derecom

ISSN: 1988-2629. Nº. 29. Nueva Época. Septiembre 2020-Marzo 2021

Cómo citar este texto:

Rodríguez Abril, R. (2020). ¿Puede la tecnología DLT servir de base para la creación de un nuevo ordenamiento cambiario electrónico?, *Derecom*, 29, 75-103. http://www.derecom.com/derecom/

¿PUEDE LA TECNOLOGÍA DLT SERVIR DE BASE PARA LA CREACIÓN DE UN NUEVO ORDENAMIENTO CAMBIARIO ELECTRÓNICO?

COULD THE DISTRIBUTED LEDGER TECHNOLOGY SERVE AS THE BASIS FOR A NEW KIND OF ELECTRONIC NEGOTIABLE INSTRUMENTS?

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

Resumen

El autor de este artículo propone usar la tecnología de protocolo distribuido (DLT) para crear un nuevo ordenamiento cambiario de carácter electrónico, en el que el giro, la transmisión y la presentación al pago de letras de cambio, cheques y pagarés se realizarían mediante transacciones dentro de una *blockchain* privada gobernada por el protocolo de Libra. La creación, modificación y extinción de los títulos-valores se realizarían por contratos inteligentes (módulos) ubicados en la cuenta de la Fábrica Nacional de la Moneda y Timbre (en el caso de las letras de cambio) o en las cuentas de los bancos particulares (en el caso de los cheques). En ningún caso los datos de los títulos-valores estarían a disposición de terceros, sino que su contenido quedaría ocultado mediante diversas técnicas de ofuscación. Aunque, por razones de espacio, se ha analizado fundamentalmente el caso de las letras de cambio, los esquemas presentados en este artículo serían de plena aplicación al conjunto de los títulos-valores y valores negociables.

Summary

The author of this paper proposes to use distributed protocol technology (DLT) to create a new system of electronic negotiable instruments, in which the drawing, transmission and presentation for payment of bills of exchange, cheques and promissory notes would be carried out through transactions within a private blockchain governed by the Libra protocol. The creation, modification and extinction of securities would be carried out by smart contracts (modules) located in the account of the Royal Spanish Mint (in the case of bills of exchange) or

Recibido: 15/04/2020 Revisado: 03/09/2020
Aceptado: 04/09/2020 Publicado:15/09/2020

in the accounts of private banks (in the case of cheques). The securities' data would under no circumstances be made public and avalaible to third parties. Instead, their content would be concealed by means of various obfuscation techniques. Although, for reasons of space, only the case of bills of exchange has been mainly analysed and researched, the schemes presented in this paper would be fully applicable to all securities and negotiable instruments.

Palabras clave: Títulos. Valores cambiarios. Libra. Blockchain. DLT.

Keywords: N*egotiable instruments. Libra. Blockchain. DLT.*

1. Introducción: De los títulos valores a los derechos digitales (*digital assets*)

Los títulos-valores son aquellos documentos que llevan incorporado un derecho de contenido patrimonial, y cuya posesión legitima para el ejercicio de este último. Pueden utilizarse para documentar múltiples fenómenos jurídicos, como los créditos, las acciones, los bonos de deuda pública o las obligaciones emitidas por las sociedades anónimas. En todos estos casos, la característica esencial del título-valor es que el derecho representado se incorpora al propio documento.

Aunque existen precedentes en Cartago y en Babilonia sobre documentación de créditos en trozos de cuero y tablillas de arcilla, el origen del concepto actual de título-valor hemos de situarlo en la Baja Edad Media. En aquel entonces, particularmente en los siglos XIII y XIV, el Derecho Común medieval de origen romano-canónico y desarrollado por las universidades europeas se estaba convirtiendo en la base de los derechos territoriales de los diferentes reinos de Europa Occidental. Sin embargo, sus normas de transmisión de créditos eran extraordinariamente rígidas y formalistas, y no eran capaces de dar satisfacción a las necesidades de la nueva y pujante clase mercantil, que exigía mecanismos que permitieran una ágil circulación de capitales. Por este motivo, a lo largo de la Baja Edad Media, se generalizó en Europa una institución, la letra de cambio, que permitía la incorporación de los créditos a documentos libremente transmisibles entre particulares. En los siglos subsiguientes, este mecanismo de documentación de derechos patrimoniales mediante papel se extendió a supuestos como las acciones de sociedades anónimas, los bonos de deuda pública o el papel moneda emitido por parte de los bancos centrales. Se convirtió en uno de los instrumentos clave en el desarrollo del nuevo capitalismo financiero a lo largo de toda la Edad Moderna.

Sin embargo, como consecuencia de la llegada de la informática y de las bases de datos, en las últimas décadas del siglo XX se produjo una tendencia inversa de *desmaterialización* de los valores negociables y de incorporación de su contenido a registros informáticos, mediante la práctica de asientos denominados "anotaciones en cuenta". De ahora en adelante, la creación y transmisión de valores ya no tendría lugar a través de la redacción y firma de documentos escritos sino a través de la práctica de asientos en una base de datos electrónica.

El siguiente paso en la digitalización de los valores mobiliarios lo constituyó la utilización de la criptografía para permitir la práctica de transferencias electrónicas completamente anónimas, tanto de dinero como de otros derechos incorporales. Aunque la circulación de dinero por vía electrónica comenzó a generalizarse a partir de los años 50 con la aparición de las primeras tarjetas de crédito y la implantación progresiva de bases de datos informatizadas dentro del sector bancario, ya en el año 1983 el criptógrafo estadounidense David Chaum hizo notar que las transferencias monetarias realizadas por vía electrónica carecían del anonimato que caracterizaba a los pagos realizados con dinero físico: en las transferencias electrónicas

estaban perfectamente identificados tanto el transmisor como el adquirente, mientras que para realizar una entrega de dinero físico (billetes de banco) no era necesario identificar ninguna de las partes. Para atribuir al dinero electrónico ese toque de anonimato que caracterizaba al dinero físico, Chaum propuso la utilización de los métodos de criptografía asimétrica que habían sido propuestos en los años 70 por Whitfield Diffie y Martin Hellman y desarrollados e implementados por Ron Rivest, Adi Shamir y Len Adleman en su sistema RSA. En el modelo de Chaum los titulares de derechos de carácter electrónico (p.e. dinero digital) se identificaban por medio de claves públicas, mientras que el poder de disposición sobre los mismos quedaba vinculado a la posesión de las correspondientes claves privadas.

Las ideas de Chaum no lograron implantarse en el comercio digital durante los años 80 y 90, pero sí que inspiraron, varios años más tarde, la creación de la criptomoneda Bitcoin, cuyas transacciones se realizan de un modo completamente anónimo. Aunque la *blockchain* de Bitcoin estaba concebida inicialmente para la transmisión de criptomonedas (y no de otro tipo de derechos), pronto surgió entre su comunidad de usuarios la idea de utilizar *monedas coloreadas* (en inglés americano *colored coins*, conjuntos de *satoshis*[1] identificados unívoca e individualmente por una serie de metadatos) para representar digitalmente valores negociables. A partir de este momento se abrió la posibilidad de practicar anotaciones en cuenta representativas de los valores negociables no sólo en registros centralizados, sino también en bases de datos electrónicas descentralizadas.

En el año 2014 apareció Ethereum, y con él, una segunda generación de *blockchains* dotadas de máquinas virtuales (ordenadores simulados) capaces de ejecutar contratos inteligentes. Fue dentro de Ethereum que se implementó definitivamente la posibilidad de documentar valores negociables a través de *tokens*, expresión inglesa que define a aquellas variables o estructuras de datos cuya creación, transmisión y amortización es controlada por un bloque de código informático, residente en la propia *blockchain*, y denominado *smart contract* (contrato inteligente). Los *tokens* pueden ser de dos tipos: fungibles y no fungibles. Los *tokens* no fungibles son aquellos identificados por características únicas, que los hacen plenamente distinguibles de los demás, y como consecuencia de ello completamente aptos para la representación de objetos como las fincas registrales, tal y como expuse en alguno de mis trabajos anteriores.[2] Los *tokens fungibles*, por el contrario, son aquellos que se identifican por su género, es decir, por características colectivas compartidas con otros de su misma clase. Los *tokens fungibles* están comenzando a ser utilizados para documentar electrónicamente valores mobiliarios, y dentro de Ethereum, están teniendo lugar iniciativas para homogeneizarlos por medio de estándares (como el célebre ERC20) que describen cuáles son las funciones esenciales de las que debe disponer como mínimo el contrato inteligente que emite un *token*, y cuáles son las características básicas que han de tener dichas funciones.

Aunque hay autores que lo cuestionan, en mi opinión, no cabe duda de que los *tokens fungibles* almacenados en las cadenas de bloques reúnen todas las características que la doctrina continental europea atribuye a los títulos-valores, a saber,

-Legitimación: La posesión y presentación del título-valor es condición *sine qua non* para el ejercicio del derecho y su defensa ante los tribunales de justicia. El tenedor de una letra de cambio o de un cheque es el único legitimado para exigir su cobro o para ejercitar una acción cambiaria en caso de impago. Históricamente, legitimación fue la primera característica que se atribuyó al título-valor, y aparece dentro de la primitiva definición que el jurista alemán Heinrich

Brunner ofreció del concepto, describiéndolo como un *documento en el que un derecho de naturaleza privada ha sido titulizado de tal manera que para el ejercicio del derecho es necesaria la posesión del documento.*[3] En el ámbito digital, la legitimación del tenedor del derecho se comprueba mediante mecanismos de criptografía asimétrica y está inseparablemente vinculada la posesión de un par de claves, pública y privada. La clave pública identifica al titular del derecho dentro del espacio criptográfico mientras que una clave privada otorga a su poseedor facultades de disposición sobre el derecho al que está vinculada. En ocasiones, la identificación (y legitimación) del titular de un derecho digital se complementa mediante un *certificado* expedido por una autoridad pública (p.e., la Fábrica Nacional de Moneda y Timbre), que vincula una cierta clave pública a una persona física o jurídica concreta. La presencia de dicho certificado atribuye a la firma digital el mismo valor que una firma manuscrita, en los términos del artículo 25.2 del Reglamento Europeo 910/2014 (Reglamento eIDAS).

