derecom

ISSN: 1988-2629. Nº. 27. Nueva Época. Septiembre 2019-Marzo 2020

Cómo citar este texto:

Rubén Rodríguez Abril (2019). Sobre la legitimación criptográfica de firmas en los contratos. *Derecom*, 27, 112-138. http://www.derecom.com/derecom/

SOBRE LA LEGITIMACIÓN CRIPTOGRÁFICA DE FIRMAS EN LOS CONTRATOS

ON THE CRYPTOGRAPHIC CERTIFICATION OF SIGNATURES IN AGREEMENTS

© Rubén Rodríguez Abril
Universidad de Sevilla (España)
r_r_abril@hotmail.com

Resumen

En el presente trabajo el autor explora diferentes posibilidades de aplicación de la tecnología de cadena de bloques (*blockchain*) a los negocios jurídicos celebrados por vía telemática, particularmente en áreas reservadas hasta ahora a la intervención notarial. Esta tecnología, unida a la identificación biométrica, y a los certificados digitales, ha creado un nuevo modelo de legitimación de firmas, con los mismos efectos que la prevista en el Reglamento Notarial español. El autor propone crear un registro electrónico de documentos privados usando la tecnología de cadena de bloques. Dicho registro sería de titularidad pública y se encargaría de identificar a las partes intervinientes en los documentos, legitimar sus firmas, imponer sellos de tiempo, determinar la ley aplicable a su contenido y finalmente otorgar carácter ejecutivo a los documentos continentes de títulos de crédito, en los términos del artículo 517 de la Ley de Enjuiciamiento Civil española o el Reglamento (CE) nº 805/2004.

Summary

In the present paper, its author explores the different application possibilities of blockchain technology within the scope of legal agreements performed by electronic means, particularly in areas so far reserved to the intervention of public officials, such as notaries. This technology, combined with biometric identification and digital certificates, has shaped a new way of notarization of documents, which is different indeed from the traditional one but equal in its legal binding. The author of this paper proposes to create an electronic registry of private documents using blockchain technology. This new registry would be state-owned and its tasks would be to identify the parties of a registered document, notarize their signatures, issue timestamps, set the law applicable to its content, and finally confer the status of enforceable titles to those documents containing pecuniary claims, in conformity with article 517 of the Spanish Civil Procedure Law or the European Regulation (CE) nº 805/2004.

Recibido: 02/07/2019 Revisado: 16/08/2019
Aceptado: 27/08/2019 Publicado:15/09/2019

Palabras clave: Documentos electrónicos. Blockchain. Cadena de bloques. Notarios. Fe pública.

Keywords: Electronic documents. Blockchain. Civil-law notaries. Notarial attestation.

PARTE 1:
LA CRECIENTE INTERRELACIÓN ENTRE DERECHO Y CIBERNÉTICA

1. Introducción

Durante los siglos XII y XIII, los cambios sociales y económicos que estaban teniendo lugar en el norte de Italia dieron inicio a una verdadera revolución jurídica. El viejo Derecho Romano, rígido y formalista, que se estudiaba en las recién nacidas universidades europeas, no era capaz de dar respuesta a las crecientes necesidades del comercio a gran escala. Por este motivo, surgieron, paralelamente al Derecho Civil, una serie de usos comerciales que terminaron cristalizando en una nueva rama de la ciencia jurídica: el Derecho Mercantil. Aparecieron instituciones como las letras de cambio, las sociedades en comandita, o los apoderamientos mercantiles y se generalizó el crédito, cuya concesión por parte de cristianos había estado hasta entonces prohibida por el Derecho Canónico.

En el ámbito del derecho puramente civil, en esta misma época surgió la institución del notariado latino: La economía mercantilizada de las ciudades de Europa Occidental necesitaba de juicios ejecutivos que dieran rápida satisfacción a los acreedores impagados, y requería de títulos privilegiados en el tráfico jurídico que dieran fe de la existencia de estas obligaciones crediticias, y que sirvieran de base para los citados procedimientos de ejecución. Es en este contexto cuando surge la noción de documento público, es decir, aquel documento jurídico en cuyo otorgamiento interviene un funcionario público -el notario- que comprueba, no sólo la identidad y capacidad de los otorgantes, sino también la legalidad de las cláusulas del negocio jurídico, al igual que la veracidad de los elementos circunstanciales del mismo, como la fecha o la hora en que se otorga. El documento así otorgado goza de presunción de legalidad y es directamente ejecutivo.

2.El Derecho y la cuarta Revolución Industrial (A las puertas de una revolución jurídica)

A lo largo de estos últimos siglos, la institución de la fe pública y su más insigne creación, el documento público, han contribuido a la agilización del tráfico de derechos, aportando instrumentos fundamentales para la seguridad jurídica. Sin embargo, en mi opinión, en el momento de escribir estas líneas nos situamos en los albores de una revolución jurídica que a nuestro juicio será similar en magnitud a la que tuvo lugar en Europa Occidental en los siglos XII a XIV. Esta revolución jurídica a la que nos referimos será impulsada por las tecnologías de la llamada Revolución Industrial 4.0, que permitirán, entre otras cosas, obtener y almacenar información de una manera fehaciente, y garantizar la integridad de la misma por medio de funciones criptográficas que hagan computacionalmente inviable falsificar archivos y documentos electrónicos, sin invertir previamente grandes cantidades de energía y de recursos.

El tráfico jurídico dentro del ámbito cibernético vendrá caracterizado por las siguientes notas:

a) **Descentralización**: Hasta este momento, en la mayoría de los ordenamientos jurídicos occidentales, el tráfico de derechos reales sobre bienes inmuebles, la constitución de empresas, así como la creación de dinero y concesión del crédito han sido controlados por instancias centralizadas. En unos casos, por cuerpos de funcionarios capacitados para el ejercicio de la fe pública, como los notarios o los registradores de la propiedad. En otros casos, por bancos centrales que monopolizan la creación y emisión del dinero, y por sistemas de pago dependientes de cámaras de compensación, como los sistemas EURO1 o STEP2, operados por la sociedad EBA Clearing, y que han sido declarados "de importancia sistémica" por parte del Banco Central Europeo. En los nuevos sistemas descentralizados surgidos durante la última década, la seguridad del tráfico de derechos viene garantizada por una red descentralizada de nodos (computadoras conectadas a una red), que se comunican y se ponen de acuerdo entre sí mediante un *protocolo de consenso*, que evita que los datos almacenados en todos ellos puedan ser alterados de una manera maliciosa por parte de terceras personas.

b) **Inmutabilidad**: En el marco de los Registros de la Propiedad, la información relativa a los bienes inmuebles es almacenada en *asientos*, de los que se toma razón en las *hojas abiertas* a cada una de las fincas. Estas hojas se encuadernan a su vez en tomos y libros cuya titularidad es estatal. En el ámbito del notariado, los documentos públicos son almacenados en un conjunto de libros denominado *protocolo*, custodiado por el propio notario, que se encarga de dar fe de la veracidad, integridad y legalidad de los documentos allí archivados y de custodiar el propio protocolo. Notarios y registradores de la propiedad son garantes, por tanto, de la integridad e inalterabilidad de los datos almacenados en los archivos que ellos custodian.

   En las redes informáticas que funcionan mediante tecnología *blockchain,* los documentos electrónicos son agrupados en bloques, que a su vez son ensamblados en una cadena (de ahí la denominación inglesa *blockchain*, que significa cadena de bloques) por medio de funciones criptográficas que enlazan unos bloques con otros, y cuyo cálculo es realizado por ordenadores denominados *mineros*, que han de emplear para ello amplios recursos computacionales (potencia de la CPU, en el caso de Bitcoin, y espacio de memoria en el caso de la red de Ethereum). Para falsificar los datos almacenados en la *blockchain* sería necesario volver a reconstruir toda la cadena, y volver a calcular todos los valores criptográficos que enlazan los bloques, un costosísimo procedimiento que quedaría fuera del alcance de la potencia computacional de los ordenadores ordinarios actuales.

c) **Determinismo**: En la cadena de bloques, la seguridad jurídica se garantiza por medio de algoritmos deterministas, que son aquellos cuya aplicación arroja el mismo resultado para un mismo conjunto de datos de entrada. El determinismo permite la coordinación de todos los nodos de la red - pues todos ellos siguen unas mismas reglas de comportamiento- y la resolución del denominado **problema de los generales bizantinos**, que surge cuando en uno o varios nodos existen divergencias sobre el estado de la cadena y es necesario determinar cuál es la versión correcta del mismo.

d) **Celeridad**: Mientras que en un registro público o administrativo, la inscripción puede demorarse durante días o semanas, en el protocolo Bitcoin, cada 10 minutos un bloque

de transacciones es incorporado a la cadena. En Ethereum, cuya red permite la programación y ejecución de contratos inteligentes, este tiempo se reduce a 17 segundos. Ripple, el protocolo criptográfico más usado por los bancos en la actualidad, tiene un tiempo de actualización de su estado de tan sólo 4 segundos.

e) **Anonimato**: En la cadena de bloques, y en los negocios jurídicos cibernéticos en general, los participantes son identificados por medio de un número denominado *clave pública*, que a su vez está matemáticamente vinculado con otra variable numérica, la *clave privada.* Esta última es la que permite la realización de actos de disposición sobre criptomonedas y derechos cibernéticos. Expondremos pormenorizadamente estos conceptos en secciones subsiguientes.

3. El nuevo ordenamiento algorítmico: definición y características

En el marco de la doctrina jurídica y de la teoría de la computación sólo recientemente han comenzado a surgir debates sobre la naturaleza jurídica de las criptomonedas y de los contratos inteligentes. A nuestro juicio, se trata de fenómenos de naturaleza claramente extrajurídica que aunque no tienen conexión directa con el mundo del Derecho, sí que están comenzando a configurar una nueva institución, a la que en este trabajo denominamos *ordenamiento algorítmico* y que tiene grandes analogías con el ordenamiento jurídico. En los párrafos subsiguientes analizaremos las peculiares relaciones entre ambos conceptos.

El jurista italiano Santi Romano en su obra *L'ordinamento giuridico*, del año 1917, definía al **ordenamiento jurídico** como aquel conjunto de normas vigente en un determinado territorio, dotado de las características de **unidad, plenitud y sistematicidad**. A mi juicio, estas características son plenamente aplicables también al ordenamiento algorítmico:

La **unidad** de cada ordenamiento jurídico viene garantizada por la existencia de una única Ley Fundamental (*Grundnorm*, en la terminología de Hans Kelsen), situada en la cúspide de la pirámide normativa, y en la cual fundan su validez, de una manera mediata o inmediata, el resto de las normas vigentes en el territorio de que se trate. En el ámbito cibernético, el papel de la *Grundnorm* viene representado por el protocolo que rige las transmisiones de criptomonedas (por ejemplo, en el caso del Bitcoin) o por las normas de funcionamiento de la máquina virtual que interpreta y ejecuta los contratos inteligentes (un claro ejemplo vendría dado por la Máquina Virtual de Ethereum, EVM).

