icade núm. 101 [Revista cuatrimestral de las Facultades de Derecho y Ciencias Económicas y Empresariales]
Monográfico
FinTech: la tecnología en las finanzas. Oportunidades y desafíos
Experiencias
2. Identidad digital sobre «Blockchain» a nivel nacional (ALEX PUIG PASCUAL)

2 Identidad digital sobre «Blockchain» a nivel nacional

ALEX PUIG PASCUAL

CEO. Digital Currency Summit, alex@alastria.io

Sumario:

RESUMEN: El presente análisis se centra en la descripción de algunos fundamentos técnicos de criptografía asimétrica necesarios para asimilar la noción de cadena de bloques (blockchain), y su expresión registral, la tecnología de registro distribuido. A continuación se exponen algunas ventajas y casos de uso de la cadena de bloques, como la contratación inteligente, o la identidad digital, apuntándose a la creación de una futura red española semipública *blockchain* .

PALABRAS CLAVE: Criptografía asimétrica # Función hash # Cadena de bloques # Registro distribuido # Identidad digital

DIGITAL IDENTITY ON BLOCKCHAIN AT NATIONAL LEVEL

ABSTRAC:T This paper describes the fundamentals of asymmetric cryptography needed to understand the concept of blockchain as a sequence of data blocks, and its registry expression, distributed-ledger technology. Some advantages and cases of use of *blockchain* are exposed thereafter, as smart contracting, digital identity uses, with mention of a foreseen Spanish semipublic *blockchain* .

KEYWORDS: Asymmetric cryptography # Hash function # *blockchain* # Distributed ledger # Digital identity

I. ¿QUÉ ES «BLOCKCHAIN»?

Existe confusión alrededor de la tecnología de cadenas de cloques (en lo sucesivo, usando el argot británico, *blockchain*) y sus aplicaciones prácticas. Esto es debido a que su uso engloba muchas otras áreas e iniciativas: *Bitcoin, Ethereum, Hyperledger, sidechains, smart contracts, tokens* digitales... Casi siempre, cuando hablamos de *blockchain* , nos referimos metafóricamente a un *libro contable mayor* (en realidad, una base de datos) que contiene una lista de operaciones o transacciones. Las cuales aparecen repetidas o replicadas en múltiples ordenadores, y no únicamente en un ordenador central, como viene siendo tradicional en las operaciones de los mercados financieros (por ejemplo, en las bolsas, o en los centros de liquidación y compensación de operaciones).

Aunque, siendo más precisos, si buscamos un símil correcto, deberíamos comparar a *blockchain* , por su universalidad y por su carácter expansivo, con internet, en el sentido de que estamos hablando de una tecnología innovadora que va mucho más allá que una simple base de datos: *blockchain* tiene capacidad de *registro universal de transacciones* . Es decir, todo lo que ocurre en la red de nodos u operadores, dentro de una plataforma (transacciones u operaciones) queda reflejado simultáneamente en todos los nodos.

A esta característica se la denomina en el argot técnico *descentralización* o, más exactamente, *distribución.* El registro blockchain es distribuido (basado en *distributed ledger technology, DLT)* porque todos los operadores saben qué sucede a la vez, cuándo se ha generado nueva información, y quiénes la han generado, y en qué términos. Además, esa información se plasma de forma irreversible y única, gracias a la *criptografía* .

1. LAS BASES DE «BLOCKCHAIN»: NOCIONES DE CRIPTOGRAFÍA ASIMÉTRICA

Por eso, para entender *blockchain* y sus aplicaciones en el campo de la identidad digital necesitamos previamente adquirir ciertos conocimientos básicos sobre criptografía. Principalmente, necesitamos entender el concepto de función *hash* y las bases de la llamada *criptografía asimétrica* .

