Artículo doctrinal

FUNDAMENTOS DE BLOCKCHAIN

ALMUDENA DE LA MATA MUÑOZ
Directora General Blockchain Intelligence y
Blockchain Intelligence Law Institute

BLOCKCHAIN INTELLIGENCE
www.blockchainintelligence.es

ÍNDICE.

1. INTRODUCCIÓN

A lo largo de los últimos años, *Blockchain* se ha configurado como una de las tecnologías revolucionarias no sólo de nuestra economía sino también de nuestra sociedad. Esta tecnología nació con la creación de la red *Bitcoin* en el año 2008 (S. Nakamoto "Bitcoin: A Peer-to-peer Electronic Cash System"). Con ella se hizo posible por primera vez el intercambio de valor directamente entre partes desconocidas (*peer-to-peer*), sin intermediarios y de forma estrictamente digital.

Hasta entonces, internet había hecho posible el intercambio digital de datos. Sin embargo, este protocolo TCP/IP resultaba insuficiente para la transferencia de valor, que siempre había necesitado de un complejo entramado de terceros de confianza para tener lugar. Pensemos por ejemplo que, hasta la creación de la red *Bitcoin*, los pagos solo habían sido posibles gracias a un sistema en el que participan distintos intervinientes con el objeto de dar seguridad al intercambio. El protocolo *Bitcoin* creó una unidad de cuenta (el *bitcoin*) o moneda digital que podía ser intercambiada de forma prácticamente automática por las partes intervinientes en el sistema sin necesidad de bancos, sistemas de compensación y liquidación y otros terceros que dieran seguridad a esas transacciones.

2. ¿CÓMO ES POSIBLE EL INTERCAMBIO DIGITAL DE VALOR?

2.1. BLOCKCHAIN

Esta primera transacción de valor en forma digital y sin terceros de confianza se hizo posible gracias a la creación de la llamada cadena de bloques o *Blockchain*.

Blockchain es el tipo de protocolo que hace posible mantener una base de datos única pero distribuida o simultáneamente copiada en los respectivos ordenadores de los participantes de una red (nodos) de manera fiable. Esto da a cada parte acceso directo a los registros de su interés, eliminando la necesidad de intermediarios. El mantenimiento o gestión de esa base de datos se desarrolla de forma descentralizada a través de mecanismos de consenso. Además, el uso de criptografía hace posible atribuir cada uno de los registros de esa base de datos a una de las partes intervinientes, ofreciendo, a la vez, garantía de integridad del contenido.

En palabras de MANUEL GONZÁLEZ-MENESES "*es como si la contabilidad de todos los bancos en cuyas cuentas se refleja todo nuestro dinero y todas las transferencias dinerarias que vamos haciendo la llevásemos directamente todos los clientes de los bancos mediante nuestros propios ordenadores*" (M. GONZÁLEZ MENESES, "*Entender blockchain, Una introducción a la tecnología de registro distribuido*", 2017, 40).

Se trata de una innovación en el diseño de bases de datos que hace posible la contabilidad fiable de activos digitales (R. MATZUTT *et al*, "A Quantitative Analysis …", 2018). El elemento innovador se encuentra en la visión inteligente de combinar distintas tecnologías ya conocidas desde hacía incluso décadas: 1) registros digitales (*databases*), 2) redes distribuidas y 3) criptografía. Es la alquimia de esos tres elementos tecnológicos la que hace posible la magia de *blockchain*.

De esta manera, se consigue de forma distribuida y sin necesidad de terceros de confianza todo lo necesario para intercambiar valor de forma estrictamente digital, principalmente:

1) identificación del valor como un registro en la base de datos
2) atribución del valor a una parte y
3) seguridad en el intercambio (garantía de no manipulación de los datos y eliminación del doble gasto o la posibilidad de copiar un registro).

Una verdadera revolución.

