total y también ha habido grupos, como BTC Guild (hoy ya extinguido), que han sido capaces de resolver ramas de hasta 6 bloques consecutivos.

[33] En la dirección: https://blockchain.info/es/charts/avg-block-size?daysAverageString=7&timespan=all se puede ver el tamaño medio de bloque a lo largo del tiempo.

[34] En: https://blockchain.info/es/charts/n-transactions-per-block?timespan=all se puede obtener el número medio de transacciones por bloque.

[35] Véase: *Visa, Inc. at a Glance*. Visa Inc. Junio de 2015.

[36] Algunas de las principales propuestas en esta materia han sido las siguientes:

— BIP 100: Publicada por uno de los desarrolladores principales de Bitcoin: Jeff Garzik en junio de 2015. Consiste en que el tamaño de los bloques no sea fijo, sino que, cada 12000 bloques (unos tres meses), el tamaño del bloque se decidirá por votación entre los mineros, con un límite máximo de 32 MB. Una variante de esta propuesta es la conocida como Bitcoin Unlimited.

— BIP 101: Publicada por Gavin ANDRESEN, también en junio de 2015, y propone la ampliación del tamaño de bloque a 8 MB, ampliándose sucesivamente cada dos años, hasta alcanzar los 8192 MB, y conforme aumenta la capacidad de los procesadores —de acuerdo con la Ley de Moore—, la capacidad de almacenamiento y el ancho de banda de las redes de comunicaciones. Más tarde, Gavin ANDRESEN junto con Mike HEARN, crearían una variante de esta propuesta, llamada Bitcoin XT.

— BIP 102: de Jeff Garzik, se trataba de una propuesta de emergencia, como modo de ganar tiempo en caso de que no se llegase a un consenso. No obstante, y dado que solo era una propuesta de emergencia, no contenía una estrategia a medio y largo plazo sobre el tamaño de bloque. Consistía en ampliar a 2 MB el tamaño de bloque a partir del 11 de noviembre de 2015.

— BIP 103: Propuesta por Pieter WULLIE (Blockstream) en agosto de 2015 y consiste en incrementar el tamaño máximo de bloque un 17,7% cada año, desde enero de 2017, hasta alcanzar los 2 GB en 2063.

— BIP 109: Otra propuesta de Gavin ANDRESEN que consiste, también, en aumentar el tamaño de bloque a 2 MB y que, junto con otras medidas adicionales, posteriormente cristalizaría en la propuesta conocida como Bitcoin Classic.

— BIP 141: También conocida por Segregated Witnes o SegWit y propuesta Pieter WUILLE. Básicamente consiste en trasladar los datos de firma de las transacciones a una estructura de datos paralela, con lo que el tamaño ocupado por cada transacción en los bloques se reduce y podrían incluirse más en cada uno de ellos.

— Propuesta de los bloques extendidos de Adam BACK (Blockstream) en la que se mantendrían los bloques de 1 MB, pero los mineros que quisieran utilizar tamaños mayores (10 MB) podrían hacerlo. Esta propuesta supondría la creación de dos cadenas de bloques diferentes sobre el mismo protocolo Bitcoin.

— Propuesta de Sergio LERNER, que consiste en mantener el límite máximo de 1 MB, pero acelerar el minado de bloques de tal forma que se pasaría de los 10 minutos por bloque actuales a los 5 minutos por bloque.

[37] Véase: https://www.reddit.com/r/btc/comments/42nx74/unmasking_the_blockstream_business_plan; http://xtnodes.com/announcement.php; https://bitco.in/forum/threads/gold-collapsing-bitcoin-up.16/page-59#post-2245; etc.

[38] Véase: https://blockstream.com/technology/#sidechains

[39] Véase: https://blog.plan99.net/the-resolution-of-the-bitcoin-experiment-dabb30201f7#.ewfepr21j

[40] Por tanto, bitcoin es una moneda con un suministro progresivo, controlado y limitado (hasta que se alcance la cantidad de 21 millones de monedas). Durante los primeros años de vida de Bitcoin, de 2009 a 2012, la recompensa por el minado de cada bloque era de 50 bitcoins. El 28 de noviembre 2012 se minó el bloque número 210.000 y la recompensa pasó a ser de 25 bitcoins; posteriormente, el pasado 9 de julio, se minó el bloque número 420.000 y, nuevamente, la recompensa por bloque minado se redujo a la mitad, es decir, a una cuantía de 12,5 bitcoins y, aproximadamente, dentro de otros 4 años, en 2020, se reducirá a 6,25 bitcoins. Con esta sucesión se estima que en el año 2140 se generará el último bitcoin.