-Literalidad: Las facultades del tenedor del título deben estar concisa y detalladamente descritas en el tenor literal del mismo título o en el de la legislación que lo regula. Dentro de las *blockchains*, las características de los *tokens*, y su forma de emisión y transmisión, están reguladas en el código informático vinculado a la cuenta emisora de dichos tokens. Los interesados pueden consultar el contenido de dicho código y comprobar por sí mismos sus características.

-Incorporación: Tras la emisión de un título-valor, el derecho queda incorporado definitivamente al documento, y como consecuencia de ello la transmisión de la posesión de este último conllevará automáticamente el cambio de la titularidad del derecho. La teoría de la incorporación (Verkörperung) fue desarrollada por el jurista alemán Friedrich Karl von Savigny, para el cual el título-valor no se limitaba a representar un derecho, sino que incorporaba al mismo y se identificaba con él. Ha habido cierta renuencia por parte de sectores de la doctrina a la hora de atribuir esta característica a los *tokens*, pero en mi opinión esta renuencia está injustificada por dos razones: en primer lugar, porque ya desde tiempos del jurista romano Gayo se admite la posibilidad de que la propiedad recaiga sobre cosas incorporales, es decir, sobre "cosas que no pueden ser tocadas" (*res quae tangi non possunt*), como sucede en el caso de la propiedad intelectual, cuyo objeto puede venir constituido, no sólo por creaciones materiales y tangibles, sino también por activos digitales (*digital assets*), esto es, por cadenas binarias que representen audio, video o cualquier otra información susceptible de ser codificada digitalmente. Creo que no existe ningún obstáculo técnico o conceptual por el cual un derecho de contenido inmaterial (como un valor o un derecho de crédito) no pueda incorporarse a una base de datos electrónica por medio de una anotación en cuenta, del mismo modo que cuando un deudor y un acreedor libran y aceptan respectivamente una letra de cambio están incorporando con ello el crédito al documento, permitiendo su libre transmisibilidad. A fin de cuentas, el papel no tiene capacidades de representación superiores a las que pueda tener un disco duro o un dispositivo de memoria *flash* y, de hecho, cerca del 90% del dinero en circulación en la Eurozona está representado por simples asientos electrónicos practicados en bases de datos bancarias de carácter informático: el papel moneda se encuentra en franca regresión y la crisis sanitaria y económica provocada por la pandemia del Covid-19 ha acelerado este proceso de decadencia que puede concluir con la definitiva desaparición de la moneda física. En este trabajo defendemos que el *estado de máquina* de una cadena de bloques es tan idóneo para representar y almacenar un derecho de contenido patrimonial como lo puede ser el papel timbrado o los asientos registrales realizados en papel. Por ello proponemos la adopción de medidas legislativas tendentes a reconocer pleno valor jurídico al contenido de las *blockchains*, y, en general, al de las bases de datos electrónicas.

-**Abstracción**: En el momento en que se gira un título-valor, se crea un nuevo vínculo obligatorio *cambiario* de naturaleza abstracta entre el tenedor y el librado, que coexiste con la obligación causal original. La abstracción de la obligación cambiaria implica que el tenedor de buena fe de una letra de cambio tiene derecho a exigir el cumplimiento de la misma al librado, aunque la obligación causal primitiva que dio origen al libramiento de la letra de cambio devenga nula. Así, el artículo 20 de la Ley Cambiaria y del Cheque establece que *el demandado por una acción cambiaria no podrá oponer al tenedor excepciones fundadas en sus relaciones personales con el librador o con los tenedores anteriores, a no ser que el tenedor, al adquirir la letra, haya procedido a sabiendas en perjuicio del deudor*. En el ámbito digital, la transferencia de criptomonedas y de *tokens* tiene también lugar de un modo acausal. Basta con que el poseedor de una clave privada firme válidamente una transacción para que se produzca la transferencia del derecho, con independencia de que el negocio jurídico causal (p.e., una compraventa) que haya motivado esa transacción sea válido o no. Las relaciones jurídicas causales no se incorporan, pues, a los protocolos distribuidos.

A la vista de lo expuesto en los párrafos anteriores, en este trabajo se propone la creación de un nuevo ordenamiento cambiario completamente digitalizado, en el que los valores mobiliarios queden incorporados a una base de datos de carácter electrónico reforzada internamente mediante estructuras criptográficas. Proponemos adoptar el modelo del protocolo de Libra, que incorpora mejoras respecto a otros protocolos anteriores. Ethereum ciertamente supuso un avance tecnológico respecto a Bitcoin. Su cadena de bloques no sólo almacena y ordena transacciones digitales de criptomonedas, sino que también guarda información relativa a cuentas de usuario: se almacena el saldo de la cuenta, el código ejecutable (contrato inteligente) vinculado a la misma, así como todas las variables y estructuras de datos manipuladas por dicho código, entre las que se encuentran los *tokens*.

Sin embargo, tanto Ethereum como otras *blockchains* surgidas en los años inmediatamente posteriores a la aparición del Bitcoin presentaban algunos inconvenientes en su arquitectura, entre los que podemos citar los siguientes:

-En primer lugar, el nodo que pretende ensamblar un nuevo bloque e incorporarlo a la cadena debe resolver previamente una tarea matemática denominada *prueba de trabajo*, para cuya práctica es necesario el despilfarro de múltiples recursos computacionales y energéticos. A modo de ejemplo, en el año 2018, los nodos de la red de Bitcoin consumieron tanta electricidad como toda Dinamarca.[4] Los algoritmos de prueba de trabajo fueron utilizados casi unánimemente en la primera generación de criptomonedas con el objetivo de dificultar *ataques Sybil*[5] y atribuir el poder decisorio al conjunto de nodos que albergase la mayor parte del poder computacional de la red. Sin embargo, muchos proyectos recientes priorizan el ahorro de energía y de recursos computacionales y, por ello, prescinden no sólo de la prueba de trabajo, sino incluso del propio proceso de minado. Para ello se propone abandonar el concepto de *blockchain* abierta y adoptar en su lugar el de *blockchain* cerrada, donde los nodos requieran de permiso previo para participar y donde el ensamblado de bloques corresponda únicamente a nodos señalados dentro de la red.

-Redundancia en la ejecución de los contratos inteligentes. En Ethereum, las transacciones y las funciones de los contratos inteligentes que ellas invocan deben ser ejecutadas paralelamente por todos y cada uno de los nodos de la red. En otros proyectos de *blockchain* más recientes como Hyperledger Fabric, basta con que los contratos se ejecuten

únicamente en ciertos nodos especificados por el propio contrato inteligente y por las normas del protocolo.

-Extraordinaria volatilidad del valor de las criptomonedas, los *tokens* y otros activos digitales. A fin de cuentas, todos ellos no son más que trozos de información codificados en cadenas de unos y ceros almacenados en dispositivos de memoria electromagnética y carecen de valor intrínseco en el mundo físico, a diferencia de lo que sucede con materias primas como el oro, la plata o el petróleo. Esto ha facilitado la formación de burbujas especulativas dentro de los mercados de todos estos activos digitales. Como consecuencia de ello, y para prevenir la volatilidad del valor del dinero electrónico, recientes proyectos pretenden respaldar, con activos de valor intrínseco, la emisión de criptomonedas, estabilizando con ello su valor y previniendo (o dificultando) la realización de operaciones especulativas sobre las mismas. Libra, la *blockchain* impulsada por Facebook, tiene la intención de respaldar la emisión de sus criptomonedas mediante monedas de curso legal (dólar, euro, yen) y títulos de deuda pública,[6] mientras que el Banco Popular de China ha presentado un proyecto para emitir una nueva moneda digital, conocida oficialmente en inglés con las siglas *DCEP* (*Digital Currency Electronic Payment*) y denominada coloquialmente *criptoyuan* por la prensa especializada.[7] Los bancos que utilicen esta criptomoneda estarán obligados a respaldar sus emisiones depositando su equivalente en yuanes en las reservas del Banco Central chino.[8] Por último, el *ecosistema de blockchain* Binance Chain ha anunciado su voluntad de emitir una criptomoneda estable denominada Venus y que estaría vinculada a la libra esterlina.[9]

A mi juicio, desde la publicación del documento blanco de Satoshi Nakamoto en el año 2008, la evolución de las criptomonedas se ha estructurado en tres generaciones diferentes:

-La primera generación, liderada por Bitcoin, está basada *blockchains* abiertas, que funcionan mediante algoritmos de prueba de trabajo, y que se limitan a ensamblar las transacciones en bloques y a enlazar a estos últimos en una única cadena. Cada transacción contiene una referencia (un *hash*) a la transferencia anterior de la que trae causa, estableciendo una suerte de "*tracto sucesivo criptográfico*" entre ellas.

-La segunda generación, a la que pertenecen Ethereum e Hyperledger Fabric, reside en *blockchains* dotadas de un simulador capaz de ejecutar contratos inteligentes.[10] Estos contratos permiten la emisión, transmisión y amortización de *tokens*, una institución apta para representar objetos tan heterogéneos como las fincas registrales o las acciones de las sociedades anónimas. Algunas de estas *blockchains*, como *Hyperledger Fabric*, han abandonado el algoritmo de prueba de trabajo, e incluso el minado, y ya no requieren que los contratos inteligentes sean ejecutados por todos y cada uno de los nodos de la red. En otras redes como Ethereum, la información se estructura no sólo por transacciones, sino también por cuentas de usuario.

-Por último, en los *ecosistemas* pertenecientes a la tercera generación (Libra, DCEP) se abandonan algunos paradigmas de las generaciones anteriores (como por ejemplo, el de la descentralización, en el caso del criptoyuan chino[11]), mientras que se retiene el elemento criptológico, para garantizar de este modo que el dinero digital tenga el mismo nivel de anonimato que caracteriza al dinero físico. Además, característica esencial de las criptomonedas de este tercer nivel es que tienen un *valor intrínseco, dado que su* emisión está respaldada por activos.

Como vemos, en el momento en que se escribe este artículo (Abril de 2020), la tecnología está lo suficientemente madura como para implementar con garantías un sistema electrónico de transmisión, no sólo de dinero, sino también de títulos-valores y valores mobiliarios. Por ello, a lo largo de este trabajo plantearemos la construcción de un nuevo

ordenamiento cambiario basado en los principios de una de las criptomonedas de la tercera generación: Libra.