2.2. ACTIVOS DIGITALES

No olvidemos que los registros compartidos y verificables de una *blockchain* no son sino datos, que representan el valor que las partes quieran atribuirle.

De esta forma surgen activos digitales; datos que representan bienes, servicios o derechos que las partes reconocen. Los activos basados en *blockchain* pueden ser estrictamente digitales, como es el caso de las criptomonedas como *Bitcoin* (los *bitcoins* no son sino datos a los que los participantes en la red atribuyen un valor) o pueden ser una representación digital de un activo real o *token*. Así podemos encontrar *tokens* de bienes físicos como inmuebles, energía o coches, *tokens* de servicios (como un vale para acceder a una plataforma o la reparación de un vehículo) o un *token* que dé acceso a un derecho (derecho de frutos sobre un activo inmobiliario, derecho de voto, etc.).

Las posibilidades de programar estos datos o activos digitales abre todo un mundo de posibilidades en la automatización del intercambio de valor y la contratación sin intermediarios a través de los llamados *Smart Contracts*. A modo de ejemplo, podemos pensar en un nuevo concepto de "dinero inteligente" en el que la unidad de cuenta sea programada para ser transmitida solo a determinadas partes o empleada para el consumo de determinados bienes o servicios.

En palabras de V. BUTERIN: "*Blockchain is a magic computer that anyone can upload programs to and leave the programs to self-execute, where the current and all previous states of every program are always publicly visible, and which carries a very strong cryptoeconomically secured guarantees that programs running on the chain will continue to execute in exactly the way that the blockchain protocol specifies*" (V. BUTERIN, Visions part I: The Value of Blockchain Technologiy, Ehereum Blog, 2015).

2.3. OPERAR SIN TERCEROS DE CONFIANZA. ELEMENTOS CONFIGURATIVOS DE UNA BLOCKCHAIN

2.3.1. Confianza distribuida

Para hacer posible el intercambio de valor entre partes que no se conocen y/o no confían entre sí, la sociedad ha ido habilitando sistemas y procesos que otorgan a las partes la suficiente garantía de que la transacción se produce de forma segura en el tiempo definido, por el valor deseado y entre las partes intervinientes. Dichos sistemas se fundamentan en la existencia de intermediarios o terceros de confianza en los que depositamos la responsabilidad de ejecutar las transacciones con las características acordadas. A su vez, dichos intermediarios son "controlados" por estructuras jurídicas, regulación e instituciones de supervisión que garantizan su buen funcionamiento. Todo ello implica, por un lado, un elevado coste social acumulado y, por otro, la confianza de las partes en la estructura de gobierno de una sociedad.

La gran revolución que supone *blockchain* es lograr la confianza en la autenticidad de las transacciones sin necesidad de esos intermediarios a través de protocolos informáticos. Las redes de registro distribuido (*Blockchains o Distribute Ledger Technologíes (DLT)*) serían "artefactos" tecnológicos que reemplazan la confianza organizativa (R. BECK et al., "Opportunities and risks of Blockchain Technologies", 2016, 119). Es decir, se sustituye la confianza en estructuras humanas o instituciones por confianza en tecnología. Así, Satoshi Nakamoto en el *whitepaper* de *Bitcoin* alude a la naturaleza descentralizada de la confianza: "*an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party*" (S. NAKAMOTO "*Bitcoin: A Peer-to-peer Electronic Cash System*"). Conviene, sin embargo, tener en cuenta que el factor humano está presente tanto en el desarrollo tecnológico como en la creación del protocolo y las decisiones de los mecanismos de consenso.

¿Cómo se consigue tecnológicamente el servicio que hasta ahora vienen realizando con éxito los actuales intermediarios en la cadena de transferencia de valor? Tomemos como ejemplo representativo el funcionamiento de la *Blockchain Bitcoin*.

2.3.2. Base de datos

Bitcoin es el protocolo que sustenta una base de datos de registros que se agrupan en bloques vinculados de forma secuencial y con marca de tiempo formando una cadena.