La denominada Hash (literalmente, «picadillo»), es una función matemática que se aplica a cualquier entrada informática (texto, fichero, audio,...) y produce un resultado, producto o salida de datos que se conoce como «resultado o suma de comprobación» o *checksum*, que tiene una longitud fija y determinada. Dicho *checksum* es siempre el mismo para una misma entrada de datos introducidos; pero con sólo cambiar una coma en dichos datos, el resultado obtenido sería completamente distinto.

Un hash, por axioma, y por voluntad de quien lo crea, es *irreversible* . La razón es matemática y algorítmica. La característica de irreversibilidad no es del todo cierta, sin embargo. Existe una posibilidad de cambiar el resultado obtenido. Pero la probabilidad de materializarlo, de manipular ese resultado, y de obtener *outputs* diferentes introduciendo los mismos datos encriptados, es, a día de hoy, tremendamente baja. Por lo que, igualmente a fecha de hoy, podemos afirmas que no cabe recobrar o recuperar la entrada (texto original) hacia atrás, partiendo desde el checksum; y a su vez, que éste identifica de forma única a dicho texto. Hay una especie de correspondencia biyectiva o biyección entre cada entrada y salida: a cada entrada le corresponde, siguiendo el proceso funcional algorítmico o conjunto de instrucciones informáticas, un resultado único, y viceversa. Por eso, la longitud del checksum es siempre la misma y viene determinada por el *algoritmo criptográfico* utilizado para hacer el hash; es decir, está condicionada o predeterminada sin posibilidad de variación por el desarrollo de la función matemática introducida o programada para la modificación de datos del documento o de cualquier tipo de datos introducidos inicialmente (instrucciones configuradoras del algoritmo).

Establecida esta premisa, vamos a explicar las características del sistema criptográfico que se emplea en las cadenas de bloques, comenzando por las nociones de criptografía asimétrica y DLT o tecnología de registros distribuidos.

2. CRIPTOGRAFÍA ASIMÉTRICA

A diferencia de la llamada criptografía simétrica, donde solo se utiliza una clave para operar, la cual debe ser conocida por emisor y receptor para poder cifrar y descifrar un mensaje sin conocimiento o intervención de terceros, la criptografía asimétrica, que es la empleada en *blockchain* , se basa en el uso combinado, por todos los participantes en la red de nodos, de dos claves:

a) La clave pública, que se podrá difundir sin ningún problema a todas las personas que necesiten mandar algo cifrado; y

b) Una clave privada, que debe permanecer en posesión del usuario que la emplea exclusivamente, y que, por razones obvias de seguridad y como indica su denominación, no debe de ser revelada nunca; es lo más parecido a una contraseña informática para entrar en el sitio privado del usuario que previamente se ha identificado como tal.

El siguiente esquema ayuda a visualizar el uso combinado de ambas claves en la red de cadenas de bloques o en una plataforma DLT, considerando la posición relativa de los emisores y de los receptores de datos.

Cada emisor cifra o codifica un mensaje, introduciendo una clave pública. Nótese que esta clave es compartida, en el sentido de ser visible y conocida por todos. Por otra parte, el receptor del mensaje, que está al otro lado de la transacción (en el caso de DLT, en otro punto o nodo de la red), puede descifrar el mensaje que ha recibido de su interlocutor, pero solo puede hacerlo con una clave privada.

De esta manera, el emisor se ha dirigido al receptor elegido usando la clave pública del receptor para dirigirse concretamente a él y no a otro usuario del sistema; pero en cambio el mensaje que recibe este solo puede descifrarlo él (o quien este designe, en su caso), empleando una clave privada, la del propio receptor.

Esquema 1. Uso de claves en la red de cadena de bloques

Así, una persona puede cifrar información con la clave pública; pero sólo puede ser descifrada esa información por quien posea la clave privada. Pero también posee el sistema asimétrico otra característica que lo hace tremendamente útil: se puede *firmar digitalmente un documento con la clave privada,* y, además, *compartir el documento, la firma y la clave pública* . De tal manera que todos los participantes en la red pueden comprobar que esa firma corresponde a la clave privada (clave a la que está vinculada la firma, y firma que solo se puede poner usando dicha clave), que a su vez está ligada a la clave pública (pues hay un enlace o correspondencia entre la privada y la pública). Es decir, sólo aquella persona con su clave privada, correspondiente a la clave pública, ha podido firmar dicho documento. Lo cual da una seguridad extraordinaria a todos los participantes en la red o sistema DLT, que pueden confiar en la autoría de cada operación.