En la dirección: http://www.bitcoinblockhalf.com se puede consultar la cuenta atrás hasta la próxima reducción en la recompensa de los mineros.

[41] Véase: https://www.bitcoinmining.com/bitcoin-mining-hardware.

[42] Por ejemplo: Eobot: https://www.eobot.com; Genesis Mining: https://www.genesis-mining.com; Ghash.IO: https://ghash.io; HashFlare: https://hashflare.io; HashNest: https://www.hashnest.com; MineOnCloud: https://mineoncloud.com; MinerGate: https://en.minergate.com; Minex: https://minex.io; NiceHash: https://www.nicehash.com; etc.

[43] En la dirección: https://blockchain.info/es/pools?timespan=4days se pueden consultar estos datos para las últimas 24 o 48 horas o para los últimos 4 días.

[44] Véase: Vitalik BUTERIN. *On the comparative advantages of public and private blockchains*. Agosto de 2015. https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains.

[45] Véase: Fernando P. MÉNDEZ GONZÁLEZ. *Informe sobre el rationale y el grado de eficiencia de la organización del sistema registral inmobiliario y mercantil español*. Febrero de 2014.

[46] Para un análisis con mayor profundidad sobre esta materia, véanse: Benito ARRUÑADA. *Property Enforcement as Organized Consent*. Journal of Law, Economics, and Organization, volumen 19, número 2, 2003, 401-444; y, respecto de los registros mercantiles: Benito ARRUÑADA. *Institutional Support of the Firm: A Theory of Business Registries*. The Journal of Legal Analysis, volumen 2, número 2, 2010, 525-576.

[47] Véase: *United Nations Economic Commission for Europe, Study on Key Aspects of Land Registration and Cadastral Legislation*, HMLR, Londres, 2000.

[48] Véanse, por ejemplo: la Carta de los Derechos Fundamentales de la Unión Europea, de 7 de diciembre de 2000; el Tratado de Lisboa, 13 de diciembre de 2007; el Reglamento CE n.º 45/2001 del Parlamento y del Consejo, de 18 de diciembre de 2000; el Reglamento CE n.º 2725/2000 del Consejo, de 11 de diciembre de 2000; el Reglamento UE n.º 611/2013 de la Comisión, de 24 de junio de 2013; el Reglamento UE 2016/679 del Parlamento y del Consejo, de 27 de abril de 2016; la Directiva 2002/58/CE del Parlamento y del consejo, de 12 de julio de 2002; la Directiva 2006/24/CE del Parlamento y del Consejo, de 15 de marzo de 2006; la Directiva UE 2016/680 del Parlamento y del consejo, de 27 de abril de 2016; etc.

[49] Véase: https://www.boe.es/buscar/act.php?id=BOE-A-1978-31229.

[50] Véase: https://www.boe.es/buscar/act.php?id=BOE-A-1999-23750.

[51] Véase: https://www.boe.es/buscar/act.php?id=BOE-A-2008-979.

[52] Algunos de los principios que se extraen de las normas y jurisprudencia en España sobre protección de datos y en relación con los Registros, son los siguientes:

— El registrador está obligado al tratamiento profesional de la publicidad formal, para poder excluir la manifestación de los datos carentes de trascendencia jurídica (art. 4 LOPD 15/1999).

— Tan solo se pueden recoger aquellos datos que sean adecuados, pertinentes y no excesivos conforme a las finalidades para las que se hayan obtenido (art. 4 LOPD 15/1999).

— Los datos no podrán usarse para finalidades distintas de aquellas para las que hubieran sido recogidos (art. 4 LOPD 15/1999).

— La publicidad formal ha de expresar fielmente los datos contenidos en los asientos registrales, pero sin extenderse a más de lo que sea necesario para satisfacer el legítimo interés del solicitante.