2.Libra: una *blockchain* que permite emitir activos digitales respaldados por activos físicos

Al igual que sucede con Ethereum, dentro de Libra la información se estructura en cuentas y transacciones:

2.1 Cuentas

Las **cuentas** se identifican por su *dirección*, derivada de una *clave pública*. Cada vez que un usuario pretende crear una nueva cuenta, debe previamente generar, mediante un algoritmo de criptografía asimétrica, un par de claves, privada y pública. La dirección se calcula haciendo un *hash* a la clave pública. La cuenta es creada cuando se envía por vez primera una transacción a dicha dirección.

La información almacenada en cada cuenta se ordena en *módulos* y *recursos*. Los módulos (*modules*) son el equivalente en Libra de los contratos inteligentes (*smart contracts*) de Ethereum: en ambos casos se trata de piezas de código que controlan los cambios del estado de máquina individual de cada cuenta y, por lo tanto, regulan la modificación de los derechos y deberes individuales registrados en ésta. Los *recursos* (*resources*), por su parte, son variables utilizadas para representar derechos dentro de la base de datos: son el equivalente de las criptomonedas y de los *tokens* existentes en otras *blockchains*, y desde mi punto de vista, son plenamente aptos para documentar electrónicamente derechos incorporales de naturaleza fungible, como los títulos-valores o valores negociables. La emisión y la amortización de *recursos* se realizan por los módulos de cada cuenta.

Fig.1 Comparación entre los protocolos de Libra, Ethereum y Bitcoin

Libra	Ethereum	Bitcoin
recursos *módulos*	*tokens, criptomonedas* *contratos inteligentes*	*monedas coloreadas, criptomonedas* *scripts*

Fuente: Elaboración propia

Del mismo modo que hay diversas clases de *tokens* y de criptomonedas, dentro de Libra también pueden definirse diferentes *tipos de recursos*. La sintaxis de cada uno de estos últimos es la siguiente:

direccion_cuenta.contrato_inteligente.recurso

El tipo de recurso se identifica por tres variables, separadas entre sí por puntos. La primera corresponde a la dirección de la cuenta competente para emitir o amortizar el recurso. La segunda, al contrato inteligente encargado de realizar dichas operaciones. Y, por último, la tercera es el nombre del recurso en concreto.

Por ejemplo, si quisiéramos crear un *tipo de recurso* (en este caso, un título-valor) llamado *bono_rojo,* con cargo a un contrato inteligente denominado *emisor*, situado en la cuenta con dirección *0x45*, su sintaxis sería la siguiente:

0x45.emisor.bono_rojo

Una vez que el recurso ha sido emitido, puede ser transmitido y almacenado a través de todas las cuentas de la *blockchain*. Dentro de cada una de ellas, el recurso tiene la siguiente sintaxis:

direccion_cuenta/*resources*/tipo_de_recurso

De este modo, un título valor de nombre *bono_rojo*, emitido por el contrato inteligente de la cuenta *0x45* de nombre *emisor*, y que está en posesión de la cuenta 0x25 se expresa mediante la siguiente cadena:

0x25/resources/0x45.emisor.bono_rojo

Un principio esencial de la *blockchain* de Libra es que los recursos sólo pueden ser amortizados por la misma cuenta que los ha emitido. Fuera de dicha cuenta se impone una suerte de *principio de conservación de los recursos*, en cuya virtud los recursos pueden ser transmitidos, pero nunca creados (emitidos) o destruidos (amortizados).

A modo de ejemplo, supongamos que el usuario que controla la cuenta *0x43* pretendiera crear una nueva criptomoneda denominada *elektron*, a través de un módulo (contrato inteligente) denominado *Emisor*. El nombre completo de la criptomoneda sería *0x43.Emisor.elektron*. Después de varias transferencias entre cuentas, los saldos de estas últimas serían los siguientes:

Fig. 2: Distribución del recurso 0x43.Emisor.elektron en cuatro cuentas diferentes

Dirección de cuenta	Recurso	Cantidad
0x25	0x43.Emisor.elektron	25
0x43	0x43.Emisor.elektron	200
0x76	0x43.Emisor.elektron	175
0x93	0x43.Emisor.elektron	135

Fuente: Elaboración propia

Sólo la cuenta *0x43* (en verde) puede crear de la nada y/o destruir el recurso señalado. El resto de las cuentas (en negro) únicamente pueden transmitirse el recurso entre ellas (si tienen suficiente saldo), pero no emitirlo o amortizarlo, pues ello sólo corresponde a la cuenta *0x43*.

2.2 Transaccciones

Junto con las cuentas (y sus recursos y módulos asociados), las **transacciones** ocupan un papel prominente en el protocolo de Libra. Son el único mecanismo existente para modificar el estado de máquina de la *blockchain* y, por lo tanto, para modificar los derechos de contenido patrimonial incorporados a la misma. Cabe señalar que a diferencia de lo que sucede en los protocolos de Bitcoin y Ethereum, en Libra el estado de máquina de la cadena no se actualiza bloque a bloque, sino transacción por transacción.[12] Las transacciones se configuran como mensajes enviados de una cuenta a otra en los que deben de constar, entre otros, los siguientes campos:

-Dirección del remitente y del destinatario.

-Clave pública correspondiente a la clave privada del remitente.

-Programa: código informático que debe ser ejecutado por la máquina virtual, acompañado de sus parámetros de entrada y, opcionalmente, del código de nuevos módulos (contratos inteligentes) destinados a ser publicados.

Los programas informáticos ejecutados con cada transacción se escriben en un lenguaje específico denominado Move IR, y en ellos pueden incluirse funciones para retirar fondos de una determinada cuenta (p.e., procedimiento *withdraw_from_sender*) y asignarlos a la cuenta destinataria (p.e., procedimiento *deposit*). Las transacciones pueden ser utilizadas para transferir fondos de una cuenta a otra, pero también para otros menesteres.

Una vez que la transacción se ejecuta, en la *blockchain* se publican los *eventos* relacionados con la ejecución y resultado de la ejecución, entre ellos, un booleano que describe si dicha transacción ha sido exitosa o no.

3.Esquema del nuevo modelo de ordenamiento cambiario electrónico

En este trabajo, proponemos la construcción de un nuevo ordenamiento cambiario completamente digitalizado que desplegaría sus efectos dentro de una *blockchain* privada, gobernada por el protocolo Libra Core. En nuestro modelo, los *recursos* de Libra tienen la consideración jurídica de títulos-valores y son emitidos por los *módulos* almacenados en la cuentas.

En el caso de los documentos cambiarios propiamente dichos, su emisión se realiza mediante transacciones a la cuenta de la Fábrica Nacional de Moneda y Timbre (en el supuesto de las letras de cambio) o de los bancos comerciales (en el caso de los cheques). La cuenta de la Fábrica Nacional de Moneda y Timbre debe publicar y almacenar los módulos necesarios para dar funcionalidad al nuevo sistema cambiario, en los términos que señalaremos en los párrafos siguientes.

3.1Tipología básica de los títulos-valores electrónicos

En el presente sistema, cada documento cambiario es representado por un recurso (concepto que, como hemos visto, dentro de Libra equivale a los *tokens* de Ethereum), que ha de ajustarse a la siguiente estructura:

{
sección identificativa:
sección dispositiva:
sección de enlace:
sección de encriptación:
}

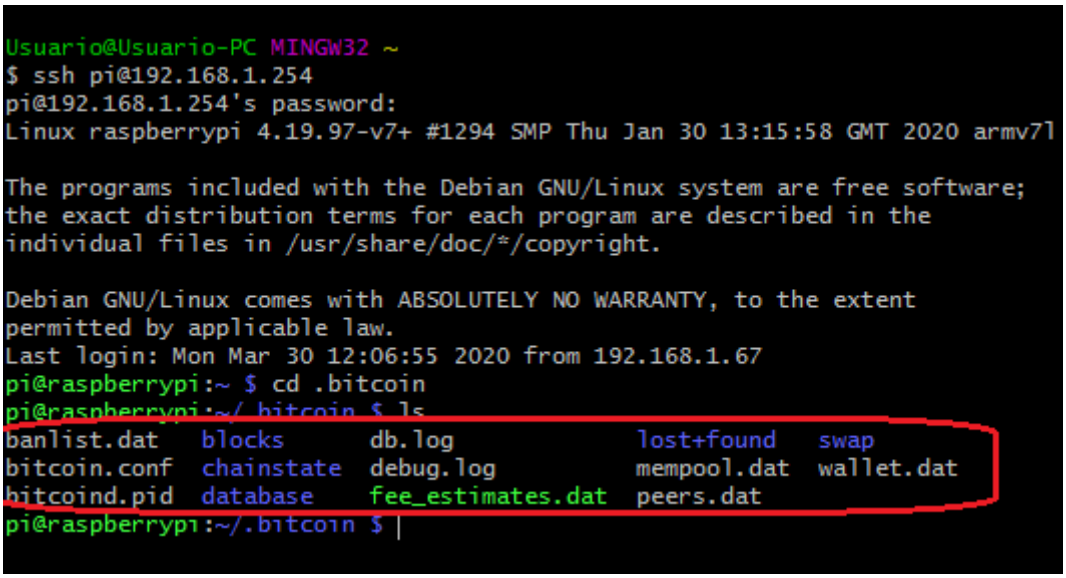
La *sección identificativa* contiene todos los extremos que identifican al documento, como su clase, su número de serie y el timbre electrónico, que es la firma de dichos datos por parte de la autoridad fiscal competente (en España, la Fábrica Nacional de Moneda y Timbre). La *sección dispositiva* alberga todas las circunstancias relativas al acreedor, al deudor, a la cantidad debida y a la fecha del vencimiento, si la hubiere, así como los certificados y las firmas de los intervinientes. Los campos de esta parte del documento se envían encriptados a la *blockchain* utilizando el sistema AES (Advanced Encryption Standard). La *sección de enlace* contiene referencias (consistentes en funciones *hash*) a las transmisiones posteriores o anteriores del documento cambiario. Por último, la *sección de encriptación* contiene la clave simétrica con la que se ha encriptado la sección dispositiva, encriptada a su vez con las claves públicas de los certificados de las partes.