El segundo elemento, el de la **plenitud**, exige que cualquier conflicto que surja en la vida social pueda ser resuelto con arreglo a las normas del ordenamiento, y que existan mecanismos para cubrir las lagunas jurídicas, esto es, la ausencia de regulación legal en un determinado ámbito de la vida social. En algunas cadenas de bloques, como Ethereum, este requisito de plenitud trata de ser garantizado mediante el uso de lenguajes de programación Turing-completos, que son aquellos que tienen el mayor poder computacional posible.[1] Estos lenguajes se corresponden con las gramáticas formales de nivel 0 dentro de la jerarquía de Chomsky, que no tienen restricción alguna y que poseen la capacidad expresiva máxima. Pero los lenguajes de programación Turing-completos, precisamente por su complejidad, facilitan la presencia de *bugs* y vulnerabilidades en el código, y posibilitan con ello ataques procedentes del exterior. Asimismo, los programas elaborados con estos lenguajes pueden contener bucles infinitos que hagan "colgarse" al programa (en este caso, el contrato inteligente) y le hagan incapaz de comunicarse con el exterior. No existe ningún procedimiento que permita determinar universalmente si un determinado programa se va a quedar colgado o no, lo que se conoce en teoría de la computación con el nombre de *problema de la parada*.

Por otro lado, se han realizado estudios que demuestran que una porción no desdeñable de contratos inteligentes desplegados (*deployed*) en la *blockchain* de Ethereum presentan defectos en su diseño de programación que bloquean los fondos almacenados en los mismos, haciendo imposible su disposición.[2] Por todos estos motivos, existen propuestas para utilizar dentro de Ethereum, u otras *blockchains*, lenguajes de programación que no sean Turing-completos, lo cual en mi opinión constituye un grave error, toda vez que ello limitaría extraordinariamente la versatilidad de los contratos inteligentes que pudieran diseñarse. Versatilidad frente a seguridad: Ése es el dilema.

Todas estas consideraciones de carácter teórico y práctico demuestran que el requisito de plenitud no puede ser garantizado desde el interior de la propia cadena de bloques. A nuestro juicio, el ordenamiento algorítmico necesita de actores externos a la propia cadena que garanticen la ausencia de lagunas en el ámbito de la contratación inteligente. Se trataría de personas físicas o jurídicas que firmarían criptográficamente el contenido de los contratos y se harían responsables del contenido de los mismos, haciendo frente patrimonialmente a los posibles perjuicios que pudieran sufrir las partes intervinientes en el caso de un ataque informático, de un error de diseño o de cualquier otra causa subsumible en el supuesto de hecho del artículo 1902 del Código Civil.

En tercer y último lugar, la **coherencia** de un ordenamiento implica la existencia de mecanismos que permitan resolver las contradicciones/colisiones que pueda haber entre las diferentes normas jurídicas del mismo. Por ejemplo, en Derecho las disposiciones de rango superior tienen prioridad sobre las de rango inferior (*lex superior derogat inferiori*), y las leyes anteriores son derogadas por las posteriores (*lex posterior derogat priori*). En el ámbito cibernético-algorítmico, la coherencia dentro de una base de datos distribuida se logra mediante el uso de un *protocolo de consenso*, encargado de resolver las posibles discrepancias que puedan existir entre los nodos de la red sobre la validez o invalidez de los negocios jurídicos realizados dentro de la misma, como por ejemplo, las transacciones de criptomonedas o *tokenes* o la ejecución de contratos inteligentes.

El **ordenamiento algorítmico** podría ser definido como *conjunto de algoritmos, residentes en la capa de aplicación, que regulan el funcionamiento y la modificación del estado de una base de datos distribuida*. El término "algorítmico" pretende subrayar el hecho de que todos los cambios de estado que tienen lugar en un protocolo distribuido (por ejemplo. transferencias de activos, variaciones en los saldos de las cuentas, etc.) tienen lugar mediante operaciones algebraicas realizadas de una manera automatizada. Como **notas que distinguen al nuevo ordenamiento algorítmico del ordenamiento jurídico tradicional**, podemos señalar las siguientes:

a) **El algoritmo es la Ley**. En otras publicaciones (Lessig, 2001) este principio aparece bajo la forma de "El código es la Ley". Nosotros recomendamos sustituir el término "código" por el de "algoritmo", dado que la primera palabra tiene un significado ambiguo, que puede dar lugar a molestas homonimias. Así, en Teoría de la Computación, *código* es el conjunto de instrucciones que componen un determinado programa informático. Por el contrario, en el marco de la Teoría del Derecho, un *código* es un texto legal, dotado de las características de unidad, cohesión y sistematicidad, que regula una parcela determinada del ordenamiento jurídico.

Las normas jurídicas pueden ser definidas como *patrones de conducta impuestos a los miembros de una comunidad social, caracterizados por las notas de* ***imperatividad, generalidad y coercibilidad*****.** Las normas son **imperativas**, dado que contienen un **mandato** a los miembros de la comunidad para que realicen, o se abstengan de realizar, una determinada conducta, como por ejemplo pagar impuestos u obedecer las leyes penales. Las normas también son **generales**: tienen vocación de ser aplicables al conjunto de la población y no a individuos en particular (lo que las diferencia de los antiguos privilegios feudales, y de los actuales actos administrativos, que son de naturaleza particular). Y por último, son también **coercibles,** en la medida en que el ordenamiento jurídico

dispone de mecanismos de sanción (multas, cárcel, etc...) para los supuestos de incumplimiento de sus normas.

Muchos ordenamientos jurídicos extienden la condición de normas jurídicas también a las cláusulas contractuales. Según la mayoría de los códigos civiles europeos, el contenido de un contrato tiene fuerza de ley entre las partes contratantes, aunque a diferencia de las leyes ordinarias -las que emanan del poder legislativo- las cláusulas de los contratos no tienen efectos frente a todos (*erga omnes*), sino que sólo tienen una eficacia relativa, que se restringe a las partes que han intervenido en el propio contrato (*res inter alios acta*).

Dentro del ordenamiento algorítmico, el concepto de norma tiene una naturaleza radicalmente diferente: el Derecho Objetivo -la Ley- viene conformado por los algoritmos que regulan el funcionamiento de cada uno de los nodos, el protocolo de consenso que permite la coordinación entre los mismos, las reglas de funcionamiento de la máquina virtual[3] encargada de ejecutar y de almacenar los variables de los contratos inteligentes, así como el código de estos últimos.

b) **Anonimato.** Los titulares de los derechos en el ámbito jurídico son identificados por un simple número, la dirección electrónica, y no es necesario dar a conocer las personas físicas o jurídicas que verdaderamente están detrás de la misma. La aparición y difusión de la criptografía asimétrica a partir de la década de los 70 del pasado siglo permitió la construcción de estructuras de transmisión de información completamente anónimas (al menos, en teoría), como la red Tor o el protocolo Bitcoin. En los sistemas de criptografía asimétrica, un computador -aplicando algoritmos de la Teoría de los Números u operando con funciones elípticas- genera dos claves, que no son más que dos números matemáticamente enlazados entre sí que son aptos para encriptar y desencriptar mensajes: El primero de estos números es la **clave pública**, que en el ordenamiento algorítmico se utiliza para identificar al sujeto, y del que deriva matemáticamente la dirección electrónica. El segundo es la clave privada, que otorga al titular del derecho la capacidad de disponer sobre el mismo (por medio de la firma electrónica, como veremos a continuación). La clave pública identifica al titular del derecho subjetivo; la clave privada, le otorga el *ius disponendi* sobre el mismo.

c) ***Quod non est in actis, non est in mundus***. (*lo que no está en las actas del Registro, no está en el mundo*): para que los derechos nazcan, es necesario que previamente se inscriban en un Registro jurídico. Este principio, también llamado *de inscripción constitutiva* (*Eintragunsgrundsatz*) rige en el Derecho Inmobiliario de Alemania y de Suiza e impone una identidad absoluta entre el contenido de los asientos registrales y la realidad jurídica extrarregistral. En el ámbito cibernético-algorítmico, los derechos subjetivos se almacenan y se inscriben en el *estado de la cadena de bloques*. Toda mutación jurídica (real o personal) que pretenda producir efectos debe conllevar una modificación correlativa de dicho estado. A menudo, los protocolos de funcionamiento de cadena de bloques, como por ejemplo Ethereum o Hyperledger, disponen de funciones que permiten consultar los datos inscritos, introducir nuevo código ejecutable (*deployment transaction*), o bien invocar este código (*invocation translation*).

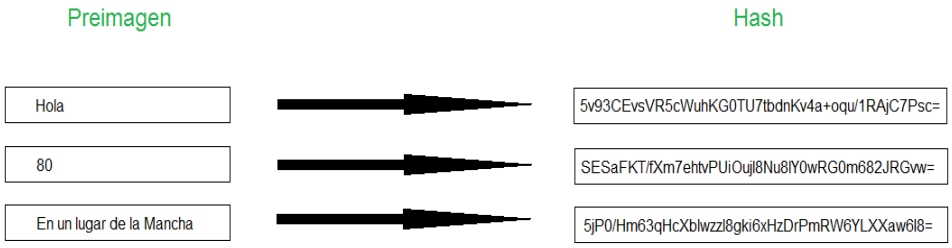
d) **Inembargabilidad**. Los derechos cibernéticos son, en la práctica, inembargables por los tribunales de justicia, dado que el *ius disponendi* está inseparablemente vinculado a las claves privadas de su titular. Si dichas claves se pierden, la única manera de recuperar las criptomonedas es obligando a la mayor parte de los nodos de la red a aceptar unas nuevas reglas de juego, un nuevo estado de la cadena de bloques que reponga los daños causados por los atacantes. Este procedimiento se denomina *bifurcación dura* (*hard fork*), y fue utilizado para reparar los daños causados por el ataque al DAO

(*Decentralized Authonomous Organization* -"Organización Autónoma Descentralizada"-, una plataforma de contratos inteligentes) de Ethereum que tuvo lugar en Julio de 2017. En otros casos, si la implementación de un *hard fork* no es posible, las pérdidas producidas por la sustracción de contraseñas devienen irreparables, como han demostrado casos recientes de gran resonancia mediática.[4]

4. Elementos de criptografía utilizados en el ordenamiento algorítmico

a) Funciones resumen (hashes)

Las denominadas *funciones resumen* (o funciones *hash*, en su original inglés) gozan de una extraordinaria importancia en materia de criptografía y de derecho cibernético. Pueden ser definidas como aquellas funciones matemáticas que transforman cadenas de caracteres, cualquiera que sea su extensión, en números de una longitud fija. No importa cuán larga o corta sea la longitud de la cadena original: el tamaño de la función resumen es siempre el mismo, y viene predeterminado por el algoritmo que lo calcula.