Por ejemplo, un notario dispone de un par de claves. La clave privada está guardada de forma segura, y la pública está publicada en su web (o firma del email). Cuando dicho notario firma digitalmente un documento, puede compartir la prueba de firma. Nadie podrá replicar, contestar u oponerse a la autenticidad de dicha prueba, al no disponer de la clave privada (salvo, naturalmente, que el notario la revelara o traspasara, lo cual sería su responsabilidad, y además puede suceder en cualquier sistema no digitalizado); pero, en cambio, y como ventaja incomparablemente superior, cualquier persona podrá en cualquier momento y sin coste, con tal que participe en el sistema o tenga acceso, comprobar que la firma es válida, sólo entrando con la clave pública.

3. «DISTRIBUTED LEDGER TECHNOLOGY» (DLT): FUNCIONAMIENTO PRÁCTICO

Ahora ya podemos explicar cómo funciona la tecnología *blockchain,* también conocida como cadena de bloques o *Distributed Ledger*

Technology (DLT). Imaginemos estar en una mesa con 20 personas, cada una con un libro de contabilidad en el que está reflejado el estado de cuentas de todo el grupo. Cuando una decide enviar una de sus propiedades o activos (dinero, inmueble, producto financiero,…) a otro de los comensales, simplemente lo comunica al grupo: «Yo (clave pública que envía) quiero enviarte x unidades (de criptomoneda, asset o *token*) a *ti* (dirección pública que recibe)».

Recibida la comunicación, todos los participantes realizan dos acciones: primero verifican la transacción, es decir que yo tengo x unidades del activo que se va a enviar, y que mi firma es correcta; para a continuación, escribir en su libro contable una nueva anotación en la que se actualiza el saldo de nuestras cuentas.

Como se ve, el sistema funciona por consenso: es decir, para que una transacción se lleve a cabo todos los miembros del grupo tienen que estar de acuerdo en la viabilidad de dicha transacción. Hay acuerdo entre todos sobre el estado de la base de datos que todos comparten.

En esencia, lo que permite una DLT o red de registro distribuido que emplee la tecnología *blockchain*, es algo a la vez muy sencillo e increíblemente potente: transmitir propiedad entre particulares sin necesidad de mediadores, testigos o terceros de confianza *(trustable third parties)* , en condiciones completamente libres *(peer to peer)* . Obviamos conscientemente, llegado este punto, las cuestiones legales y de seguridad jurídica que esta afirmación plantea, y que no son objeto de este trabajo (papel de notarios y registradores antes, durante y después de la transacción, desintermediación bancaria, sustitución o reemplazo de gestores de transacciones y otros mediadores en la contratación, por citar algunas de las más candentes).

Por otro lado, e igualmente sin entrar en consideraciones jurídicas, sabemos por experiencia física que si damos en mano un billete de 20 euros a alguien, nosotros dejamos automáticamente de tenerlo (poseerlo). Es imposible la posesión o detentación material de un activo por varias personas simultáneamente, y por eso el mundo jurídico habla de «posesión ficticia» cuando se quiere transmitir la propiedad y decir que un nuevo propietario «posee» la cosa transmitida.

En el mundo digital sucede algo parecido a lo que hemos descrito como posesión ficticia, pero con peculiaridades determinantes para la seguridad de las transacciones. Es muy fácil enviar y recibir información (*emails*, documentos música…), pero ya no es tan fácil asegurar que dicha información se destruye *en origen* cuando el destinatario la recibe; el que envía la información podría retenerla, deformarla, e incluso negociar con ella, la haya o no manipulado. Sucede, como en el mundo real, eso sí, que cuando cedemos el activo en cuestión dejamos de tener el dinero, y hemos perdido la posesión del equivalente al billete de 20 € del ejemplo anterior.