Por el modo de designación del titular, los títulos electrónicos puede ser *al portador*, *nominativos* y *a la orden*:

a) Títulos al portador

El titular es identificado únicamente por su dirección electrónica, que en Libra -como ya habíamos señalado con anterioridad- equivale al *hash* de una clave pública. Los pares clave pública/clave privada se almacenan en un archivo denominado *monedero* o, en lengua inglesa, *wallet*. A modo de ejemplo, en la figura 3 se muestra la estructura de directorio de un nodo de Bitcoin (en el espacio de la pantalla rodeado de rojo). El archivo wallet.dat (situado en la columna de la derecha) es un *monedero* que almacena pares de claves pública-privada.

Fig. 3: Estructura de directorio de un nodo de Bitcoin



Fuente: Elaboración propia

Aquella persona que tiene en su poder la clave privada vinculada al título es considerada como poseedor, portador y titular del mismo. La transmisión del título-valor puede realizarse entregando físicamente la clave privada a otra persona, cambiando dicha clave privada (una posibilidad admitida por el protocolo de Libra) o transfiriendo el título electrónicamente a otra dirección mediante una transacción.

Los títulos al portador electrónicos pueden utilizarse para incorporar múltiples derechos de contenido patrimonial. En el ámbito de los títulos al portador documentados por escrito, el jurista español Rodrigo Uría establecía una clasificación que, sin duda alguna, es plenamente aplicable a los títulos electrónicos:

-Títulos de pago (cheques, billetes de Banco respaldados por un patrón metálico, obligaciones emitidas por sociedades anónimas, etc.), que convierten a su titular en el acreedor de una obligación dineraria.

-Títulos de participación social (acciones de sociedades anónimas), que conceden a su titular derechos políticos o económicos en el ámbito de una sociedad.

-Títulos de tradición (p.e., resguardo de depósitos), que facultan para exigir la entrega de algún objeto o mercadería.

Todos estos supuestos son susceptibles de ser documentados electrónicamente.

b) Títulos a la orden

El titular es identificado con su nombre, apellidos y documento nacional de identidad. Dicha identificación se realiza mediante un certificado electrónico expedido por la Fábrica Nacional de Moneda y Timbre, que vincula la identidad de la persona física (o, en su caso, la jurídica) a una clave pública. El certificado electrónico (que incluye en su interior a la clave pública) y la clave privada se almacenan en un tipo de archivo específico denominado *PKCS12* (en Windows, a estos archivos les corresponde la extensión *.pfx*).

La característica esencial de los títulos a la orden es que su transmisión se realiza mediante un negocio jurídico específico denominado *endoso electrónico*. El título a la orden por antonomasia es la *letra de cambio electrónica*.

c) Títulos nominativos

La identificación de su titular reúne los mismos requisitos que la de los títulos a la orden (es decir, el titular se debe identificar mediante un certificado electrónico). Su particularidad reside en que el módulo que emite el título-valor debe guardar un registro en el que conste cada título individualmente emitido, representado por un *recurso*. La transmisión de cada uno de ellos se realiza mediante la modificación de su correspondiente recurso. Los títulos nominativos pueden utilizarse para documentar los más heterogéneos derechos patrimoniales, desde pagarés hasta acciones de sociedades anónimas.

3.2 Letras de cambio

Una *letra de cambio* es un título-valor que contiene una orden abstracta e incondicional de pago a un acreedor, llamado *tenedor*, por parte de un deudor, denominado *librado*, que éste debe cumplir y ejecutar en un tiempo determinado. Para que este título-valor ostente la condición de letra de cambio, ha de reunir además una serie de requisitos formales exigidos por la legislación cambiaria.

En este apartado introduciremos un nuevo concepto, el de *letra de cambio electrónica*. Analizaremos su tipología, su estructura y sus mecanismos de emisión (libramiento) y transmisión (endoso).

a) Tipología de la letra de cambio

En nuestro modelo, cada letra de cambio es configurada como un recurso de tipo *Letra* emitido por el módulo (contrato inteligente) denominado *Emisor*, situado en la cuenta de la Fábrica Nacional de Moneda y Timbre, dentro de una *blockchain* privada gobernada por el protocolo Libra Core. Para que el recurso reúna la condición de letra de cambio electrónica, ha de contener la siguiente estructura de datos, exigida por lo demás por el artículo 1 de la Ley Cambiaria y del Cheque española:

1: module Emisor{

```
2:      resource Letra {
3:              numero_serie: char[16],                 // Número de serie
4:              clase: int[4],                          // Clase de la letra
5:              tributo: float[16],                     // Tributo a pagar
6:              timbre: char[736],                      // Código expedido por la FNMT
(padding nulo de 2 bytes)
7:              lugar_libramiento: char[48],            // Lugar del libramiento
8:              fecha_libramiento: char[16],            // Fecha del libramiento
9:              moneda: char[16] ,                      // Moneda
10:             importe_letra: char[48],                // Importe a pagar (en letras)
11:             importe_numero:  float[32],             // Importe a pagar (en número)
12:             certificado_librador: char[736],        // Certificado digital del librador
(padding nulo de 2 bytes)
13:             domicilio_librador: char[96],           // Domicilio del librador
14:             certificado_tenedor: char[736],         // Certificado digital del tenedor
(acreedor, padding nulo de 2 bytes)
                domicilio_tenedor: char[96],            // Domicilio del tenedor
15:             IBAN_tenedor: char[48],                 // IBAN del tenedor (padding nulo de 14
bytes)
16:             certificado_librado: char[736] ,        // Certificado digital del librado (deudor,
padding nulo de 2 bytes)
17:             domicilio_librado: char[96],            // Domicilio del librado
18:             ID_librado: char[96],                   // Nombre común (common name) del
librado
19:             fecha_vencimiento: char[16],            // Fecha del vencimiento
20:             firma_librador: char[256],              // Firma del librador
21:             firma_tenedor: char[256],               // Firma del tenedor
22:             firma_librado: char[256],               // Firma del librado (sólo si ha sido
aceptada)
23:             endoso: bool,                           // ¿Ha sido la letra endosada?
24:             direccion_endoso: address,              // Dirección siguiente en la cadena de
endosos

                                                        (nulo, si se trata del último endoso)
25:             aceptacion: bool,                       // ¿Ha sido la letra aceptada?
26:             clave_librador: char[256],              // Clave simétrica encriptada con la
clave pública                                               del librador
27:             clave_tomador: char[256],               // Clave simétrica encriptada con la
clave                                                       pública del tomador
28:             clave_autoridad: char[256]              // Clave simétrica encriptada con la
clave pública                                               correspondiente al certificado
raíz de la FNMT
                //
                ..
                //
40:     }
41:     //...
42: }
```

En las líneas 2 a 28 se crea una suerte de plantilla a la que se han de ajustar todas las letras de cambio, y que tendrá que ser rellenada cada vez que se emita una de ellas. Los parámetros de líneas 3 a 6 (ambas incluidas) conforman la *sección identificativa*, y como su propio nombre indica, se utilizan para identificar a la letra de cambio. Los parámetros de las líneas 7 a 19 reciben el nombre de *sección dispositiva*, y contienen toda la información relativa al negocio jurídico cambiario. Todos ellos serán encriptados utilizando una clave simétrica generada por el ordenador del librado. Albergan en su interior la siguiente información:

-Lugar de libramiento, expresado en una cadena de 16 caracteres (char[16]).

-Fecha de libramiento, codificada en formato YYYYMMDD (en castellano, AAMMDD, año, mes y día), y expresada en una cadena de 8 caracteres (char[8]).

-Tipo de moneda (euro, dólar, yen…). Es una cadena de 16 caracteres (char[16]).
-Importe de la cantidad a pagar. Es un número en coma flotante de 32 bits, y cuyo rango, por tanto, se extiende desde el número 0 hasta el 18.446.744.073.709.551.615.

-Importe de la cantidad a pagar, expresado en letras, y concretamente en una cadena de 48 caracteres (char[48]).

-Número de serie. Es una cadena de 16 caracteres (char[16]).

-Tributo. Indica la cantidad pagada por las partes, en concepto de timbre.

-Certificado digital (X.509) del tenedor y del librador, necesarios para que sus firmas sean consideradas jurídicamente vinculantes, en los términos del artículo 25.2 del Reglamento Europeo 910/2014 (Reglamento eIDAS). Los certificados se guardan en formato DER, y constan de 736 bytes (char[736]) cada uno.

-IBAN de la cuenta bancaria del tenedor, donde se ha de realizar el pago. Cadena de 48 bytes (char[48]), con un almohadillado (*padding*) nulo de 14 bytes.

-Certificado digital del librado (el deudor de la letra).

-Fecha del vencimiento, codificada en formato YYYYMMDD, y expresada en una cadena de 16 caracteres (char[16]), con almohadillado nulo de 8 bytes.

-Firma del librador. Cadena de 256 bytes (char[256]).

-Firma del tenedor. Cadena de 256 bytes (char[256]).

-Firma del librado (deudor). Cadena de 256 bytes (char[256]) que se adjunta una vez que el librado ha aceptado la letra.

Los parámetros de las líneas 23 a 25 reciben el nombre genérico de *sección de enlace*, y se utilizan para la reconstrucción del tracto sucesivo cambiario:

-El campo endoso es un booleano que señala si la letra ha sido transmitida (o no) a una tercera persona por medio de un endoso.
-En el caso de que se haya producido un endoso, el campo direccion_endoso contendrá la dirección donde se ubique el endoso.

-Por último, un booleano señala si la letra ha sido aceptada por el librado o no. Su valor originario es 0. Cuando la letra se acepta, su valor cambia a uno.

Las tres últimas líneas, que conforman la sección de encriptación, almacenarán la clave simétrica encriptada con las claves públicas del librador, el librado y la autoridad estatal emisora de los certificados de identificación digital (en el caso español, la FNMT).

¿En qué cuenta se ha de guardar una letra de cambio electrónica? El lector recordará que la dirección de cada cuenta se calcula a partir de una clave pública, así que, en principio, lo más lógico sería usar la clave pública del certificado del tenedor, mientras que la clave privada se utilizaría para firmar transacciones.