Fuente: Elaboración propia

Las funciones resumen se caracterizan por las siguientes propiedades:

-**Unidireccionalidad**: No es posible obtener el texto original, denominado a veces con la expresión matemática de *preimagen*, a partir del valor de su función resumen.

-Bajo coste computacional: Pueden ser fácilmente calculadas por ordenadores con potencia de cálculo y espacio de memoria limitado.

-**Resistencia a colisiones**: Por lo general, es bastante baja la probabilidad de encontrar aleatoriamente dos textos diferentes que tengan un mismo valor (*colisión*) de función resumen.

-**Efecto avalancha**: Idealmente, el cambio de tan sólo un único bit en el mensaje original debe provocar la alteración de la mitad de los dígitos de su *hash.* Para garantizar el efecto avalancha, buena parte de las funciones resumen que se usan hoy en día en criptografía utilizan el esquema de Merkle-Darmgard. El mensaje a comprimir se divide en bloques de igual tamaño y cada uno de los caracteres del mensaje originario es codificado mediante un número natural. Un número, denominado raíz, y cuyo valor depende del algoritmo que utilicemos, va progresivamente combinándose con los bloques del texto a comprimir.

Las características descritas en los párrafos anteriores hacen de las funciones *hash* un instrumento particularmente apropiado para la corrección de errores producidos durante una

transmisión de datos (*código MDC*, *Manipulation Detection Code*), para la verificación de la autenticidad de un mensaje (*código MAC, Message Authentication Code*), así como para firmar electrónicamente documentos, como veremos en la sección subsiguiente.

a) Criptografía asimétrica

Los sistemas criptográficos utilizados para garantizar la confidencialidad y la integridad en las comunicaciones suelen clasificarse en dos grandes familias:

-Sistemas basados en **criptografía simétrica**: El emisor y el receptor usan la misma clave para encriptar y para desencriptar sus mensajes. A esta familia pertenecen, entre otros, el *algoritmo AES (Advanced Encryption Standard)*, utilizado en buena parte de las comunicaciones que tienen lugar a través de Internet -particularmente en el protocolo WPA2, que garantiza la integridad de las comunicaciones a través de WiFi-, el *cifrado de Vigenère*, que resistió los intentos de ruptura por parte de los criptógrafos durante más de tres siglos, y el algoritmo de la legendaria máquina Enigma, utilizada por las fuerzas armadas alemanas durante la II Guerra Mundial y quebrado por los especialistas británicos que trabajaban en las instalaciones de Benchley Park. Los sistemas de criptografía simétrica requieren que ambas partes hayan compartido previamente, a través de un canal seguro, la contraseña utilizada para el cifrado.

-Sistemas basados en **criptografía asimétrica**: Las partes no necesitan compartir previamente ninguna clave común. El ordenador del sujeto interviniente genera dos números, que representan dos claves diferentes: La **clave pública**, que se pone a disposición de todos, y la **clave privada**, que queda en manos del propio sujeto, y cuyo valor tiene que ser cuidadosamente preservado en secreto, so pena de que el cifrado de las comunicaciones se rompa.

Cada una de estas dos claves es utilizada respectivamente por el usuario para cifrar o para descifrar un mensaje. Se abren con ello dos posibilidades:

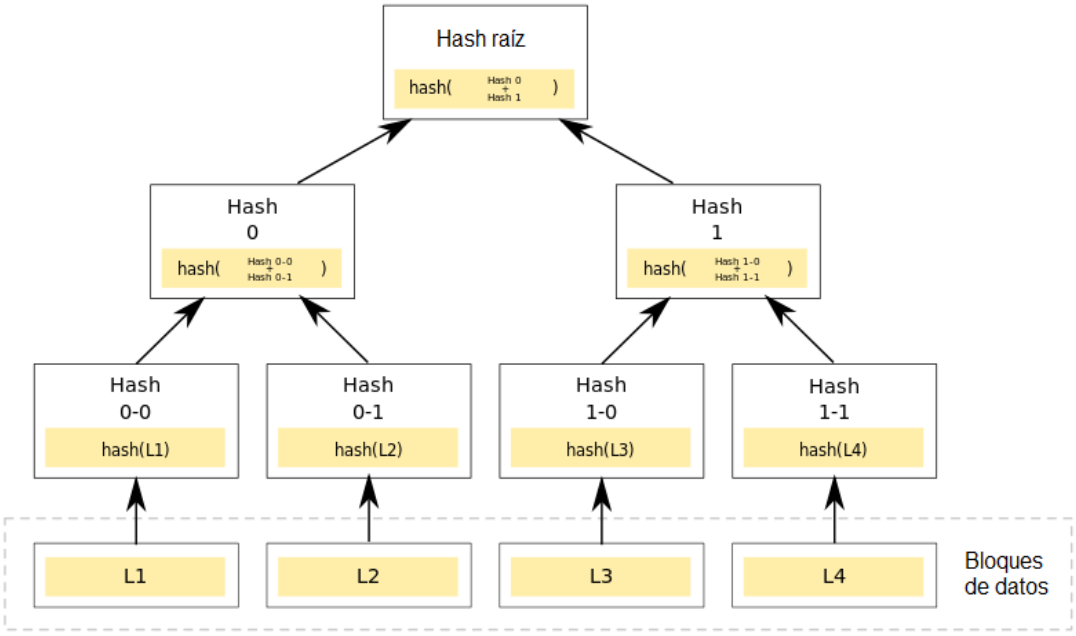
a) En la ***encriptación de clave pública***, el usuario pone su clave pública a disposición de los demás usuarios, que *encriptan* sus mensajes mediante la realización de operaciones matemáticas con dicha contraseña. Los mensajes son enviados al usuario, que con ayuda de su clave privada puede a su vez *desencriptarlos*.

b) En el caso de la ***firma de documentos electrónicos*** sucede exactamente lo contrario. El usuario hace un *hash* al documento que pretende firmar, y combina matemáticamente dicho *hash* con su clave privada. El número resultante es la firma electrónica, que queda incorporada al documento. Los demás usuarios pueden verificar dicha firma con ayuda de la clave pública.

c) Árboles de Merkle

Un árbol de Merkle es una estructura de datos, en la que los *hashes* (funciones resumen) de diferentes bloques de datos (archivos de texto, imágenes, documentos electrónicos, etc...) se estructuran en un esquema arborescente, de tal manera que el hash de cada nodo del árbol se obtiene a partir de la combinación de sus dos nodos hijos. Por este motivo, los árboles de Merkle se denominan a menudo **árboles binarios**.

Para que el lector se haga una idea, si quisiéramos construir un árbol de Merkle a partir de un conjunto de archivos, primero deberíamos extraer sus hashes, y luego estructurar a estos últimos en una suerte de árbol, en el que cada rama, cada nodo, sólo pudiera bifurcarse en dos. Los hashes quedarían colocados en los extremos de cada rama, siguiendo el esquema de este diagrama.[5]



Fuente: Wikimedia Commons

Tras ello, procederíamos a calcular los valores resumen de los nodos intermedios. El hash de cada nodo se obtiene combinando los hashes de sus dos nodos hijos. Aplicando recurrentemente este procedimiento llegamos a la raíz del árbol, y el valor-resumen de esta última es el que corresponda al árbol de Merkle al completo.

Como veremos en subsiguientes secciones, los árboles de Merkle ofrecen un marco muy útil para el archivo -y la codificación en bloques- de los negocios jurídicos electrónicos.

5.Los negocios jurídicos cibernéticos

El protocolo bitcoin sólo configura dos tipos de negocios jurídicos: las *transmisiones* de criptomonedas y las *adquisiciones originarias* de las mismas por parte de los mineros.

En el Derecho Continental de origen romano, la doctrina jurídica ha venido distinguiendo -ya desde la Edad Media- entre *adquisiciones originarias* y *adquisiciones derivativas*. Las adquisiciones *originarias* son aquellas en las que el derecho de propiedad nace en el mismo momento en que es incorporado al patrimonio de una persona determinada, tal y como sucede en el caso de la ocupación de una cosa mueble que hasta ese momento carece de dueño. Las adquisiciones *derivativas* de derechos nacen como consecuencia de la transmisión de los mismos, como sucede en el caso de las compraventas, o las constituciones de usufructo u otro tipo de derechos reales sobre cosa ajena.

El protocolo Bitcoin mantiene esta dualidad y también distingue entre adquisiciones de criptomonedas derivativas y originarias. Las primeras se articulan a través de las denominadas

transacciones regulares (*regular transactions*), mientras que las segundas tienen lugar a través de las llamadas *transacciones de acuñación* (*coinbase transactions*). En terminología jurídica, se puede decir que el protocolo bitcoin regula tanto la tradición como la ocupación.

Las **transacciones regulares pueden ser definidas como aquellos negocios jurídicos electrónicos en los que el titular de una o varias direcciones públicas transmite(n) a otro u otros titulares una cantidad cierta y determinada de bitcoins**. Cada transacción incorpora el *número de versión (nVersion)* del protocolo Bitcoin que se ha utilizado para elaborar el documento que la contiene, el *vector de entradas (vin)* de la transacción -donde se recogen los datos de cada uno los transmitentes de criptomonedas-, el *vector de salidas* (*vout*) -donde se hace lo propio con los datos de los adquirentes de las mismas- y, por último, el *plazo de tiempo* (*nLockTime*) concedido a todos los intervinientes para firmar electrónicamente la transacción.

El **vector de entradas** debe contener la siguiente información **de cada uno** de los transmitentes de bitcoins:

a) El número identificativo de la transacción anterior (*transaction ID* o *TXID*) de la que la transmisión actual trae causa, y en la que el transmitente actual adquirió sus bitcoins. Los sucesivos titulares de bitcoins forman una suerte de cadena, en uno de cuyos extremos se halla una *coinbase transaction* -donde se acuñaron originariamente los bitcoins- y en el otro, una transacción aún no gastada. Los eslabones de la cadena vienen formados por las transmisiones sucesivas de bitcoins, que forman una suerte de ***tracto sucesivo criptográfico***, muy parecido al señalado por el artículo 20 de la Ley Hipotecaria española, que señala que

> *Para inscribir o anotar títulos por los que se declaren, transmitan, graven, modifiquen o extingan el dominio y demás derechos reales sobre inmuebles, deberá constar previamente inscrito o anotado el derecho de la persona que otorgue o en cuyo nombre sean otorgados los actos referidos*

o el artículo 3 del Decreto francés nº 55-22 del 4 de Enero de 1955, regulador de su sistema registral: *aucun document sujet à publicité foncière ne peut être publié au fichier immobilier avant que le tître du disposant ou du dernier titulaire de l'immeuble n'ai été lui-même publié*.

b) El número identificativo del transmitente, en el caso de que fueran varios los que intervienen en la transacción.

c) Longitud del *script* de firma del transmitente (*scriptSigLen*).

d) *Script* de firma del transmitente (*scriptSig*).

e) Número de secuencia de la transacción.