— La solicitud de información sobre datos personales sin relevancia patrimonial se realizará con expresión del interés perseguido, que ha de ser conforme con la finalidad del Registro, quedando bajo la responsabilidad del registrador la atención de las consultas relativas a la

publicidad de datos personales. En todo caso, los datos carentes de trascendencia jurídica solo pueden ser cedidos o accedidos con el consentimiento de su titular.

En este sentido debe tenerse en cuenta que por «datos personales» no debe entenderse solamente los datos íntimos de la persona, sino cualquier tipo de dato, sea íntimo o no, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales (art. 3 LOPD 15/1999).

Entre ellos están los que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias pueda constituir una amenaza para el individuo (art. 7 LOPD 15/1999).

[53] Véase: Juan María DÍAZ FRAILE. Comentarios a la Directiva y al Proyecto de Ley español de comercio electrónico de 2000. Contenido y proceso de elaboración. *Revista Crítica de Derecho Inmobiliario*. Año LXXVII; número 663; enero-febrero de 2001.

[54] Véase: https://www.boe.es/buscar/act.php?id=BOE-A-2002-13758.

[55] Véase: https://www.boe.es/buscar/act.php?id=BOE-A-2007-20555.

[56] Véanse, por ejemplo, los siguientes informes de la Comisión de las Naciones Unidas para Europa (UN-ECE): *Land Administration Guidelines with Special Reference to Countries in Transition, United Nations*, Nueva York y Ginebra, 1996 y *Social and Economic Benefits of Good Land Administration*, Ginebra, 1998.

[57] Véase: *European Commission, The Integration of the EU Mortgagee Credit Markets, Report by the Forum Group on Mortgagee Credit*, Internal Market Directorate General, Bruselas, 2004.

[58] Entre otros, los informes de la OCDE: *Flexible Personnel Management in the Public Service, Public Management Studies*, París, 1990; *Pay Flexibility in the Public Service*, París, 1993; y *Private Pay for Public Work: Performance-Related Pay for Public Sector Managers*, París, 1993.

[59] Véanse los artículos 106 y siguientes, las disposiciones adicionales 26.ª y 28.ª y las disposiciones transitorias 19.ª y siguientes de la Ley 24/2001, de 27 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social, modificada posteriormente por la Ley 24/2005, de 18 de noviembre, de reformas para el impulso a la productividad. https://www.boe.es/diario_boe/txt.php?id=BOE-A-2001-24965.

[60] Véanse, sobre esta materia, los informes Doing Business del Banco Mundial: *World Bank, Doing Business: Measuring Business Regulations*, World Bank, Washington DC, 2004-2014 (http://www.doingbusiness.org).

[61] Veáse: http://internationalpropertyrightsindex.org/country?c=SPAIN.

[62] Véase: *European Commission, The Integration of the EU Mortgagee Credit Markets*, *op. cit.*, n. 15.

[63] «*España es uno de los países más eficientes en términos de costes de operación (costes de distribución, establecimiento y servicio) como % del saldo vivo (un 0,38%), solo superado por Dinamarca (un 0,35%). En el cálculo de estos influyen factores estructurales, como por ejemplo, el tamaño del crédito, la regulación del cobro, o el tiempo requerido para el registro. La eficiencia de la garantía es un factor determinante en los costes, y en último lugar en el precio. En países como Dinamarca, Holanda o España, con un sistema de garantía hipotecaria sólido, el tiempo medio de formalización del préstamo hipotecario y la duración media de la ejecución son sin duda alguna, unos de los más rápidos de toda Europa, lo que se traduce en menores costes para las entidades, que son trasladados a los precios que soporta el prestatario*» (European Commission, The Integration of the EU Mortgagee Credit Markets, *op. cit.*, n. 15; traducción de la Asociación Hipotecaria Española, «Informe sobre los mercados hipotecarios en Europa», Madrid, 15 de diciembre de 2004, 15).

[64] Véase: COMP/2006/D3/003, Bruselas, 2007.

[65] Véase: *European Mortgage Federation, Study on the Cost of Housing in Europe*, Bruselas, 2010, mayo, figura 2, 9.

(Trabajo recibido el 31-10-2017 y aceptado para su publicación el 8-11-2017)