Precisamente, resolver ese problema, unificando o reuniendo la facilidad digital de envío propia de internet o del mundo digital, con la seguridad de la entrega física tradicional, es justamente lo que permite *blockchain.* Porque, en el sistema DLT, se destruye la prueba de propiedad en origen y no es posible que volver a enviar por segunda vez la misma propiedad (dinero, entradas a un concierto o acciones de una empresa).

4. REFERENCIA AL «SMART CONTRACT» Y A LA TRANSMISIÓN DE CRIPTOMONEDA

El ejemplo del contrato inteligente (*smart contract*) sirve poder entender el potencial real de la tecnología *blockchain*. El término, creado en 1995 por Nick Szabo, plantea la posibilidad de crear un *set* de promesas o compromisos (por ejemplo, los que contiene un contrato, aunque puede tratarse de otra peración) especificados de manera digital (en el caso de un contrato serían sus términos o condiciones), que incluyan *protocolos* o medidas e instrucciones automáticas, cursadas por vía digital, para la interacción de las partes involucradas en dichas promesas (en el lenguaje jurídico clásico, «promitente» y «promisario» o beneficiario de la promesa).

Podríamos definir las promesas como los contenidos materiales (en un contrato, «prestaciones») de los compromisos contraídos, es decir, de las promesas como palabra dada de la que nacen los derechos y obligaciones, conforme a condiciones consentidas por todas las partes en un contrato.

Dichas promesas, en cuanto contenido material, definen no tanto la naturaleza jurídica del contrato, su categorización o su tipología legal, sino más bien su objeto mismo, su contenido obligacional y los correlativos derechos de las partes; y sobre todo, el modo concreto en que las partes quieren llegar a su objetivo (por ejemplo, realizar un pago, entregar un activo), o, en la terminología legal, el «modo o sistema de cumplimiento», es decir, cómo se van a entregar o realizar las prestaciones.

Desde este punto de vista, la principal diferencia entre un *smart contract* y un contrato estándar tradicional, y también la primordial novedad que aporta la contratación llamada inteligente, es que en el caso de esta las instrucciones o el modo de cumplir las obligaciones viene escrito en código ejecutable automáticamente, de acuerdo con una secuencia de órdenes programadas y predeterminadas. Tales órdenes se desenvuelven operando en uno o más ordenadores.

Los derechos y obligaciones pactados se ejecutarán siempre de conformidad con esas instrucciones previamente introducidas (lo que hace difícil y costoso variar las condiciones de cumplimiento del contrato, de ahí la necesidad de programar correctamente y prever que no varíen las instrucciones). Por otra parte, el cumplimiento automatizado de tales órdenes previamente es introducidas es asegurado por el programa introducido, al menos, en una máquina. Así, el cumplimiento del contrato inteligente tiene lugar sin intervención de las partes contratantes. Solo es posible, además, realizar la ejecución una vez las partes cierren definitivamente el contenido del contrato, el modo de ejecutar las instrucciones, y realicen la programación del trato «inteligente»; generalmente, si el contrato es sencillo, lo normal es que se realicen las instrucciones de modo estándar, en forma de condiciones generales, a las que los clientes de las empresas fintech proveedoras de contratos inteligentes y de tecnología *blockchain* pueden adherirse, aunque es normal y posible que prevean instrucciones alternativas, o programen de forma distinta a la ofrecida por el proveedor de servicios tecnológicos o de tecnología financiera.

Por lo que se refiere al momento en que el contrato inteligente queda celebrado, en la práctica de la contratación inteligente se considera que el proveedor de servicios y su cliente, o en general, los contratantes, celebran la operación (o, en el lenguaje jurídico, «perfeccionan» el contrato), desde el momento en el que, previa instalación del programa (*smart contract program*,) se firma criptográficamente por las partes, comprometiéndose a la ejecución del mismo siguiendo las instrucciones.