El **vector de salidas** contiene las siguientes menciones relativas a cada uno de los adquirentes de bitcoins:

a) Cantidad de bitcoins adquiridos por el *accipiens* (*nValue*). La suma total de los bitcoins que se adquieren no puede ser superior a la de los bitcoins que se hallan en poder de los transmitentes, en línea con lo que señalaba el viejo brocardo latino -acuñado por el jurista Ulpiano-*nemo plus iuris transferre potest quam ipse habet* ("nadie puede dar más de lo que uno tiene")-. En el caso contrario, cuando se transmiten más bitcoins de los que se adquieren, la transmisión es válida, y el minero hace suya la diferencia.

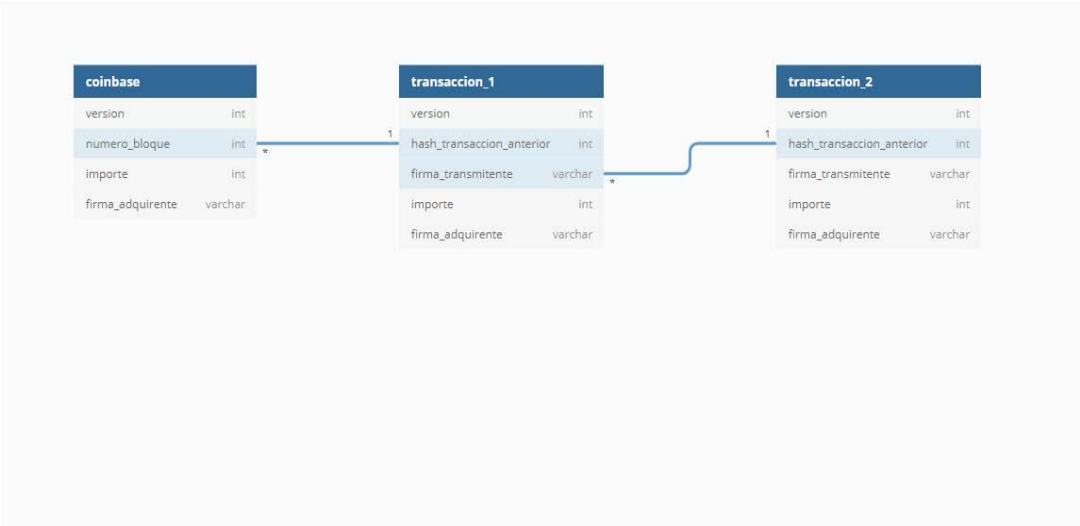
b) Longitud del script de firma del adquirente (*scriptSigLen*)

c) *Script* de firma del adquirente (*scriptSig*).

Como ya se ha señalado anteriormente, las transacciones son ensambladas en bloques por nodos denominados mineros. El nodo que consigue ensamblar un bloque de transacciones recibe un premio en bitcoins, cuyo importe ha ido variando a lo largo del tiempo. A medida que el número de bitcoins en circulación aumenta, disminuye el premio a recibir por los nodos. En el momento en que se escribe este artículo (Agosto de 2019) hay 18 millones de bitcoins en circulación y el ensamblado de un nuevo bloque de la cadena supone un premio de 12,5 bitcoins.

La adquisición de este premio en bitcoins se instrumentaliza a través de un *negocio jurídico electrónico, de carácter originario*, denominado *transacción de acuñación* (*coinbase transaction*), que tiene la misma estructura que las transacciones regulares. Sólo se diferencia en la estructura de su vector de entradas, que es la siguiente:

a) El campo del ID de la transmisión anterior (*TXID*), tiene un valor nulo.
b) El campo relativo al número de identificación del transmitente tiene un valor de 2^32-1.
c) El *campo de acuñación* (*coinbase field*), que codifica y almacena la longitud de la cadena de bloques hasta este momento.
d) Longitud del campo de acuñación (*coinbaseLen*).



Fuente: Elaboración propia

6.Comparación entre los protocolos notariales y la estructura de la cadena de bloques

Los documentos públicos otorgados ante notario se conservan en poder del mismo, y son encuadernados en su archivo personal, denominado **protocolo**, cuya titularidad es estatal. A los otorgantes del documento no se les entrega el original del mismo, sino una copia fehaciente dotada de los efectos de la fe pública. El protocolo notarial así descrito puede ser definido como *el conjunto ordenado de escrituras públicas y pólizas intervenidas otorgadas por un notario durante un año natural*. Los documentos jurídicos integrados en este protocolo deben estar ordenados cronológicamente y adecuadamente encuadernados en forma de libros.

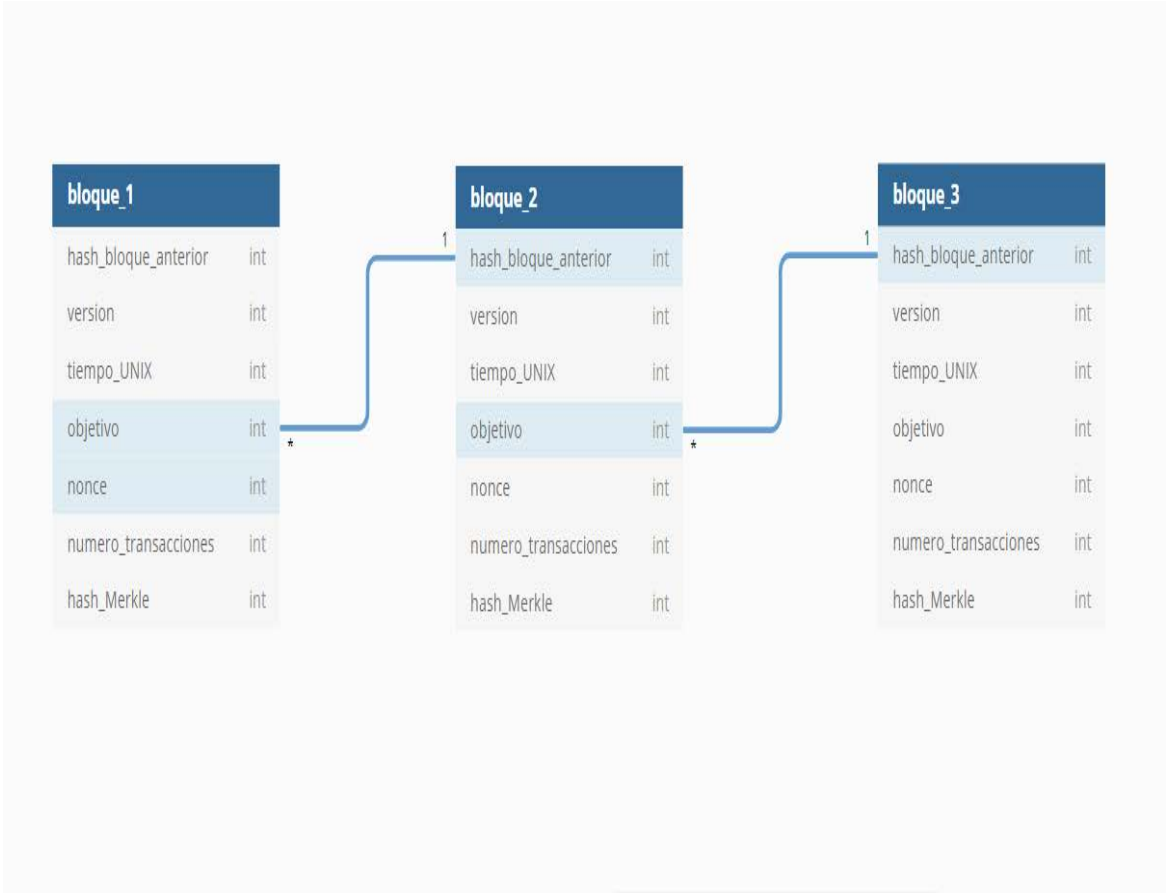
El origen de los protocolos notariales se remonta a tiempos de la Escuela de Bolonia (escuela de escribanos surgida en el norte de Italia a mediados del siglo XIII), en el seno de la cual se estableció la costumbre de que los notarios guardasen los originales de los documentos autorizados, entregando a los otorgantes tan sólo un traslado (copia autorizada) del contenido íntegro de los mismos.

En el caso del protocolo Bitcoin, los negocios jurídicos traslativos de criptomonedas son ensamblados en *bloques de transacciones*, que usualmente tienen un tamaño de un megabyte, aunque este valor ha ido oscilando con el tiempo. Estas transacciones son ensambladas por nodos (ordenadores conectados a la red) denominados *mineros*, que para completar dicho ensamblado deben resolver previamente un complejo problema matemático, cuya solución requiere de amplios recursos computacionales. Los mineros que consiguen resolver el problema -y con ello ensamblar un bloque de transacciones- son premiados con una suma en bitcoins.

La **estructura de los bloques** es simple: Se componen de un *encabezado*, que actúa como una suerte de índice y que contiene referencias a los bloques inmediatamente anterior y posterior, y del *cuerpo del bloque*, que contiene todas las transacciones del mismo.

El encabezado ha de contener las menciones siguientes:

-La versión del protocolo Bitcoin usada por el minero que ensambló los bloques.
-El *hash* del encabezado del bloque inmediatamente anterior.
-El *hash* de la raíz del árbol de Merkle de las transacciones integradas en el bloque. Los hashes de cada una de las transacciones se ensamblan en la estructura arborescente señalada en la sección anterior. El hash de la raíz del árbol resultante se incorpora al encabezado.
-Tiempo universal de UNIX, que mide la cantidad de segundos transcurridos desde el 1 de Enero del año 1970.
-El objetivo (*target*), que determina la dificultad del problema computacional que debe ser superado por el minero que ensambla el bloque.
-El *nonce*: es el número que resuelve dicho problema matemático, y por cuya obtención trabaja el minero.



Fuente: Elaboración propia

El encabezado de cada bloque contiene -como vemos- el *hash* del encabezado del bloque anterior y, de este modo, los diferentes bloques se ordenan temporalmente y se enlazan los unos a los otros mediante *hashes*, formando una cadena en cuyos extremos se encuentra el bloque primigenio, denominado "Bloque del génesis" y creado en el año 2009, mientras que en el otro de los extremos se encuentra el más reciente de los bloques.

En el protocolo Bitcoin, el principio de tracto sucesivo existe en un doble ámbito: en el de las transacciones individuales y en de los bloques. Los negocios jurídicos y los bloques se encadenan mediante funciones criptográficas que forman una estructura que da nombre al sistema: cadena de bloques o *blockchain*.