El problema es que el protocolo de Libra sólo permite almacenar un recurso de cada tipo (en este caso, una letra de cambio electrónica) en cada cuenta, y en consecuencia no podría librarse (emitirse) más de una letra de cambio con cargo a una misma dirección. Por ello, proponemos la siguiente solución técnica: cada vez que una persona pretenda emitir una letra de cambio, su ordenador generará un par de claves de criptografía asimétrica, y a partir de la clave pública calculará una dirección electrónica, que será donde se almacene la letra. Una vez creada la cuenta, se modificará su clave privada, haciéndola corresponder con la del certificado. Tras ello, se almacenará la letra de cambio en la cuenta.

b) Ofuscación de los datos de la letra de cambio

A diferencia de lo que sucede con los derechos reales sobre bienes inmuebles, que están sometidos al principio de publicidad formal y cuyos datos están, por lo tanto, a disposición de terceras personas, la tenencia de un documento cambiario sólo es conocida, en principio, por las personas que lo hayan otorgado.

Por este motivo, es necesario crear mecanismos de ofuscación en la *blockchain*, que aseguren que el contenido de los documentos cambiarios sólo sea accesible para las personas que dispongan de una clave determinada.

Proponemos el siguiente mecanismo:

-Los datos de la sección dispositiva será encriptados utilizando el sistema de encriptación simétrica AES (*Advanced Encryption Standard*), utilizando para ello una clave simétrica generada por el ordenador del librador. Esta clave será compartida con el tomador y los demás tenedores ulteriores de la letra, de tal manera que todos ellos tengan acceso a los datos de todo el tracto sucesivo cambiario.

-Los datos de la *sección identificativa* y de la *sección de enlace* permanecerán sin encriptar.

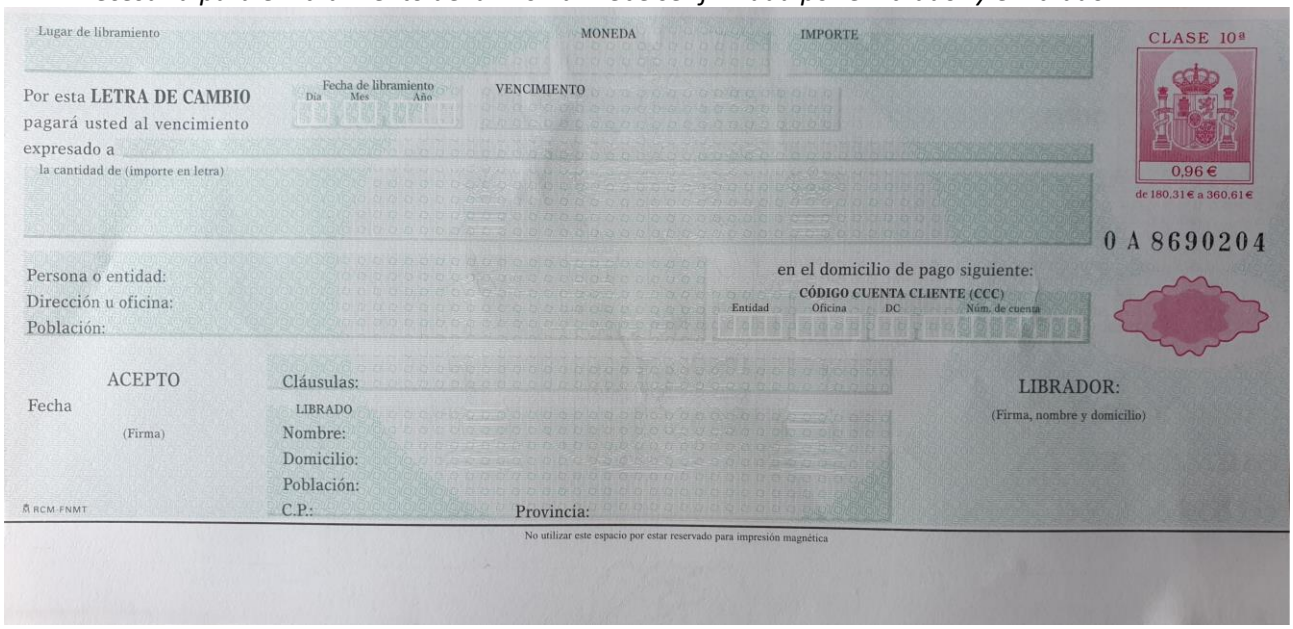
-La clave simétrica será a su vez encriptada utilizando para ello las claves públicas del tomador, del librador y de la autoridad pública encargada de los expedir los certificados digitales.

El resultado se almacenará en los campos clave_librador, clave_tomador y clave_autoridad, respectivamente (todos ellos ubicados en la sección de encriptación). Cada vez que el tomador y el librador pretendan recuperar la clave simétrica original, podrán hacerlo utilizando para ello sus respectivas claves privadas.

c) Libramiento

El acto por el cual se emite una letra de cambio se denomina *libramiento* o *giro*. En el acto intervienen dos personas: el *librador* y el primer tenedor de la letra de cambio, denominado *tomador*. El librador ordena a una tercera persona, el deudor (también llamado librado), pagar una cierta cantidad de dinero al tomador en un tiempo determinado. El deudor no interviene en el libramiento, y no queda obligado cambiariamente hasta que no acepte la letra de cambio, transformándose a partir de ese momento en el *aceptante*. La relación jurídica existente entre el librador y el deudor se denomina *relación de cobertura,* la existente entre el librador y el tomador se llama *relación de valuta*.

Fig.4: Anverso de una letra de cambio española, en el que debe constar toda la información necesaria para el libramiento de la misma. Debe ser firmada por el librador y el librado.



Fuente: Elaboración propia.
El libramiento de una letra de cambio electrónica se estructura en los pasos siguientes:

-A través de la web de la autoridad fiscal competente, el usuario comprará el timbre electrónico necesario para dar validez a la letra. La autoridad entregará al usuario un JSON con los valores de los campos numero_serie, clase y tributo, así como con la firma (“timbre”) de los mismos por parte de dicha autoridad. A cada uno de estos campos se le aplicará la función hash Keccak-256. Las tres cadenas de 256 bits resultantes serán ensambladas y al conjunto se le aplicará de nuevo la misma función. Seguidamente, al resultado se le aplicará la clave privada del certificado raíz de la citada autoridad, y con ello se obtendrá el timbre electrónico a incorporar a la letra de cambio, que será entregado al librador vía protocolo TLS.

-De una forma externa a la blockchain, el tomador enviará en formato JSON su certificado y sus datos bancarios al librador, que rellenará los datos restantes de la letra de cambio (aún sin encriptar). La firma del tomador recaerá sobre las secciones identificativa y dispositiva del documento. La letra firmada será enviada al tomador, que también firmará las mismas secciones. La firma de los participantes se realizará sobre los datos aún no encriptados, puesto que en caso contrario, cualquiera de las dos partes podría instar la nulidad del negocio

cambiario, alegando la existencia de error (que es un vicio de la voluntad invalidante de un negocio jurídico, conforme a lo dispuesto en múltiples ordenamientos civiles europeos).

-Las secciones identificativa y dispositiva del documento serán encriptadas siguiendo el procedimiento establecido en la sección b).

-El ordenador del tomador generará un par de claves, pública y privada. A partir de la primera se calculará la dirección electrónica de la cuenta donde se almacenará la futura letra de cambio.

-La clave privada de la cuenta del tomador será modificada y se hará coincidir con la correspondiente a su certificado digital.

-Por último, el envío de la letra a la blockchain se realizará mediante una transacción por parte del tomador a la cuenta de la FNMT, en la que invocará la función librar_letra dentro del módulo Emisor. Los parámetros de la transacción serán el lugar (lugar_i), y la fecha (fecha_i) del libramiento, la moneda (moneda_i) en que se realiza, su importe en número (importe_i) y letra (importe_letra_i), el número de serie (numero_serie_i), el timbre electrónico (timbre_i), el certificado del librador (certificado_librador_i), la firma del librador (firma_librador_i), el certificado del tomador (certificado_tenedor_i), el IBAN del tomador (IBAN_i), la fecha del vencimiento (fecha_vencimiento_i) y las claves encriptadas del librador, el tomador y la autoridad estatal encargada de expedir los certificados electrónicos (clave_librador_i, clave_tomador_i, clave_autoridad_i). La transacción será firmada por el librador y el tomador.

Fig. 5. Esquema del libramiento de una letra de cambio. En el primer paso, el tenedor envía su certificado y datos bancarios al librador. En el segundo paso, el librador completa la letra, la firma y la envía al tenedor. Finalmente, el tenedor vuelve a firmarla, encripta los datos y los envía a la blockchain.

Fuente: Elaboración propia.

La función *librar_letra* debe tener una estructura similar a la siguiente:

```
1: module Emisor{
2:      public librar_letra(lugar_libramiento_i, fecha_libramiento_i, moneda_i, importe_i,
importe_letra_i, 3:      numero_serie_i, timbre_i, certificado_librador_i, firma_librador_i,
certificado_tenedor_i, firma_tenedor_i, IBAN_i, fecha_vencimiento_i, clave_tomador_i,
clave_librador_i, clave_tomador_i):
                Letra {
                //
                ...     // En las primeras líneas de código, la función comprueba que la firma
de la                   …       // transacción por el librador y el librado es válida
                //
100:            RejectUnless(numero_serie != 0);
101:            move_to_sender<Letra>(
102:            Letra {
103:                    lugar_libramiento: lugar_libramiento_i,
104:                    fecha_libramiento: fecha_libramiento_i,
105:                    moneda: moneda_i,
106:                    importe: importe_i,
107:                    importe_letra: importe_letra_i,
108:                    numero_serie:  numero_serie_i,
109:                    timbre: timbre_i,
110:                    certificado_librador: certificado_librador_i,
111:                    certificado_tenedor: certificado_tenedor_i,
112:                    IBAN_tenedor: IBAN_i,
113:                    fecha_vencimiento: fecha_vencimiento_i,
114:                    firma_librador: firma_librador_i,
115:                    firma_tenedor: firma_tenedor_i,
116:                    clave_librador: clave_tomador_i,
117:                    clave_tomador: clave_librador_i,
118:                    clave_FNMT: clave_tomador_i
119:                    }
120:            );
121:    }
122:    //...
123: }
```

Para interpretar estas líneas desde un punto de vista jurídico, no es necesario dominar el lenguaje de programación Move IR, y tampoco entrar en los pormenores de cada una de ellas.