El ejemplo más sencillo para entender cómo se celebran estos contratos se puede hallar en Bitcoin (criptomoneda o divisa criptográfica que consiste en un activo virtual basado en tecnología *blockchain*) y en una de sus características: la multifirma. Hay que entender que en *blockchain*, cualquier transacción, no se realiza entre usuarios (a través de sus monederos digitales o *wallets*). Los bitcoins no circulan de un wallet a otro, sino de un programa (un *smart contract* en su forma o versión más primitiva) a otro. Significa esto que cuando se envían Bitcoins (o cualquier otra criptomoneda, como Ethereum) lo que se hace es «instalar» un nuevo programa (con sus órdenes) en la plataforma Bitcoin. Dicho programa tiene entradas (el programa o programas anteriores que ahora guardan los bitcoins), y una serie de condiciones que definen quién y cómo se pueden gastar los fondos.

Para la comprensión más básica de este proceso debe señalarse que el programa lo que hace es *verificar la identidad del operador*. Si alguien quiere gastar las monedas digitales guardadas en el mismo, debe demostrar (firmar) que posee la clave privada correspondiente a la clave pública de destino de la transacción.

Podría crearse dicho programa para que la condición para gastar los bitcoins fuera tener múltiples firmas (y verificarlas para lograr la

ejecución del contrato inteligente que materializa el cumplimiento del contrato), por ejemplo dos de un total de cuatro. Esto se materializaría enviando, para lograr la verificación que desencadena el cumplimiento, las cuatro claves públicas, y especificando la condición de que solo verificando dos de las cuatro firmas se podrán gastar los bitcoins bloqueados en el programa.

De hecho, nunca vamos a «tener» Bitcoins; nunca hay posesión de moneda virtual. Lo que tenemos en cambio es la disponibilidad una clave privada que permite ejecutar el programa, y ésta sí «contiene» (al menos virtualmente) dichos bitcoins, para transferirlos a una nueva clave pública. Es entonces el propietario de la clave privada correspondiente a dicha clave pública quien tiene la capacidad para ejecutar este nuevo programa y transferir o transmitir (enviar de nuevo, encriptado) ese bitcoin.

5. IDENTIDAD DIGITAL EN «BLOCKCHAIN»

Si estamos de acuerdo en que hay miles de ordenadores en el mundo, con una misma copia de una base de datos distribuida (el libro mayor), se podría pensar que es un mismo ordenador global con muchos discos duros replicados. Por lo que *blockchain* sería el disco duro que gestiona dicha plataforma, y los *smart contracts* serían programas que instalo en dicho sistema operativo. La forma de interactuar con estos programas es a través de firmas digitales (claves públicas y privadas).

Tiene sentido pues, que uno de estos programas, sea en realidad una representación de nuestra identidad en *blockchain,* que nos permita interactuar con otros *smart contracts* dentro de la red o con otras identidades.

En el ejemplo anterior, los *smart contracts* gestionaban fondos y poco más. En las nuevas versiones de *blockchain* (Ethereum, Hyperldger,...) la tecnología subyacente a los *smart contract* ha evolucionado mucho, permitiendo programas *turing complete,* es decir, con un nivel de complejidad mucho más alto.

Se pueden crear programas donde el usuario da permiso a alguien para que escriba y firme información en su programa (o dicho de otra manera: identidad). Por ejemplo, tras un proceso de KYC por parte de un banco, les podríamos pedir que certifiquen el resultado en nuestra identidad en *blockchain.* Nosotros, pese a ser los propietarios de dicha identidad, no podríamos modificar nada, ya que esa información está firmada. Lo importante, es que al ir a darnos de alta a otro banco, este podría comprobar lo que el primer banco ha escrito sobre nosotros sin comprometer la privacidad, y en base a ello permitirnos el onboarding automático.