De conformidad con el artículo 274 del Reglamento Notarial, los protocolos son secretos, y su contenido, en general, no es libremente accesible a los ciudadanos. Por el contrario, en el ámbito de los Registros de la Propiedad, el contenido de los libros es público y los ciudadanos pueden acceder a él a través de certificaciones expedidas por el Registrador o mediante el examen directo de los libros. Las cadenas de bloques pueden configurarse de tal manera que su contenido sea accesible a todos - como sucede en el caso de las redes de Ethereum o Bitcoin- o de modo que la mayor parte de su contenido esté encriptado y sea de acceso restringido.

PARTE 2:
PROPUESTA DE UN NUEVO ESTÁNDAR DE DOCUMENTO ELECTRÓNICO, CON FIRMAS LEGITIMADAS CRIPTOGRÁFICAMENTE

7. Tipología del nuevo documento electrónico

Siguiendo de cerca a Antonio Rodríguez Adrados (1996), podríamos definir al *documento electrónico* como aquel *conjunto de datos -codificados en formato binario- que expresan el pensamiento jurídicamente relevante de su autor*. En el nuevo estándar que proponemos, un documento electrónico que haya de producir efectos jurídicos se codificará en formato ASN.1 y deberá estar dotado de la estructura siguiente:

Documento (Estructura de datos)
- *Negocio jurídico (Estructura de datos)*
  - *Encabezado (Estructura de datos)*
    - *Comparecencia (Estructura de datos)*
      - *Número de contratantes (Número entero)*
      - *Contratante individual (Estructura de datos)*
        - *Nombre y apellidos del contratante (Cadena UTF-8)*
        - *NIF del contratante (Cadena de bytes)*
        - *Certificado X-509 (Cadena de bytes)*
        - *Vector de identificación biométrica (Cadena de bytes)*
        - *Sexo (Booleano)*
        - *Estado civil (Número entero)*
        - *Edad (Número entero)*
        - *Intervención en nombre propio (booleano)*
          - *Mandato en forma electrónica (Estructura de datos)*
    - *Fecha y hora (Estructura de datos)*
      - *Tiempo UTC*
      - *Número de bloque (Número entero)*
      - *Hash del bloque (Cadena de bytes)*
    - *Lugar (Estructura de datos)*
      - *Longitud (Número entero)*
      - *Latitud (Número entero)*
  - *Parte dispositiva (Estructura de datos)*
- *Firmas (Estructura de datos)*
  - *Número de firmantes (Número entero)*
  - *Firma individual (Estructura de datos)*

7.1.¿Es viable técnicamente la creación de registros descentralizados de documentos electrónicos?

Las cadenas de bloques (*blockchain*s) son un tipo de base de datos. En ellas puede almacenarse en principio todo tipo de información susceptible de ser serializada, esto es, codificada en cadenas de *bytes*: no sólo los *hashes* de los documentos electrónicos, sino también el contenido de los mismos. El problema estriba en que el almacenamiento en una cadena de bloques es muy caro. Ensamblar cada bloque de Bitcoin, cuyo tamaño es de poco más de un *megabyte*, supone una recompensa para el minero que ha realizado el ensamblado de unos 12,5 *bitcoins*, suma equivalente a unos 125.000 euros en la cotización que esta criptomoneda tiene en el momento en que se escriben estas líneas (Agosto de 2019). Incorporar un sólo *byte* de información al *blockchain* de Bitcoin cuesta, por lo tanto, 12´5 céntimos de euro. Es un precio superior en varios órdenes de magnitud a los honorarios que pueda percibir cualquier notario en un sistema de Derecho Civil continental basado en la fe pública.

El fenómeno que acabo de describir es conocido en la literatura especializada con la denominación de *problema de la escalabilidad*. La *blockchain* es una base de datos descentralizada cuyos elementos son ensamblados en bloques, que a su vez se ensamblan en una cadena. Dicho ensamblado se realiza por medio de funciones criptográficas (*hashes*), que enlazan unos elementos con los otros, y para cuya determinación es necesario realizar una cierta *prueba de trabajo* por parte de un ordenador incorporado al protocolo, denominado minero. La obligación de realizar *pruebas de trabajo* antes de incorporar bloques a la cadena ha proporcionado –ciertamente- robustez y garantías de integridad a las bases de datos estructuradas en *blockchains*, pero ello ha tenido lugar a costa de dificultar la incorporación de nuevos datos a las mismas.

En mi opinión, mientras no se solucione el problema técnico de la escalabilidad no será posible la creación de registros descentralizados de documentos electrónicos. En el estado actual de la técnica, lo único que se puede hacer es incorporar los *hashes* de dichos documentos a cadenas de bloques como Ethereum, que es lo que en España ofrecían determinadas empresas informáticas cuyos directivos afirmaban, en medios de comunicación, haber creado un sistema alternativo a la fe pública notarial.[6] En realidad, el sistema ofrecido por estas empresas ni identificaba a las partes ni almacenaba (y mucho menos daba publicidad al contenido de los documentos aportados. Su único efecto sustantivo era el de dar por cierta la fecha de un documento privado frente a terceros, en los términos del artículo 1227 del Código Civil.

7.2.Secciones en las que se divide el documento electrónico

El documento electrónico se configurará como una estructura de datos compuesta por tres grandes bloques:

–El **negocio jurídico** propiamente dicho, que es la declaración de voluntad emitida por las partes, y que en el caso de ser un contrato vinculará jurídicamente a las mismas.
–Las **firmas** electrónicas de los intervinientes en el otorgamiento del documento electrónico.
– El **sello de tiempo** del negocio jurídico.

7.2.1.Negocio jurídico

En el modelo que proponemos, los negocios jurídicos se documentarían electrónicamente mediante una estructura de datos compleja articulada en dos secciones: el encabezado y la parte dispositiva.

7.2.1.1.Encabezado

El encabezado del documento habrá de contener información sobre la identidad de los intervinientes en el negocio, el estado civil de los mismos, y la fecha y hora en que tuvo lugar la generación del negociojurídico.

a)Comparecencia eintervención

La comparecencia es la parte del documento electrónico en que se enumeran las personas que otorganelnegociojurídicoycuyadeclaracióndevoluntadconfiguraelcontenidodelmismo.

Mientrasqueenlasescrituraspúblicasordinariaseselnotarioelquedafedeconocimientoy de la identidad de los comparecientes, en los documentos electrónicos dicha fe de conocimiento es reemplazada por los medios de verificación de la cadena de bloques.

Por cada uno de los participantes en el negocio jurídico, deben hacerse constar las siguientes circunstancias:

-Nombreyapellidosdelcontratante, expresados como una cadena en formato Único de (UTF-8).

-**Número de Identificación Fiscal**, que será codificado como una cadena de bytes.

-**Certificado X-509 del contratante**, codificado en cadena de bytes. Los certificados digitales tienen como misión vincular una clave pública con una determinada persona -física o jurídica- o con un servidor determinado (en el caso de los protocolos SSL y TSL, utilizados para garantizar una navegación segura). La verificación de las firmas digitales tiene lugar utilizando los datos contenidos en estos certificados. En España, es la Fábrica Nacional de Moneda y Timbre el organismo competente para la expedición de certificados digitales para personas físicas y jurídicas, de carácter oficial, y que permiten a las mismas perfeccionar negocios y actos jurídicos plenamente válidos frente las Administraciones Públicas.

-Vector de identificación biométrica (Cadena de bytes): Los sistemas de identificación biométrica son aquéllos en los que una persona es identificada por medio de sus rasgos físicos, sean faciales, dactilares, de voz o de cualquier otro tipo. Por lo general, los datos de identificación biométrica del usuario son condensados en archivos denominados *plantillas o modelos,* custodiados en bases de datos, y frente a los cuales se realiza la comparación cada vez que se realiza un proceso de identificación. El robo de las plantillas constituye en sí un problema de seguridad extraordinariamente grave, puesto que si una contraseña o un dispositivo son sustraídos siempre existe la posibilidad de cambiar la primera o desactivar el segundo, pero ello no sucede con los datos biométricos, que están vinculados intrínsecamente a las características físicas de la persona y por ello no pueden ser reemplazados por otros, incluso después de una sustracción de los mismos. Por este motivo, nuestro modelo no propone la incorporación plena de los datos biométricos de los contratantes a la cadena de bloques, sino tan sólo el almacenamiento de una referencia indirecta a los mismos. Proponemos dos sistemas

alternativos: en el primero de ellos, el documento electrónico incorporaría tan sólo el *hash* de la plantilla biométrica, cuyo contenido se almacenaría en una base de datos externa a la cadena de bloques, y que sería consultada por los nodos de la misma cada vez que tuviera que procederse a un procedimiento de identificación. En el segundo de los sistemas, las plantillas se encriptarían homomórficamente y se almacenarían en la propia cadena de bloques. Al estar encriptadas, no sería posible extraer de las mismas los datos biométricos del contratante, pero dado que el cifrado es homomórfico sí que sería posible realizar sobre las mismas las operaciones matemáticas necesarias para la identificación del usuario.

-**Sexo** (Booleano)

-**Estado civil** (Número entero). A nuestro juicio, bastaría con un simple *nibble* (unidad de información de 4 bits) para codificar numéricamente el estado civil del contratante (de este modo, el número 0 simbolizaría el estado civil de soltero, el número 1 el de casado, y así sucesivamente).

-**Edad** (Número entero).

-**Intervención en nombre propio** (booleano). Esta variable tomaría el valor 1 si el contratante interviniese en nombre propio, y 0 si lo hace en nombre ajeno. En este último caso, el documento debería incluir un poder cibernético, una suerte de poder especial en cuya virtud una determinada persona física/jurídica confía a otra la gestión de una o varias cuentas dentro de una dirección de *blockchain*.

b)Fecha y hora de celebración del negocio jurídico

La fecha y la hora de celebración de los negocios jurídicos se determina con ayuda de un sello de tiempo, que contiene la fecha y la hora (correspondiente al huso horario del meridiano de Greenwich, UTC) en que ha tenido lugar la perfección del mismo.

Hasta la aparición de las cadenas de bloques, los sellos de tiempo eran expedidos por instancias centralizadas, las autoridades de sellado de tiempo (TSA), cuyo funcionamiento estaba regulado en el plano técnico por el documento RFC 3161, y en el jurídico por el Reglamento europeo eIDAS, que analizaremos pormenorizadamente en la próxima sección.

La nueva tecnología *blockchain*, y particularmente las funciones-resumen criptográficas (*hashes*) empleadas en ella, han permitido el surgimiento de ***sellos de tiempo descentralizados***, que no requieren de la intervención de ninguna instancia centralizada. Estos sellos fijan los términos *ante quem* y *post quem* de los negocios jurídicos:

- El **término *post quem*** es aquel momento de tiempo en el que, como muy temprano, ha debido de haberse perfeccionado el negocio jurídico. Dicho término se fija mediante la incorporación al documento del *hash* de un bloque de la cadena. La fecha de dicho bloque funciona como **término *post quem***.