En términos generales, podemos realizar las siguientes observaciones:

-En los cuatro primeras líneas se fijan los parámetros de entrada de la función, que son, precisamente, los datos necesarios para librar la letra de cambio.

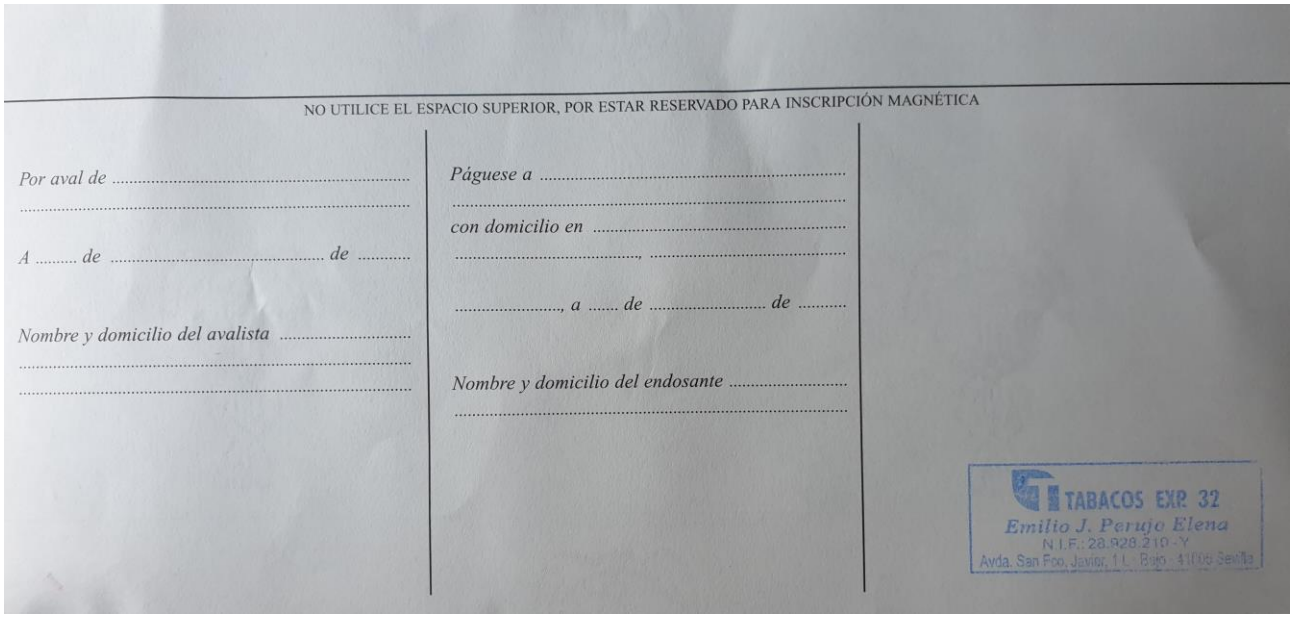
-En las líneas 5 a 99, que no aparecen desarrolladas en el diagrama de arriba, la función comprobará que la cantidad transferida a la cuenta FNMT es igual a la descrita en el campo *timbre* y que las firmas de los participantes son válidas.

-Por último, en las líneas, 101 a 114, la función rellena la plantilla de la letra de cambio con los datos de entrada proporcionados en las cuatro primeras líneas. Tras ello, la letra es enviada a la dirección electrónica del librador (línea 101, instrucción *move_to_sender*).

d) Endoso

El endoso es aquel negocio jurídico en cuya virtud el tenedor de un título a la orden transfiere su posición jurídica de acreedor cambiario a otra persona. En los títulos-valores documentados en papel, el endoso se hace constar en el dorso del *mismo* documento donde consta la letra de cambio, como una suerte de añadido al documento cambiario original, tal y como se muestra en la imagen:

Fig. 6: Dorso del modelo oficial de una letra de cambio. Los datos relativos al endoso se escriben en la columna del centro.



Fuente: Elaboración propia.

En el plano electrónico este trabajo propone que los endosos sean representados por un recurso específico, denominado *Endoso*, que quedaría vinculado a una determinada letra de cambio por medio de una referencia (*hash*) a los contenidos de esta última. La estructura de cada endoso es relativamente simple:

```
1: module Emisor{
2:         resource Endoso {
3:                 numero_endoso: int,                    // Posición en la cadena de endosos
```

```
4:      direccion_anterior: address,          // Dirección anterior en la cadena de endosos
5:      hash_letra: char[256],                // Hash de los contenidos encriptados del endoso (o la letra) anterior
6:      certificado_endosatario: char[736],   // Certificado del endosatario (almohadillado - padding- nulo de 2 bytes)
7:      IBAN_endosatario,                     // Cuenta del endosatario
7:      nuevo_endoso: bool,                   // ¿Ha habido un nuevo endoso?
8:      direccion_siguiente: address,         // Dirección siguiente en la cadena de endosos
                                              (nulo, si se trata del último endoso)
9:      firma_endosante: char[256]            // Firma del endosante
10:     firma_endosatario: char[256]          // Firma del endosatario
        clave_endosatario:                    // Clave simétrica encriptada con la clave pública del endosatario
    //...
21:     }
22:     //...
23: }
```

Los datos contenidos en este recurso son los siguientes:

-La variable *direccion_anterior* (línea 4) alberga la dirección de la cuenta donde se haya almacenado la letra de cambio original (en el caso de que se trate del primer endoso), o bien la del endoso inmediatamente anterior (en el caso en que previamente haya habido otro endoso). De este modo, se forma una suerte de *"tracto sucesivo cambiario"*, en cuyo inicio se encuentra la letra de cambio original, tal y como fue librada, y en cuyo final se sitúa el último endoso. Este tracto sucesivo es reforzado por medio de una referencia criptográfica (*hash*) al documento cambiario inmediatamente anterior (letra o endoso). El número de endosos producidos hasta el momento quedará registrado en la variable *numero_endoso*.

-Como en otros casos, el recurso (en este caso, el endoso) deberá almacenar el certificado electrónico de su titular (*certificado_endosatario*).

-Si la letra de cambio ha sido endosada de nuevo, el booleano al que hace referencia la línea 7 tomará el valor de uno y la dirección del nuevo endoso será almacenada dentro de la variable *direccion_siguiente*.

Todos los datos reseñados serán encriptados, salvo los almacenados en los campos *nuevo_endoso*, *direccion_anterior* y *dirección_siguiente*, que conservarán sus valores originales.

Los endosos electrónicos se realizan mediante un procedimiento muy parecido al del giro de la letra: en primer lugar, el endosatario envía su certificado y sus datos bancarios al endosante. El endosante descifra la clave simétrica gracias a su clave privada, la vuelve a cifrar con la clave pública del certificado del endosatario y la guarda en el campo *clave_endosatario*. Tras ello, rellenará los datos restantes del endoso y calculará dos firmas: una, sobre los datos sin encriptar (exigencia del Derecho Civil) y otra, sobre los datos encriptados (exigencia del protocolo de Libra). Ambas se enviarán al endosatario, junto con el contenido de la letra.

Seguidamente, el endosatario enviará un mensaje a la cuenta de la FNMT, invocando la función *construir_tracto*, que llevará por parámetro la dirección del documento electrónico que se va a

endosar. Por medio de las referencias *direccion_anterior* (que no está encriptada) y *hash*, la función reconstruirá la cadena de endosos, remontándose hasta la letra original. Los datos de toda la cadena serán enviados al endosatario, que los descifrará, y comprobará la validez de los mismos.

Si todo es correcto, el endosatario firmará los datos del nuevo endoso, los encriptará y los enviará mediante una transacción a la cuenta de la FNMT. La transacción invocará la función *publicar_endoso* que, como su propio nombre indica, publicará un nuevo endoso en la cuenta del endosatario. Los parámetros de la transacción (y de la función) vendrán constituidos por todos los extremos del nuevo endoso, así como por la firma del endosante de los datos encriptados de la letra. La función *publicar_endoso*, que debería ser ejecutada por todos los nodos de la red, tendría en lenguaje Move IR la estructura siguiente:

```
1: module Emisor{
2:      public publicar_endoso (...) {
            //
            ...          // En estas líneas la función calculará el hash de los contenidos
publicados          ...          // del endoso anterior, y comprobará que los datos
(encriptados) del          …          // nuevo endoso han sido firmados por
el endosante
            //

101:        let direccion_endosatario address = GetTxnSenderAddress();
102:        let ref_endosante: &mut Endoso =
BorrowGlobal<Endoso>(move(direccion_endosante));
103:        let ref_endosatario: &mut Endoso =
BorrowGlobal<Endoso>(move(direccion_endosatario));
104:        numero_endoso_i =  *move(&mut move(ref_endosante).numero_endoso) + 1;
105:        *move(&mut move(ref_endosante).endoso) = 1;
106:        *move(&mut move(ref_endosante).direccion_siguiente) =
direccion_endosatario;

201:        move_to_sender<Endoso>(
202:        Endoso {
203:              certificado_endosatario: certificado_endosatario_i,
204:              IBAN_endosatario: IBAN_endosatario_i,
              numero_endoso: numero_endoso_i
              ...
              }
            )
      }
```

En sus primeras líneas (2 a 106), no reproducidas en el esquema, la función verificará la firma del endosante, calculará el *hash* del endoso anterior y modificará dos de los campos de este último: el booleano *nuevo_endoso* tomará el valor de uno y la variable *direccion_siguiente*, la dirección del nuevo endoso. Seguidamente se rellenarán los datos del nuevo endoso, y éste será publicado en la cuenta del endosatario.

e) Recuperación de contraseñas

Dado que el poder de disposición sobre *tokens* y criptomonedas está intrínsecamente vinculado a una clave privada, la pérdida de esta última por parte de su titular conlleva la imposibilidad del ejercicio del derecho. Para prevenir este indeseable resultado, en el caso de los títulos-valor emitidos nominativamente o a la orden, el módulo emisor deberá disponer de una función, *recuperar_contraseña*, para recobrar las claves perdidas.