Cada bloque guarda información sobre transferencias de *bitcoins* de un miembro de la red a otro, junto con otra información que puede ser vinculada a cada transacción (imágenes, texto, archivos…).

Cada bloque tiene un encabezado con la función de organizar la base de datos. En este encabezado se incluyen una huella única (*hash*) de todas las transacciones contenidas en ese bloque junto con la huella temporal (*timestamp*) y el *hash* del bloque anterior. Este sistema de *hasheado* enlazado hace visible una potencial manipulación del contenido de los bloques, siendo, en parte, la garantía de integridad de los datos introducidos en el registro.

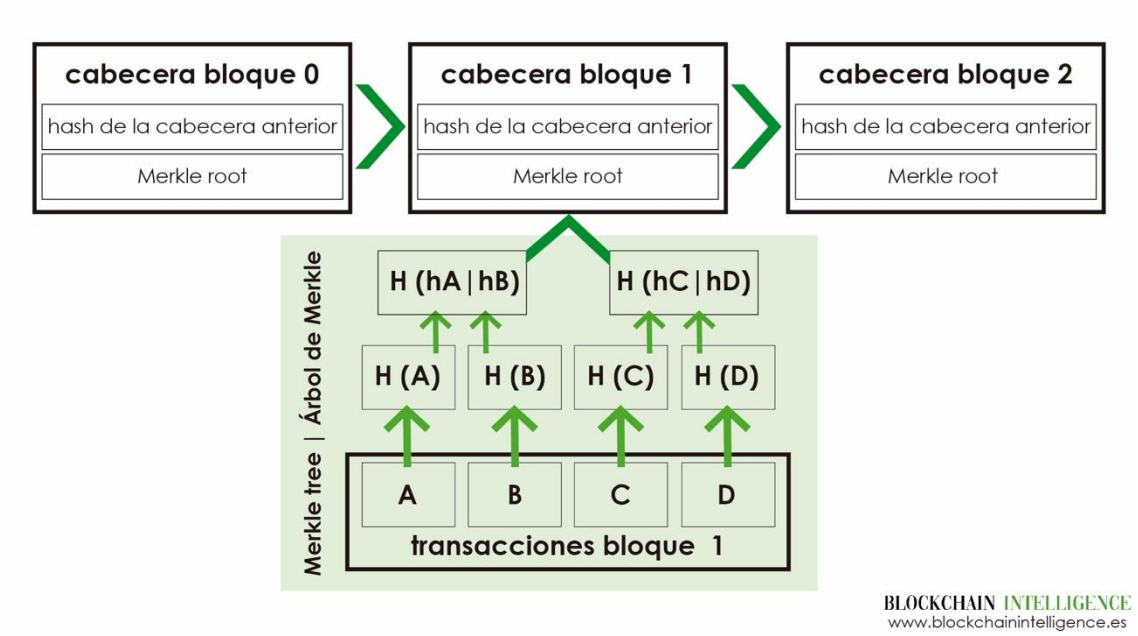

Imagen 1. Estructura de bloques en blockchain (elaboración propia)

Los *hashes* se generan usando funciones criptográficas de *hash* estándar que permiten representar cualquier tipo de información, como las transacciones de un bloque, en una línea de caracteres y números que se asocian de forma univoca con las transacciones de ese bloque (Lawrence Carter and Wegman, "*Universal Classes* (…)", 1979, 143-154).

A través de un *Merkel Tree* o *Hash* de los *hashes* de las transacciones contenidas en el bloque podemos hacer una gestión eficiente de los datos. ("*Each block has a block header, a hash pointer to some transactiondata and a hash pointer to the prvious block in the sequence. The second data structure is a pe-block tree of all of the transactions that are included in that block. This is a Merkle tree and allows us to have a digest of all the transations in the block in an efficient way*". NARAYANAN et al., "Bitcoin and Cryptocurrency Technologies" 2016.)