- El **término *ante quem*** es aquel punto del tiempo antes del cual hubo de tener lugar - necesariamente- la perfección del negocio jurídico. Una vez que el documento electrónico se ha incorporado a la cadena, el último bloque de esta última sirve como **término *ante quem***.

c) Lugar a cuya *lex loci* se somete el negocio jurídico

A diferencia de lo que sucede con los sellos de tiempo, a nuestro juicio aún no ha surgido un mecanismo claro de *prueba de localización,* que permita determinar, de una manera indubitada, en qué lugar concreto han emitido su declaración de voluntad los intervinientes en un negocio jurídico. Una solución podría ser proceder al archivo -dentro del documento electrónico- de cuatro (como mínimo) señales de satélites GPS, que permitan calcular las coordenadas de latitud y longitud del dispositivo. Sin embargo, las señales GPS pueden ser debilitadas o anuladas mediante inhibidores de

frecuencias (*jamming*) y tras ello ser objeto de falsificación (*spoofing*) por actores maliciosos, tal y como han demostrado los secuestros y pirateos de drones guiados por sistemas de geolocalización producidos en los últimos años[7].

Por todo ello, recomendamos prescindir de la inclusión en el documento de cualquier mención al lugar donde estén situadas las partes. En su lugar, **el documento electrónico debería señalar el lugar a cuya legislación se somete el negocio jurídico contenido en el mismo**. El artículo 3.1 del Reglamento de la Unión Europea 593/2008, de 17 de Junio, sobre la Ley aplicable a las Obligaciones Contractuales (Roma I) permite a las partes, en general, elegir la ley aplicable a la totalidad del contrato, o a partes del mismo. En el sistema que proponemos, la localización del contrato se realizaría mediante sendas coordenadas de latitud y de longitud, acordadas por los propios contratantes y expresadas en sendas cadenas de bytes. Los nodos encargados de verificar la validez del negocio jurídico codificado en el documento, comprobarán que dichas coordenadas se corresponden efectivamente con un punto localizable en el territorio de un determinado país, y no en aguas internacionales.

7.2.1.2.Parte dispositiva

La parte dispositiva del documento es aquella sección en la que se recoge el contenido del negocio o del acto que las partes han firmado. Este contenido puede ser de lo más heterogéneo: puede consistir en las cláusulas de un contrato ordinario al que las partes quieren dar publicidad y sellar temporalmente por vía electrónica. Puede consistir también en una simple orden de pago o bien en el código de un contrato inteligente, dependiendo de la configuración de la *blockchain* de que se trate.

7.2.2. Firmas

Los datos de la firma electrónica de cada participante se calcularán conforme a lo dispuesto en su certificado electrónico X.509.

La sección se estructurará como un arreglo (*array*) de datos, que tendrá tantos elementos como firmantes haya en el negocio jurídico.

7.2.3. Sello de tiempo

Fija el término *ante quem* y se compone de dos variables:

-Número de bloque al que se incorpora el negocio jurídico.

El sello de tiempo no se incorpora a la *blockchain*, sino tan sólo a las certificaciones electrónicas expedidas por los nodos de la misma, que dan fe criptográfica de la identidad de los contratantes, del contenido del negocio y de la fecha y la hora en el que tuvieron lugar las declaraciones de voluntad.

7.3.Requisitos formales de serialización de los documentos electrónicos

Proponemos que los documentos electrónicos se representen mediante el sistema de notación ASN.1 (*Abstract Syntax Notation One*), utilizado también para la codificación de los certificados X.509. En terminología informática, se llama *serialización* a aquel procedimiento en cuya virtud una estructura de datos (p.e., un archivo gráfico, un documento, etc...) es transformada en una cadena, en una "serie", de bytes con el objeto de permitir su almacenamiento. Desde un punto de vista jurídico, es indiferente

que se use un sistema u otro. Sin embargo, a nuestro juicio, el sistema ASN.1 tiene una doble ventaja desde un punto de vista técnico:

-Puede ser convertido con facilidad a formato XML o JSON, que a su vez pueden ser manejados con facilidad por los navegadores o por los editores de texto.

8.Propuesta de un registro descentralizado de documentos privados electrónicos, con efectos legitimadores

8.1.Efectos jurídicos de los documentos electrónicos

A nuestro juicio, para que los negocios documentados en el plano meramente cibernético puedan producir efectos jurídicos –efectos en el ámbito del derecho y de los tribunales de justicia- es necesario proceder a la **plena identificación de las partes intervinientes en los mismos**. En Derecho Civil no son posibles los derechos sin sujeto. Hay autores que defienden lo contrario y ponen como ejemplo los títulos cambiarios al portador abandonados (p.e. cheques); pero en mi opinión ello se trata tan sólo de un supuesto de indeterminación transitoria del sujeto. **El estándar de documento electrónico que proponemos en este trabajo identifica plenamente a las partes intervinientes, legitima sus firmas y dota con ello de plena eficacia al negocio, al menos con el valor de un documento privado**. Así lo reconocen la legislación europea y la estadounidense, como veremos.

Si las partes de un negocio jurídico documentado electrónicamente se identifican utilizando los medios expuestos en la próxima sección (*autenticación de doble factor* y *firma electrónica avanzada*), y si los datos de firma electrónica y de sello de tiempo descentralizado son correctos, entonces la parte dispositiva del documento electrónico tendrá fuerza de ley entre las mismas, en los términos de los artículos 1091 y 1262 del Código Civil español.

8.2.El surgimiento de un nuevo modelo de legitimación de firmas.

Tradicionalmente, la doctrina ha venido distinguiendo entre *public notaries* del Common Law y notarios de Derecho Civil continental. Los primeros se limitan a identificar a los contratantes así como garantizar la autenticidad de sus firmas, pero sin realizar ningún juicio acerca de la legalidad del contenido del negocio jurídico que se va a celebrar. En el caso del notariado de tipo continental -que es el que existe en los ordenamientos basados en el Derecho Común de origen romano-canónico- el notario TAMBIÉN ha de comprobar la legalidad, la veracidad y la integridad del documento, que a partir de su autorización pasa a ser un título de carácter ejecutivo.

El simple acto por el cual el notario se limita a comprobar la identidad de los contratantes y la autenticidad de sus firmas (pero no la legalidad del documento) se denomina ***legitimación de firmas***, y en España está regulado por los artículos 255 y siguientes del Reglamento Notarial. Tal y como señala el artículo 256 de este texto legal *el notario no asumirá la responsabilidad por el contenido del documento cuyas firmas legitime*.

A nuestro juicio, los recientes desarrollos en identificación biométrica y tecnología de cadena de bloques, así como las reformas legislativas que han tenido lugar en la Unión Europa y en Estados Unidos en estas dos últimas décadas, han creado un ***nuevo modelo de legitimación criptográfica de firmas***, alternativo al modelo de legitimación notarial.

En el marco de la legislación estadounidense, la regulación de esta materia está contenida en dos grandes textos legales:

-**La *Uniform Electronic Transactions Act* (*UETA*)**, de carácter estatal y que ha sido adoptada por cuarenta y siete Estados de la Unión. Dado que Estados Unidos es un país fuertemente federalizado, a menudo las competencias legislativas en múltiples áreas están en manos de los Estados y se hace necesario proceder a la armonización de sus legislaciones. Esta armonización se lleva a cabo a través de "leyes uniformes" *(uniform acts*), redactadas por la Conferencia Nacional de Comisarios en Leyes Estatales Uniformes (*National Conference of Commissioners on Uniform State Laws*), y que progresivamente son aprobadas por las asambleas legislativas de los Estados.

-**La *Electronic Signatures in Global and Commerce Act* (*ESIGN*)**, de carácter federal, que entró en vigor el 30 de Junio de 2000, aprobada en virtud de lo dispuesto en el artículo 1 de la Constitución de los Estados Unidos de América, que atribuye al Congreso la facultad de regular el comercio interestatal. De particular importancia es su Sección 101, cuyo apartado (a) establece que:

> *sin perjuicio de lo que disponga cualquier estatuto, regulación o disposición legal (diferentes de este título y del título II) con respecto a cualquier transacción que afecte al comercio interestatal o con el extranjero, (1)* ***no puede denegarse efecto legal, validez o ejecutividad a una firma, contrato o cualquier otro registro relativo a tal transacción por el mero hecho de que esté en forma electrónica****; (2) no se puede negar efecto, validez o ejecutividad a un contrato relacionado con tal transacción por el mero hecho de que una firma electrónica fue usado en su formación*[8].

Dentro de la Unión Europea, gozan de particular importancia el **Reglamento europeo 910/2014** (referido a menudo como ***Reglamento eIDAS***), que regula aspectos relativos a la firma electrónica, los terceros de confianza y los sellos de tiempo, y la **Directiva europea 2015/2366** sobre Servicios de Pago (conocida como ***Directiva PS2*****),** que reviste un amplio interés por su tratamiento de la liquidación y el cumplimiento de las obligaciones pecuniarias.

El **Reglamento eIDAS**, en su artículo 3, define **tres tipos de firma electrónica diferentes**:

-Firma electrónica simple, definida como aquellos *datos en formato electrónico anejos a otros datos electrónicos o asociados de manera lógica con ellos que utiliza el firmante para firmar*.

-Firma electrónica avanzada *o firma electrónica que cumple los requisitos contemplados en el artículo 26*.

-Firma electrónica cualificada *o una firma electrónica avanzada que se crea mediante un dispositivo cualificado de creación de firmas electrónicas y que se basa en un certificado cualificado de firma electrónica*.

El **artículo 25** del mismo reglamento reconoce **plena validez jurídica** al tercero de los tipos citados -al de las **firmas electrónicas cualificadas**- en términos muy parecidos a la legislación estadounidense:

> *1. No se denegarán efectos jurídicos ni admisibilidad como prueba en procedimientos judiciales a una firma electrónica por el mero hecho de ser una firma electrónica o porque no cumpla los requisitos de la firma electrónica cualificada.* 2.***Una firma electrónica cualificada tendrá un efecto jurídico equivalente al de una firma manuscrita****.*

> 3. *Una firma electrónica cualificada basada en un certificado cualificado emitido en un Estado miembro será reconocida como una firma electrónica cualificada en todos los demás Estados miembros.*

El segundo de los textos legales al que nos referimos, la **Directiva europea 2015/2366, sobre Servicios de Pago (*Directiva PS2*)**, define, en su artículo 4, a la ***autenticación reforzada*** como

> *la autenticación basada en la utilización de dos o más elementos categorizados como conocimiento (algo que solo conoce el usuario), posesión (algo que solo posee el usuario) e inherencia (algo que es el usuario), que son independientes —es decir, que la vulneración de uno no compromete la fiabilidad de los demás—, y concebida de manera que se proteja la confidencialidad de los datos de autenticación*.