El usuario que pretenda recuperar su clave debe previamente obtener un nuevo certificado digital de parte de la FNMT y abrir una nueva cuenta dentro de la *blockchain* de Libra. Seguidamente, desde esta cuenta enviará una transacción invocando la función *recuperar_contraseña*. Sus parámetros serán dos:

-El nuevo certificado electrónico, encriptado con la clave *pública* del certificado raíz de la FNMT.
-La dirección donde se alberga la letra de cambio cuya contraseña se ha perdido.

La función comprobará que el nuevo certificado es válido, y que el viejo ha sido revocado, y que ambos corresponden a la misma persona. Si la comprobación ha sido exitosa, la función ordenará un tipo de endoso específico (firmado esta vez con la clave privada del certificado raíz de la FNMT), cuya dirección de destino será, precisamente, la nueva cuenta de donde procede la transacción. La clave simétrica será encriptada con la clave pública del nuevo certificado y se almacenará en el campo *clave_endosatario* del nuevo endoso.

f) Aceptación

La aceptación es aquel acto por el que el librado presta su consentimiento para convertirse en obligado cambiario, comprometiéndose con ello a ejecutar el mandato de pago ordenado por el librador. Sólo es necesaria cuando la letra es exigible a un plazo desde la vista.

La aceptación puede realizarse en el mismo momento en que la letra es girada o puede realizarse con posterioridad. En el primer caso, el documento original deberá incorporar el *certificado del librado*, su *domicilio*, así como la *firma* de este último sobre todos los datos de la misma, en los mismos términos que se exigen al tenedor. El booleano *aceptada* deberá tener el valor 1.

Si la aceptación se realiza con posterioridad, el librado deberá enviar una transacción a la FNMT, invocando la función *aceptar_letra*, dentro del módulo *Emisor*. Los parámetros de esta función vendrán constituidos por la dirección de la letra, así como el certificado y la firma del librado. La función comprobará que la cadena *ID_librado*, que tenía efectos identificativos, está presente en el certificado del librado, y que este último es válido, y no ha sido revocado. Si la verificación de la firma arroja un resultado positivo, el certificado del librado se incorporará a la letra de cambio original, cuyo booleano *aceptada* tomará el valor de 1.

g) Presentación al pago y cancelación de la letra

Cuando llegue la fecha del vencimiento, la letra podrá ser presentada al pago ante la entidad bancaria correspondiente donde tuviese domiciliada su cuenta el librado. Se creará un nuevo

recurso denominado *Cancelacion* dentro de la cuenta que la entidad bancaria tenga en la *blockchain*.

La estructura del recurso *Cancelacion* será la siguiente:

```
1: module Emisor{
2:      resource Cancelacion {
3:          numero_endoso: int,                  // Posición en la cadena de endosos
4:          direccion_presentante: address,      // Dirección de la cuenta del presentante
5:          hash_letra: char[256],               // Hash de los contenidos encriptados en el documento cambiario del presentante
6:          certificado_banco: char[734],        // Certificado del banco
7:          firma_presentante: char[256]         // Firma del presentante
8:          firma_banco: char[256]               // Firma del banco
9:          clave_banco:                         // Clave simétrica encriptada con la clave pública del banco
            pagada: bool,                        // Letra pagada
            protestada: bool                     // Letra impagada y protestada
      //...
20:   }
11:   //...
12: }
```

El mecanismo de la presentación al pago es relativamente simple:

Una vez que la obligación cambiaria se haga exigible, el tenedor solicitará el pago de su letra a través del servidor del banco domiciliatario, de una forma completamente externa a la *blockchain*. Junto con la petición, enviará los datos encriptados de toda la cadena de endosos. El Banco descifrará la clave simétrica de la letra, comprobará que todos los datos son correctos e intentará realizar una transferencia de fondos desde la cuenta bancaria del librado a la del tomador. Si las cuentas bancarias de origen y de destino pertenecen a diferentes entidades, la letra y su cadena de endosos será presentada ante una Cámara de Compensación.

Si la transferencia de fondos ha sido exitosa, el booleano *pagada* tomará el valor de uno. En caso de una transferencia fallida, el booleano *pagada* tomará el valor cero, mientras que el booleano *protestada* tomará el valor uno. En ambos casos, el Banco enviará una transacción a la *blockchain* en la que ejecutará la función *cancelar_letra*. Esta última función comprobará que los datos han sido firmados por el banco y, si así ha sido, publicará un recurso Cancelacion en la dirección atribuida a la entidad bancaria. La cancelación de la letra implica que ya no podrán realizarse más endosos a la misma.

3.3Cheques

De acuerdo con su definición inglesa originaria, un cheque puede ser definido como *"una letra de cambio pagadera a la vista, cuyo librado es un banco"*.

Consideramos plenamente aplicables a los cheques electrónicos los esquemas de libramiento, transmisión y presentación al pago de las letras de cambio, pero con las siguientes particularidades:

a) En el plano escrito, los cheques no se emiten sobre papel timbrado, sino sobre un talonario proporcionado al librador por el propio banco librado. En la esfera electrónica, proponemos que la emisión, transmisión y presentación al pago de los cheques se realicen mediante transacciones realizadas a la cuenta que el banco librado tiene en la *blockchain*. El código albergado en esa cuenta tendrá que estar estandarizado y aprobado previamente por el Ministerio de Justicia o el de Economía.

b) Los cheques no necesariamente han de emitirse en forma nominativa. También pueden emitirse al portador. En este último caso, no es necesario adjuntar el certificado digital del tenedor al documento electrónico. El acreedor del cheque quedaría identificado exclusivamente con su clave pública, mientras que la pérdida de su clave privada implicaría el perjuicio definitivo del documento.

c) En el cheque no es necesario fijar la fecha de su cobro. Será siempre pagadero a la vista.

3.4Pagarés

Un pagaré es un documento cambiario en cuya virtud una persona, denominada firmante, se obliga a pagar a otra, denominada tenedor, una cantidad de dinero en una fecha determinada. Los pagarés son siempre nominativos y no pueden transmitirse. Dado que no están destinados a circular, en ellos la relación jurídica que se documenta no es triangular, sino bilateral.

Proponemos que la firma del pagaré se realice mediante una transacción a la FNMT, siguiendo un procedimiento similar al de la letra de cambio, sólo que, en este caso, los campos relativos al librador de la letra y su tomador, dentro de la parte dispositiva, serán sustituidos por los del firmante del pagaré y su tenedor, respectivamente. Dado que los pagarés no son transmisibles, la sección de enlace será inexistente.

4.La plena validez jurídica de los títulos-valores residentes en una blockchain

A lo largo de los apartados anteriores hemos esbozado las bases para la creación de un nuevo ordenamiento cambiario de carácter electrónico, que residiría en el ámbito de una cadena de bloques. Aunque muchos autores cuestionan que los *tokens* de Ethereum o los *recursos* de Libra puedan constituir verdaderos derechos subjetivos, ya que residen exclusivamente en el plano cibernético, lo cierto es que, tal y como expusimos en uno de nuestros trabajos anteriores,[13] el ordenamiento jurídico y el ordenamiento algorítmico están íntima y crecientemente interconectados y lo que acontezca en el ámbito cibernético tiene una cada vez mayor influencia el ámbito legal, a través de instituciones como las acciones de enriquecimiento injusto o la acción aquiliana.
En esta línea, podemos decir que la aparición de Libra dio un paso más en esta compenetración, toda vez que la creación de la nueva *blockchain* vino acompañada de la fundación de una persona jurídica, la *Libra Association*, entre cuyos cometidos se hallaban los de crear y mantener un fondo compuesto de divisas y de títulos de deuda pública, para respaldar la emisión de criptomonedas. Los estatutos del consorcio establecieron con claridad que la emisión o amortización de criptomonedas debía venir acompañada de la respectiva compra o venta de

activos en el ámbito jurídico-económico y establecían asimismo mecanismos a través de los cuales los tenedores de libras podían en cualquier momento liquidar su inversión y transformarla de nuevo en activos físicos. De esta manera, el proyecto Libra demostró a la opinión pública y a los mercados financieros que era posible la emisión de criptomonedas y *tokens* respaldados por activos físicos y, por lo tanto, con valor intrínseco, transformando lo que sólo eran cadenas de unos y ceros en verdaderos derechos patrimoniales. Dado que una criptomoneda de estas características tenía la potencialidad de transformarse en un verdadero mecanismo de pago, rivalizando con el propio dólar, el proyecto Libra fue temporalmente paralizado por presiones de la Reserva Federal[14] y de la propia Casa Blanca.[15]

Conclusiones

Con todo, a pesar de los contratiempos sufridos por Libra, consideramos que la digitalización del ordenamiento cambiario es un proceso inexorable y que la pandemia global generada por la Covid-19 no hará sino acelerar la transferencia de buena parte del tráfico jurídico al ciberespacio. Desde mi punto de vista, la incorporación de documentos cambiarios a una base de datos electrónica conlleva las siguientes ventajas:

-*Agilidad*: La negociación y transmisión de los títulos cambiarios tiene lugar en contados segundos, aunque el librador o el librado se encuentren a miles de kilómetros de distancia y confinados en sus domicilios, a diferencia de lo que sucede con los títulos plasmados en papel.

-*Descentralización*: La información no está presente en un único servidor, sino que se encuentra replicada en múltiples nodos, y con ello queda protegida frente a ataques de *ramsonware*. No sería necesario realizar copias de seguridad periódicas de la misma, dado que éstas se efectuarían automáticamente por el propio sistema. Aún así, algunos esquemas de criptomonedas de titularidad estatal, como el chino, están comenzando a prescindir de la descentralización y, en su lugar, prevén la utilización de bases de datos centralizadas y gestionadas por autoridades públicas.

-*Anonimato*: La utilización de criptografía permite la creación de sistemas de transmisión de derechos electrónicos con el mismo nivel de anonimato que en el caso del dinero físico o los títulos al portador, a diferencia de lo que sucede con las transferencias bancarias electrónicas de dinero, en las que tanto pagador como receptor quedan plenamente identificados.