Por lo tanto, para que dicha identidad en *blockchain* sea efectiva, necesitamos un punto de conexión con el mundo físico. Es decir, necesitamos que alguien de fe de que realmente la identidad que me representa en *blockchain* coincida con mi identidad real. Una tarea que en mi opinión debería recaer en el cuerpo de notarios.

Además, no sólo identidades personales pueden ser certificadas en *blockchain,* también se pueden representar empresa, propiedades... Yo podría demostrar que soy el administrador único de mi empresa y permitir que esta u otros soportes de operaciones y contratos...

II. PROPUESTA DE UNA RED «BLOCKCHAIN» NACIONAL

Por lo tanto, la tecnología nos permite, ya a día de hoy, crear una red distribuida, y su correspondiente registro, con identidades y transacciones programables. Es llegados a este punto en el que nos preguntamos hasta qué punto es esta configuración legal; si puede tener proyección internacional la DLT, en la medida en que participan personas situadas en cualquier punto del planeta; y cuestiones conexas, como todas las referentes al cumplimiento de las leyes relacionadas con blanqueo de capital, y otras normas de supervisión administrativa.

Debemos advertir que la tecnología nos ofrece actualmente posibilidades que de momento no encajan dentro de ningún marco legal. Existen lagunas normativas, y son enormes. No estamos afirmando que sea ilegal contratar en *blockchain,* sencillamente es una materia nueva, desde el punto de vista del derecho se trata de modos de contratar *atípicos* y falta encaje de muchas de las figuras y situaciones producidas en este ámbito dentro de la regulación existente.

La solución más efectiva, que está comenzándose a desarrollar en otros países por empresarios que han tomado las riendas de nuevos mercados *blockchain,* está consistiendo, a falta de una normativa internacional, crear una red *blockchain* dentro del territorio nacional. Y no pensar en tecnología, sino en regulación local, analizando la compatibilidad de la red DLT con el marco legal existente y viendo cómo encajar la tecnología dentro de los procesos legales existentes. Una red en la cual grandes empresas y pymes puedan operar en igualdad de condiciones.

El principal reto que habrá de abordarse a continuación por quienes tengan la iniciativa de crear redes DLT y asociarse en «nodos» o puntos de conexión para operar en *blockchain,* a nuestro parecer, será la creación de *esquemas de identidad digital sobre blockchain* .

Tales esquemas deberían, para lograr eficientemente los fines de un consorcio amplio de operadores que pretendan operar en un espacio común donde desarrollar sus proyectos en *blockchain,* tener las siguientes características:

a) Apertura. Los contratos suscritos para crear redes *blockchain* han de ser acuerdos asociativos abiertos, a la medida de las necesidades de los usuarios de la red. A este efecto se pueden utilizar varias tecnologías subyacentes, por ejemplo la de la mencionada cripto-moneda Ethereum.

b) Seguridad técnica. La red tiene que garantizar, a través de sus gestores, que quienes operan en ella lo hacen con plena seguridad, lo cual viene de suyo con la propia tecnología criptográfica integrada en el sistema de empleo de claves. Además, la red ha de ser integrable con los sistemas de información disponibles actualmente.

c) Seguridad en la certificación de identidad. Dicha identidad, junto a la capacidad de realizar transacciones inteligentes (programables) permitirá un grado de optimización en los procesos de cualquier empresa jamás visto hasta hoy, lo que significa lograr muy superior eficiencia a menos coste, siempre dentro del marco legal.

d) Carácter semipúblico (o semiprivado). Se dice que una red es pública si permite el acceso universal a quienes deseen operar (como sucede en Bitcoin). En las cadenas de bloques «privadas» en cambio, el consenso para llegar a introducir datos nuevos (y hacer el siguiente eslabón de la «cadena de bloques») estaría limitado, no sería de todos los partícipes o «nodos». En el caso de una red española para prestar distintos servicios en *blockchain* para introducir datos, lo ideal sería limitar el consenso a nodos específicos, y permitir sin embargo el uso de la red a todos los nodos operantes u operativos, que realizan transacciones. Así, habría distintos niveles o tipos de nodos u operadores, y solo algunos podrían controlar el proceso de consenso, lo que no limita el carácter «distribuido» de los datos, pero sí el control de las operaciones, circunscrito a nodos o socios seleccionados.