Este precepto impone un esquema de **autenticación denominado *de doble factor* (2FA)**, en cuya virtud, para que un pago sea válido, el usuario debe identificarse utilizando al menos dos de los elementos categorizados como **inherencia** (una característica propia del mismo), **posesión** (algo que sólo posee un usuario por ejemplo, un dispositivo) y **conocimiento**.

El modelo de documento electrónico que proponemos en este trabajo configura una autenticación de doble factor, pues incorpora una referencia a los datos biométricos de los contratantes (característica de *inherencia*), así como un certificado X.509 perteneciente a cada uno de los mismos (característica de *posesión*). La presencia de este último certificado asegura asimismo que la firma electrónica de los contratantes tenga el mismo valor que su firma manuscrita, en los términos del ya citado artículo 25.2 del Reglamento eIDAS.

8.3. Un nuevo registro estatal de documentos electrónicos

Dentro de la Unión Europea, la regulación de los efectos jurídicos de los negocios documentados en *protocolos distribuidos* (de los que *blockchain* es una variante) es aún bastante incompleta y fragmentaria. En Italia, el artículo 8-ter de la reciente *Legge 11 de Febraio 2019 n. 12,*[9] define las nociones de *protocolo distribuido* y *smart contracts*, y declara que estos últimos tienen el mismo efecto jurídico que el de un contrato con simple forma escrita siempre y cuando reúnan los requisitos técnicos exigidos por la *Agenzia per l'Italia digitale*. Igualmente, el apartado tercero de este mismo precepto concede a los asientos electrónicos de los protocolos distribuidos un efecto similar al del artículo 1227 del Código Civil español.

Nosotros, en este trabajo, recomendamos la creación por parte del Estado Español de un registro de documentos privados electrónicos que funcionaría mediante *tecnología de protocolo distribuido* (tecnología de la que *blockchain* es una simple variante), y cuyas características principales serían las siguientes:

a) La *titularidad* de este registro será *pública* por razones de seguridad nacional: Los nodos de la red pertenecerán a instituciones públicas españolas y el contenido del *protocolo distribuido* será declarado legalmente de propiedad estatal. Si permitimos que la red sea abierta y que su protocolo funcione mediante prueba de trabajo (al estilo del Bitcoin o de las primeras versiones de Ethereum), corremos el riesgo de que cualquier agente exterior con suficiente poder computacional pueda hacerse con el control de toda la red. Esto es lo que está sucediendo en la actualidad (verano de 2019) con la red de Bitcoin, cuyo *poder de hash* está controlado en un 70 por ciento por nodos situados en la República Popular China, particularmente de la

provincia de Cantón.[10] A mi juicio, sólo una red cerrada puede garantizar la seguridad del tráfico jurídico español, y asegurar que éste no pueda ser amenazado por agentes situados en el exterior.

b) Los documentos privados sometidos a inscripción tendrán un *contenido estandarizado*. En la sección anterior hemos realizado una propuesta estándar de documento electrónico que cumple plenamente con los requisitos establecidos en el Reglamento eIDAS y la Directiva PS2.

c) Los *efectos sustantivos* de las inscripciones serán los de legitimar criptográficamente las firmas de los negocios jurídicos, identificar a las partes intervinientes, determinar la ley aplicable a su contenido y dar por cierta su fecha frente a terceros (sello descentralizado de tiempo).

d) El registro podría configurarse para dar publicidad formal (aunque no material) *erga omnes* a los negocios jurídicos archivados en el mismo, como sucede en la actualidad en las *blockchains* de Bitcoin y de Ethereum (cuyos contenidos pueden ser escaneados y consultados libremente con ayuda de aplicaciones web diseñadas a tal efecto) o en los Registros de la Propiedad de España (cuyos libros son declarados públicos por el artículo 221 de la Ley Hipotecaria española). Sin embargo, el registro que proponemos podría ser también programado para que el contenido de los negocios jurídicos archivados en el mismo sólo sea accesible a aquellos que tengan en su posesión determinadas claves criptográficas, como sucede en el protocolo Monero, cuyas transacciones quedan ocultas al público debido a un fenómeno denominado *ofuscación de la blockchain* (*blockchain obfuscation*). Este último sistema se asemejaría más al funcionamiento del protocolo notarial en España, cuyo contenido es declarado secreto por el artículo 274 del Reglamento Notarial español.

e) Se concederá *carácter ejecutivo* a los documentos inscritos que reconozcan obligaciones pecuniarias para cuya liquidación sea tan sólo necesaria la práctica de simples operaciones aritméticas.

Se dice que un título lleva aparejada ejecución cuando las obligaciones de naturaleza pecuniaria recogidas en sus cláusulas son directamente ejecutables por el acreedor sin necesidad de que éste deba incoar un juicio declarativo previo. El origen del carácter ejecutivo de los documentos públicos se halla en las denominadas *cláusulas guarentigias* desarrolladas en el norte de Italia durante la Edad Media, en cuya virtud el deudor autorizaba al acreedor a ejecutar directamente su crédito impagado sobre los bienes del primero. Más tarde, a lo largo del siglo XIV los tribunales consideraron que las *cláusulas guarentigias* estaban sobreentendidas en todo tipo de documentos notariales, algo que dentro de la corona de Castilla tuvo expresa sanción legal mediante la Ley Toledana de 1398. En la actualidad, el carácter ejecutivo de las escrituras públicas aparece sancionado por el artículo 517 de la Ley de Enjuiciamiento Civil española.

A nuestro juicio, no deberían existir excesivos reparos por parte del legislador a la hora de atribuir carácter ejecutivo a los títulos electrónicos incorporados al registro de documentos cuya creación proponemos. De hecho, la Ley de Enjuiciamiento Civil reconoce en su artículo 517.2 carácter ejecutivo a los laudos arbitrales, que desde el año 2012 no necesitan ser protocolizados notarialmente, y que pueden ser codificados en cualquier forma, incluida la electrónica (*Todo laudo deberá constar por escrito (...) se entenderá que el laudo consta por escrito cuando de su contenido y firmas quede constancia y sean accesibles para su ulterior consulta en soporte electrónico, óptico o de otro tipo*[11]).

Podría pensarse que la tecnología *blockchain* no garantiza ni la capacidad de las partes para contratar ni la legalidad de las cláusulas del negocio jurídico. Sin embargo, de acuerdo con la jurisprudencia del Tribunal Supremo español, ***la capacidad de las personas se presume siempre****, mientras que su incapacidad debe ser probada de un modo evidente y completo* (STS 3 de Febrero de 1952). La presunción *iuris tantum* de capacidad sólo puede destruirse mediante una prueba en contrario *muy cumplida y convincente* (STS 10 de Abril de 1944) y *de fuerza inequívoca* (STS 20 de Febrero 1975). Por otra parte, el juicio de capacidad que el Notario realiza antes de autorizar un documento no deja de ser un simple reforzamiento de esta presunción *iuris tantum* de capacidad. No es, en modo alguno, una presunción *iuris et de iure*[12]. De este modo, la STS 20/2015, de 22 de enero de 2015 establece que *"la afirmación del Notario acerca de la capacidad del testador puede ser destruida por ulteriores pruebas que demuestren que el otorgante no estaba en pleno uso de sus facultades*.

Por lo que se refiere al **control de legalidad del contenido de los negocios jurídicos**, cabe señalar que a lo largo de los últimos siglos los fedatarios públicos han venido realizando una invaluable labor de supervisión de la legalidad del tráfico jurídico. La frase "notaría abierta, juzgado cerrado", acuñada por el notario español Joaquín Costa a finales del siglo XIX, expresaba el hecho de que la supervisión de las cláusulas de los negocios jurídicos por parte de los notarios -antes de autorizar escrituras públicas- reducía la litigiosidad y coadyuvaba a la descongestión de los tribunales de justicia. Sin embargo, en nuestra opinión, **los recientes desarrollos legislativos en el ámbito del Derecho Europeo están lentamente haciendo desplazar este control de legalidad desde el notario hacia la figura del juez**, particularmente en los procedimientos ejecutivos. Así, múltiples Sentencias del Tribunal de Justicia de la Unión Europea -entre ellas las del caso Banesto, el asunto Brusse o el caso Banco Primus- imponen al juez encargado de tramitar una demanda ejecutiva contra un consumidor la obligación de controlar **de oficio** el carácter abusivo de las cláusulas contractuales. El Tribunal de Luxemburgo, en su sentencia de 30 de Mayo de 2013 (asunto C-488/11) establece que

> *la Directiva 93/13 debe interpretarse en el sentido de que [...] cuando el juez nacional que conoce de una demanda formulada por un profesional contra un consumidor acerca de la ejecución de un contrato esté facultado, según las normas procesales internas, para examinar de oficio la disconformidad entre la cláusula en la que se fundamenta la demanda y las normas nacionales de orden público, deberá apreciar de oficio de igual manera, una vez haya determinado que dicha cláusula entra en el ámbito de aplicación de esa Directiva, el carácter abusivo en su caso de esa cláusula a la luz de los criterios enunciados en la Directiva*.

Para adecuar la legislación española a la Sentencia del Tribunal de Justicia de la Unión Europea de 14 de Marzo de 2013, el legislador español modificó, por medio de la **Ley de 14 de Mayo de 2013**, el artículo 552 de la Ley de Enjuiciamiento Civil, cuyo párrafo segundo establece que el *tribunal examinará de oficio si alguna de las cláusulas incluidas en un título ejecutivo de los citados en el artículo 557.1 puede ser calificada como abusiva*. A nuestro juicio, **esta reforma legal alteró profundamente el esquema de seguridad jurídica preventiva existente en nuestro ordenamiento jurídico**: En la actualidad, además del control de legalidad que pueda realizar el Notario antes de autorizar cualquier documento crediticio, la Ley de Enjuiciamiento Civil impone al Juez la obligación de realizar un nuevo control a la hora de examinar las demandas ejecutivas a las que se refiere el artículo 549 y sus documentos complementarios.

Las cláusulas abusivas son consideradas ilegales por la legislación de la Unión Europea y por el Tribunal de Luxemburgo, y por ello **la supervisión de los títulos que el juez realiza al inicio de cada procedimiento ejecutivo tiene la naturaleza jurídica de un control de legalidad, aunque limitado**. Proponemos una modificación de la Ley de Enjuiciamiento Civil para que el control de legalidad del

juez se extienda, no sólo al carácter abusivo de las cláusulas de un negocio jurídico con forma electrónica, sino también a todo tipo de circunstancias del mismo que puedan contravenir la ley, la moral o el orden público.