-Existencia de *contratos inteligentes*, que realizan operaciones de creación, transferencia y modificación de derechos digitales de un modo automatizado.

Como posibles desventajas/riesgos de la digitalización del tráfico jurídico podríamos señalar, aparte de las inherentes a la seguridad de los sistemas informáticos y la debilidad de los algoritmos de criptografía, la posibilidad de que se produzca un *colapso cibernético* como consecuencia de un acontecimiento extraordinario, como una tormenta solar,[16] que afectaría sobre todo a la memoria *flash,*[17] aunque quizá no tanto a los dispositivo de almacenamiento ferromagnéticos[18] (hay rocas capaces de preservar información magnética durante miles de millones de años).[19] Para prevenir los daños de un evento catastrófico de estas características, proponemos que los servidores que almacenen cualquier tipo de información jurídica realicen periódicamente copias de seguridad (*backups*) en soporte óptico o en papel.

Para implementar el sistema esbozado en este artículo, en España ni siquiera sería necesario reformar la *Ley Cambiaria y del Cheque*, dado que ninguno de sus artículos impone la redacción en papel de los documentos cambiarios. Por otra parte, aunque el artículo 37.1 del *Reglamento del Impuesto de Transmisiones Patrimoniales y Actos Jurídicos Documentados* establece que la letra de cambio se ha de redactar en "efectos timbrados", en mi opinión esta expresión tampoco excluye la posible creación de *efectos timbrados electrónicos* por parte de la FNMT, en los términos establecidos con anterioridad. Para regular la expedición de títulos-valores electrónicos y garantizar el pago del impuesto de actos jurídicos documentados bastaría con la aprobación de una orden ministerial del mismo rango que la *Orden de 30 de junio de 1991 por la que se aprueba el modelo de letra de cambio*.

De todo lo dicho consideramos esencial para el desarrollo tecnológico de España que dentro del Ministerio de Justicia se cuente con una Dirección General de Nuevas Tecnologías en el marco de la cual expertos en derecho patrimonial y en ciencias de la computación programen el funcionamiento de una base de datos, dotada de elementos criptográficos, y que sea capaz de garantizar la segura transferencia de títulos-valores y valores negociables electrónicos tanto desde el punto de vista de la seguridad informática como de la jurídica. En el momento en que se escribe este artículo (primavera de 2020), el modelo de globalización liberal implantado a lo largo de los años 40 del siglo XX se encuentra en franca regresión y como consecuencia de ello muchos países van a comenzar a desarrollar de nuevo políticas de industrialización, particularmente en el sector tecnológico. Nosotros consideramos que la transferencia de amplios sectores del tráfico jurídico hacia el ciberespacio puede constituir un extraordinario acicate para el sector tecnológico español.

Notas

[1] Un *satoshi* es una fracción de *bitcoin*. 100 millones de satoshis equivalen a un *bitcoin*.

[2] "Propuesta de un nuevo modelo de Registro de la Propiedad basado en tecnología blockchain", en *www.derecom.com La Revista Internacional de Derecho de la Comunicación y Nuevas Tecnologías*, http://www.derecom.com/derecom [accedido el 15 de abril de 2020]

[3] La definición original en lengua alemana apareció por primera vez en la entrada *"Die Wertpapiere"* del manual de derecho mercantil y cambiario editado y publicado por Wilhelm Endemann en 1882. Rezaba así: "*ein Wertpapier ist eine Urkunde, in der ein privates Recht in der Weise verbrieft ist, dass zur Geltendmachung des Rechts die Innehabung der Urkunde erforderlich ist*".

[4] "La minería de bitcoin consume más energía que Dinamarca", en *IHODL.com,* https://es.ihodl.com/topnews/2018-11-06/el-bitcoin-consume-mas-energia-que-dinamarca/ [accedido el 15 de abril de 2020]

[5] En un *ataque Sybil*, los *hackers* tratan de hacerse con el control de una red creando usuarios virtuales, falsos, con el objetivo de conseguir una mayoría de votos dentro de la misma.

[6] "Facebook pretende darle giro a libra al ligarla a monedas de países donde opere para calmar a bancos reguladores", en *xataka.com,* https://www.xataka.com/criptomonedas/facebook-plantea-darle-giro-a-libra-al-ligarla-a-monedas-paises-donde-opere-para-calmar-a-bancos-reguladores [accedido el 15 de abril de 2020]

[7] "El DCEP de China será la primera moneda digital del mundo, según funcionario sino", en *Asociación de Especialistas Certificados en Delitos Financieros.org,* https://www.delitosfinancieros.org/el-dcep-de-china-sera-la-primera-moneda-digital-nacional-del-mundo-segun-funcionario-chino/ [accedido el 15 de abril de 2020]

[8] "DCEP: China's National Digital Currency Overview", en *Boxmining.com*, https://boxmining.com/dcep/ [accedido el 15 de abril de 2020]

[9] Ver: *Binance.zendesk.com,* https://binance.zendesk.com/hc/es/articles/360032604131 [accedido el 15 de abril de 2020]

[10] El simulador virtual es *EVM (Ethereum Virtual Machine)* en el caso de Ethereum y un contenedor Docker en el caso de Hyperledger Fabric.

[11] El profesor chino Zhigou He comenta en una entrevista con Forkast.News lo siguiente respecto al criptoyuan: *Es una enorme base de datos que usa la función hash y tecnología en cadena. No hay ningún protocolo distribuido. Cada vez que lo menciono, mis colegas en la Universidad de Chicago me dicen que eso no es blockchain. Estoy de acuerdo*. (*It's a huge database using the hash function, chain technology. There's no distributed ledger portal. Every time I mention [it], my colleagues at UChicago will immediately tell me it's not blockchain. I actually agree*).
Ver: *forkast.news Future thinking in Times of Change,* https://forkast.news/wp-content/uploads/2019/12/Forkast.Insights-China-Blockchain-Report-2019-2020.pdf [accedido el 15 de abril de 2020]

[12] En Ethereum y Bitcoin, las transacciones son ensambladas en bloques que, a su vez, se enlazan a una única *cadena de bloques*. En Libra, las transacciones se incorporan directamente a la cadena, sin que sea necesario ensamblarlas previamente en bloques.

[13] "Una aproximación al ordenamiento algorítmico y a su proyección civil, mercantil y financiera", en *www.derecom.com La Revista Internacional de Derecho de la Comunicación y Nuevas Tecnologías,* http://www.derecom.com/derecom [accedido el 15 de abril de 2020]

[14] "La Fed se pronuncia sobre Facebook Libra y no son buenas noticias para la red social", en *El blog salmón.com*, https://www.elblogsalmon.com/economia/fed-se-pronuncia-facebook-libra-no-buenas-noticias-para-red-social [accedido el 15 de abril de 2020]

[15] "Trump carga contra la moneda virtual de Facebook", en *Economía digital.es,* https://www.economiadigital.es/tecnologia-y-tendencias/trump-carga-contra-la-moneda-virtual-de-facebook_637643_102.html [accedido el 15 de abril de 2020]

[16] La tormenta solar más poderosa registrada hasta el momento es la de 1859, también conocida con el nombre de *Evento Carrington*:
Ver Wikipedia.org., https://es.wikipedia.org/wiki/Tormenta_solar_de_1859.

[17] La memoria *flash* es utilizada en dispositivos de memoria USB y en discos duros sólidos (SSD).

[18] La memoria ferromagnética es utilizada en discos duros convencionales.

[19] Como curiosidad, gracias a los registros paleomagnéticos de las rocas, se han podido reconstruir los continentes desaparecidos cientos de millones de años.

Bibliografía

BANO S. *et al.*. "State machine replication in the Libra Blockchain". Disponible en: https://developers.libra.org/docs/state-machine-replication-paper (consultado el 1 de abril 2020).

BLACKSHEAR S. *et al.*. "Move: A language with programmable resources". Disponible en: https://developers.libra.org/docs/move-paper (consultado el 1 de abril 2020).

GARCIA, M. (2019). "Facebook Move Instructions & Builtins Cheat Sheet". Disponible en: https://medium.com/facebook-libra-developers/facebook-move-instructions-built-in-cheat-sheet-a91de15bcb82 (consultado el 15 de abril 2020).

HUECK A. y CANARIS C.-W. (1986). *Recht der Wertpapiere*. Múnich: Vahlen.

JIMÉNEZ SÁNCHEZ, G. y DÍAZ MORENO, A. (2019). *Lecciones de Derecho Mercantil*. Madrid: Editorial Tecnos.

MALIWAL, C. (2019). "Move language tutorial: Building token on Libra using Move". Disponible en: https://deqode.com/blog/move-language-tutorial/ (consultado el 15 de abril 2020).

MENÉNDEZ, A. y URÍA, R. (1999). *Curso de Derecho Mercantil*. Madrid: Civitas Ediciones.

PAZ-ARES C. (2005). *La naturaleza jurídica de la letra de cambio*. Madrid: Colegio de Registradores.

PAZ-ARES C. (1996). "La desincorporación de los títulos-valor". *Revista de Derecho Mercantil,* núm. 219, págs 7 y ss. Madrid: Thomson Reuters Aranzadi.

RODRÍGUEZ ABRIL, R. (2019). "Sobre la legitimación criptográfica de firmas en los contratos*". Derecom. La Revista Internacional de Derecho de la Comunicación y las Nuevas Tecnologías,* 27, 112-139. http://www.derecom.com/derecom (consultado el 1 de abril 2020).

RODRÍGUEZ ABRIL, R. (2020). "Una aproximación al ordenamiento algorítmico y a su proyección civil, mercantil y financiera*". Derecom. La Revista Internacional de Derecho de la Comunicación y las Nuevas Tecnologías*, 28, 01-28. http://www.derecom.com/derecom (consultado el 1 de abril 2020).

RODRÍGUEZ ABRIL, R. (2020). "Propuesta de un nuevo modelo de Registro de la Propiedad basado en tecnología blockchain". *Derecom, La Revista Internacional de Derecho de la Comunicación y las Nuevas Tecnologías* 28, 65-94. http://www.derecom.com/derecom (consultado el 1 de abril 2020).

THE LIBRA ASSOCIATION. "An Introduction to Libra". Disponible en: https://libra.org/en-us/whitepaper (consultado el 1 de abril 2020).