e) Carácter «autorizado» (permissioned). La base de datos es mantenida por una o varias entidades preseleccionadas, autorizadas al efecto. También puede enviar y producir la información que se registra en la base de datos solo quien esté autorizado o facultado por el sistema. Lo mismo cabe decir del acceso a los datos, donde el grupo de nodos o participantes que pueden leer será más amplio que el grupo productor de datos, pero también puede limitarse.

f) Ausencia de ánimo de lucro: los nodos no crean valor monetario (minería), participando en el sistema por motivos de reputación. La asociación o consorcio de nodos no reparte dividendos, no es una sociedad. Sin perjuicio de que la red deba autofinanciarse para cubrir los costes de producción y almacenamiento de datos distribuidos entre los participantes autorizados o seleccionados por los creadores de la DLT semipública (o si se prefiere el término equivalente, «semiprivada».

III. CONCLUSIÓN

Estamos ante una oportunidad única para dar un salto cualitativo importante en la forma en cómo particulares y empresas se relacionan digitalmente. Gracias a *blockchain* y la distribución en redes con nodos o puntos de recepción y registro simultáneo de operaciones criptográficas contaremos con una tecnología con cuyo uso podremos identificarnos de forma segura, mantener nuestra privacidad y recuperar el control de nuestra información. Y una vez identificados correctamente, mediante el uso de claves criptográficas, será muy fácil intercambiar cualquier tipo de valor online de forma rápida y segura entre personas, empresas e instituciones. Entre otros mecanismos, a través de la programación de contratos con instrucciones de ejecución automática o *Smart*.

En el caso español, el auténtico potencial de *blockchain* empieza a desplegarse con la asociación en red de personas a través de un contrato por el que los asociados dispondremos de una plataforma abierta donde desarrollar nuevas aplicaciones y servicios, siempre dentro de un entorno regulado. Dispondremos de todos los ingredientes necesarios (seguridad, apertura, certificación digital) para que la innovación operativa sea posible a un nivel no conocido hasta ahora.

IV. BIBLIOGRAFÍA

Agrawal, A., Gans, J., & Goldfarb, A. (2017). The simple economics of machine intelligence. *Harvard Business Review,* November.

Catalini, C. (2017). How blockchain Technology Will Impact the Digital Economy. *Oxford Law Faculty Blog,* April 2017.

Chamber of Digital Commerce (2016). Smart Contracts: 12 Use Cases for Business & Beyond A Technology, Legal & Regulatory Introduction. Washington.

European Banking Authority (2014). EBA Opinion on virtual currencies. EBA/Op/2014/08, 4 July 2014.

Financial Conduct Authority (2017). Discussion Paper on distributed ledger technology. Discussion Paper DP17/3.

Green, S. (2016). Smart Contracts. *Oxford Law Faculty Blog,* February.

Harpaz, J. (2016). Will blockchain become the Internet of Finance? *Forbes,* May 31.

Luca, M. (2016). Designing online marketplaces: trust and reputation mechanisms. *NBER Working Paper Series,* 22616, September.

Preukschat, A. (2017). Los contratos inteligentes serán cada vez más complejos gracias al blockchain. *El economista,* abril.

Tapscott, D., & Tapscott, A. (2016). The impact of blockchain goes beyond Financial Services. *Harvard Business Review,* May.

UK Government Chief Scientific Adviser (2016). *Distributed Ledger Technology: beyond blockchain.*

Wardyński & Partners (2016). blockchain, smart contracts and DAO.

Wojdylo, K. (2014). Smart contracts: on approaching legal revolution. *In Principle,* July.

World Economic Forum (2016a). A blueprint for Digital Identity: the role of financial institutions on building digital identity, August.

– (2016b). The future of Financial Infraestructure: an ambitious look at how blockchain can reshape financial services, August.