Conclusiones

A medida que avanza el siglo XXI, la carrera tecnológica entre las diferentes potencias planetarias se recrudece. Las autoridades de la República Popular China han elaborado una estrategia tecnológica denominada *Made in China 2025*, con el propósito de convertir a este país en una potencia tecnológica puntera en múltiples sectores como la robótica, la inteligencia artificial, la domótica o el aprendizaje de máquinas. Dentro de dicha estrategia, el desarrollo de la tecnología de cadena de bloques (*blockchain*) jugará un papel fundamental, tal y como expuso Xi Jinping en un discurso suyo pronunciado el 14 Mayo de 2018 ante la Academia de Ciencias China. [13] No en vano, *blockchain* es el término más buscado en el motor de búsqueda Baidu,[14] y las autoridades del Banco Central chino han diseñado un esquema para emitir papel timbrado electrónico[15] y para validar títulos cambiarios utilizando para ello contratos inteligentes.[16]

Es esencial que España no quede atrás en esta carrera tecnológica, y por ese motivo, recomendamos encarecidamente a los diferentes grupos del Congreso de los Diputados que promuevan la creación en nuestro país de un registro de documentos privados electrónicos. Dicho registro sería de titularidad pública, funcionaría mediante tecnología de *protocolo distribuido*, y entre sus funciones se encontrarían la de legitimar las firmas de los documentos inscritos, identificar a las partes intervinientes, generar sellos de tiempo, y determinar la ley aplicable al contenido de los mismos. Consideramos que una iniciativa de estas características puede proporcionar a España una extraordinaria ventaja competitiva en el desarrollo de la tecnología de protocolo distribuido respecto a sus vecinos europeos.

[1] "Ethereum es Turing-completo, ¿y eso qué es?". [Accedido el 26 de Agosto de 2019] https://www.eleconomista.es/economia/noticias/8817210/12/17/Ethereum-es-Turing-completo-y-eso-que-es.html

[2] "Finding The Greedy, Prodigal, and Suicidal Contracts at Scale" [Accedido el 26 de Agosto de 2019] https://arxiv.org/pdf/1802.06038.pdf?_gclid=5af13bbb734704.73471170-5af13bbb734778.12658421&_utm_source=xakep&_utm_campaign=mention157476&_utm_medium=inline&_utm_content=lnk396338746320
(En este trabajo se realiza una descripción de los "contratos tacaños" -"greedy contracts"- presentes en Ethereum que, por un error de diseño, bloquean indefinidamente los fondos almacenados en los mismos)

[3] La "máquina virtual" es una suerte de ordenador simulado por cada nodo del protocolo que ejecuta e interpreta los contratos inteligentes. Las instrucciones que interpreta esta máquina, y que constituyen el código del contrato inteligente, se denominan con el término inglés *opcodes*.

[4] El Banco Central de China desarrolla un sistema respaldado por blockchain para digitalizar los cheques de papel. [Accedido el 27 de Mayo de 2019]

https://es.cointelegraph.com/news/chinese-central-bank- develops-blockchain-system-to-digitize-paper-checks nota 12

[5] Diagrama extraído de Wikimedia Commons.

[6] "El Blockchain va a reemplazar a los notarios". [Accedido el 26 de Agosto de 2019] https://www.media-tics.com/noticia/6715/internet/el-blockchain-va-a-reemplazar-a-los-notarios.html

[7]Euronews. Irán se niega a devolver el avión teledirigido a EEUU. [Accedido el 27 de Mayo de 2019] https://es.euronews.com/2011/12/13/iran-se-niega-a-devolver-el-avion-teledirigido-a-eeuu

[8] *SEC. 101. GENERAL RULE OF VALIDITY.*
(a) IN GENERAL.—Notwithstanding any statute, regulation, or other rule of law (other than this title and title II), with respect to any transaction in or affecting interstate or foreign commerce—
(1) a signature, contract, or other record relating to such transaction may not be denied legal effect, validity, or enforceability solely because it is in electronic form; and
(2) a contract relating to such transaction may not be denied legal effect, validity, or enforceability solely because an electronic signature or electronic record was used in its formation.

[9] Gazzetta Ufficiale della Repubblica Italiana. Roma – Martedì, 12 febbraio 2019.[Accedido el 26 de Agosto de 2019]
https://www..gazzettaufficiale.it/eli/gu/2019/02/12/36/sg/pdf

[10] Los mineros de Bitcoin comienzan a mudarse de China a Estados Unidos [Accedido el 26 de Agosto de 2019]
https://bitcoin.es/actualidad/los-mineros-de-bitcoin-comienzan-a-mudarse-de-china-a-estados-unidos/

[11] Artículo 37 de la Ley de Arbitraje española.

[12] Presunción *iuris et de iure* es aquélla que no admite prueba en contrario. Presunción *iuris tantum* es aquella que sí lo admite

[13] Cointelegraph. El Presidente de China Xi dice que Blockchain es parte de una nueva "revolución tecnológica". [Accedido el 27 de Mayo de 2019]
https://es.cointelegraph.com/news/chinas-president-xi-says-blockchain-part-of-new technological-revolution

[14] Bitcoin.es. Baidu lanza plataforma para desarrollo de aplicaciones blockchain. [Accedido el 27 de Mayo de 2019] https://bitcoin.es/actualidad/baidu-lanza-plataforma-para-desarrollo-de-aplicaciones-blockchain/

[15] Cripto Tendencia. Bitcoin es el término más popular en el buscador chino Baidu. [Accedido el 27 de Mayo de 2019]
https://criptotendencia.com/2019/04/05/bitcoin-es-el-termino-mas-popular-en-el-buscador-chino-baidu/

Bibliografía

ANGIANO, J.M. (2019). "'Smart Contracts'. Introducción al 'contractware'". *Garrigues Opina*, 15 de noviembre. Disponible en http://www.garrigues.com/es_ES/noticia/smart-contracts-introducción-al-contractware (consultado el 26 de Agosto 2019)

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

BRANCÓS, E. (2019). "*Blockchain*, función notarial y registro". *El Notario del siglo XXI*, Julio-Agosto, nº 86. Disponible en http://www.elnotario.es/academia-matritense-del-notariado/7325-blockchain-funcion-notarial-y-registro (consultado el 26 de Agosto 2019)

CARMELO LLOPIS, J. (2018). Blockchain y el sistema de seguridad jurídico preventiva. Disponible en http://www.notariallopis.es/blog/i/1466/73/blockchain-y-el-sistema-de-seguridad-juridica-preventiva (consultado el 26 de Agosto 2019)

DIFFIE, W.; HELLMAN, M. (1976). "New directions in cryptography". *IEEE Transactions on Information Theory*. Noviembre. 22 (6): 644–654.

GONZÁLEZ GRANADO, J. (2016). *Eficacia probatoria de la blockchain. Criptografía y artículo 1227 del Código Civil*. Disponible en https://tallerdederechos.com/eficacia-probatoria-de-la-blockchain-criptografia-y-articulo-1227-del-codigo-civil/ (consultado el 26 de Agosto 2019)

GONZÁLEZ-MENESES ROBLES, M. (2017). *Entender blockchain. Una introducción a la Tecnología de Registro Distribuido*. Navarra: Thomson-Reuters Aranzadi.

IBÁÑEZ JIMÉNEZ, J. W. (Ed.) (2018). *Derecho de blockchain y de la tecnología de registros distribuidos*. Cizur Menor (Navarra): Thomson Reuters Aranzadi.

IBÁÑEZ JIMÉNEZ, J. W. (s.a.). "*Blockchain*, ¿el nuevo notario?", *Everis. An NTT Data Company*, Madrid. Disponible en: http://repositorio.comillas.edu/xmlui/bitstream/handle/11531/14564/Blockchain_el_nuevo_notario.pdf?sequence=1&isAllowed=y (consultado el 26 de Agosto 2019)

KELSEN, H. (2000). *Teoría pura del derecho.* México: Porrúa.

LAMPORT, L.; SHOSTAK, R.; PEASE, M.(s.a.). *The Byzantine generals problem*. Disponible en: https://people.eecs.berkeley.edu/~luca/cs174/byzantine.pdf (consultado el 26 de Agosto 2019)

LESSIG, L. (2001). *El código y otras leyes del ciberespacio*. Madrid: Grupo Santillana de Ediciones.

NAKAMOTO, S.(s.a.). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Disponible en: https://bitcoin.org/bitcoin.pdf (consultado el 26 de Agosto 2019)

NYU SCHOOL OF LAW. (2013). Governing Algorithms. A Conference on Computation, Automation, and Control. New York University. May 16. Disponible en: http://governingalgorithms.org (consultado: 26 de Agosto 2019).

PREUKSCHAT, A. (2017). Blockchain: La revolución industrial de Internet. Barcelona: Gestión 2000.

PREUKSCHAT, A. (2017). *Ethereum es Turing-completo, ¿y eso qué es?* Disponible en: https://www.eleconomista.es/economia/noticias/8817210/12/17/Ethereum-es-Turing-completo-y-eso-que-es.html

RODRIGUEZ ADRADOS, A. (1996). *Documento*. Madrid: Escritos Jurídicos. Vol. III, CGN,, p. 11.

RIVEST, R.; SHAMIR, A.; ADLEMAN, L. A . (s.a.). *Method for Obtaining Digital Signatures and Public-Key Cryptosystems*. Disponible en: https://people.csail.mit.edu/rivest/Rsapaper.pdf (Consultado el 26 de Agosto 2019)

ROMANO, S. (2013). *El ordenamiento jurídico*. Madrid: Centro de Estudios Políticos y Constitucionales.

ROSALES, F. (2017). *Blockchain: ¿tecnología útil para el notariado?*. Disponible en: https://www.notariofranciscorosales.com/uso-blockchain-los-notarios (consultado el 26 de Agosto 2019)

ROSALES, F. (2017). Notarizar con *blockchain*. Disponible en: https://www.notariofranciscorosales.com/notarizar-con-blockchain (consultado el 26 de Agosto 2019)

RUIZ-GALLARDÓN GARCÍA DE LA RASILLA, M. (2018). "Fe pública y *tokenización* de activos en *blockchain*". En GARCÍA MEXÍA, P. (Dir.). *Criptoderecho. La regulación de blockchain*. Madrid: Wolters Kluwer, p. 449-488.

TUR FAÚNDEZ, C. (2018). *Smart Contracts. Análisis jurídico*. Madrid: Reus Editorial.

WERBACH, K.; CORNELL, N. (2017). "Contracts ex machina". En *Duke Law Journal* 67, pág. 320 y nota 26. Disponible en: https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=3913&context=dlj (consultado el 26 de Agosto 2019)

WOOD, G. (s.a.). *Ethereum: A secure decentralised generalised transaction ledger*. Disponible en: https://gavwood.com/paper.pdf (consultado el 26 de Agosto 2019)