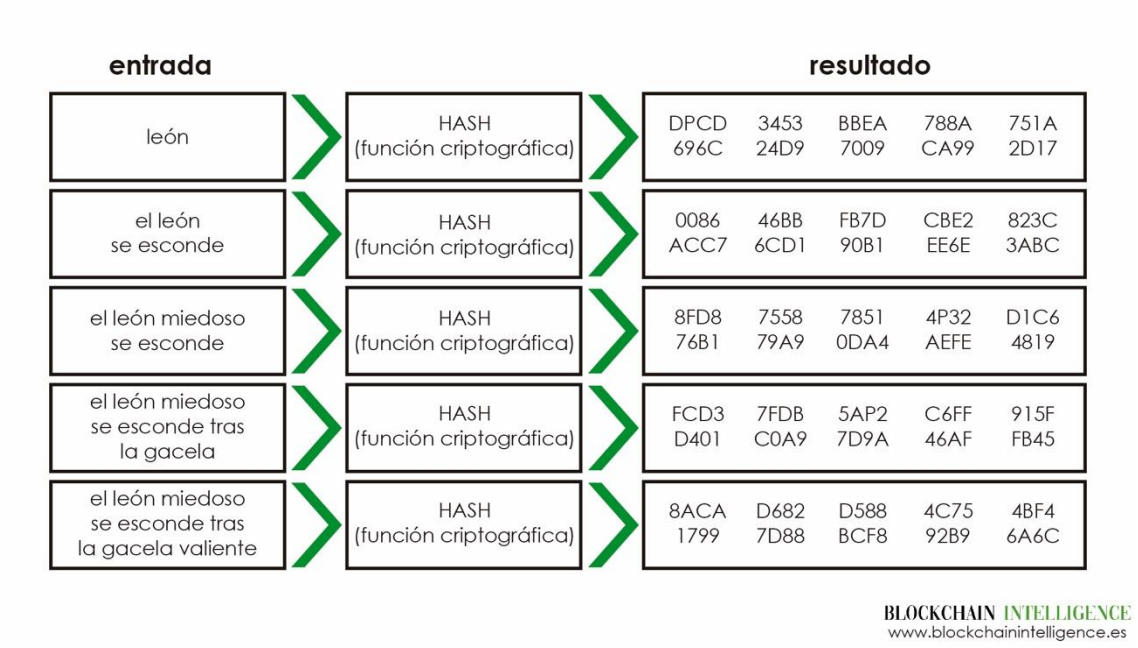

Figura 2. Función Hash (elaboración propia)

La información contenida en el encabezado a través, en parte, de las funciones *hash*, permite estructurar el contenido de la *blockchain* y acceder a él con más rapidez. Sería algo similar a la función del índice y la numeración de las páginas en un libro.

2.3.3. Distribución

Cuando el registro de datos se replica en los distintos nodos, se construye una estructura descentralizada (si la gobernanza de la red es también descentralizada).

Frente al modelo tradicional en el que los intermediarios mantienen los datos guardados en sus propias bases centralizadas, *blockchain* se configura como registro distribuido entre los distintos nodos de la red. Cada nodo mantendrá una copia exacta de la base de datos y contribuirá a la garantía de autenticidad del registro. De esta forma también cada nodo tiene acceso al contenido del registro sin tener que fiarse de un tercero.

Las ventajas de los registros distribuidos son claras. Por un lado, se reduce el poder del responsable del registro que podría, por ejemplo, modificar el contenido del mismo o denegar su acceso (en una red distribuida no existe un único tercero responsable de la gestión de los datos, con el riesgo que eso supone de fallos en la administración y posibilidades de manipulación del contenido de la base de datos). También se reducen riesgos de ataques o *hackeos* derivados de un único punto de fallo ("*single point of failure*") en la red.

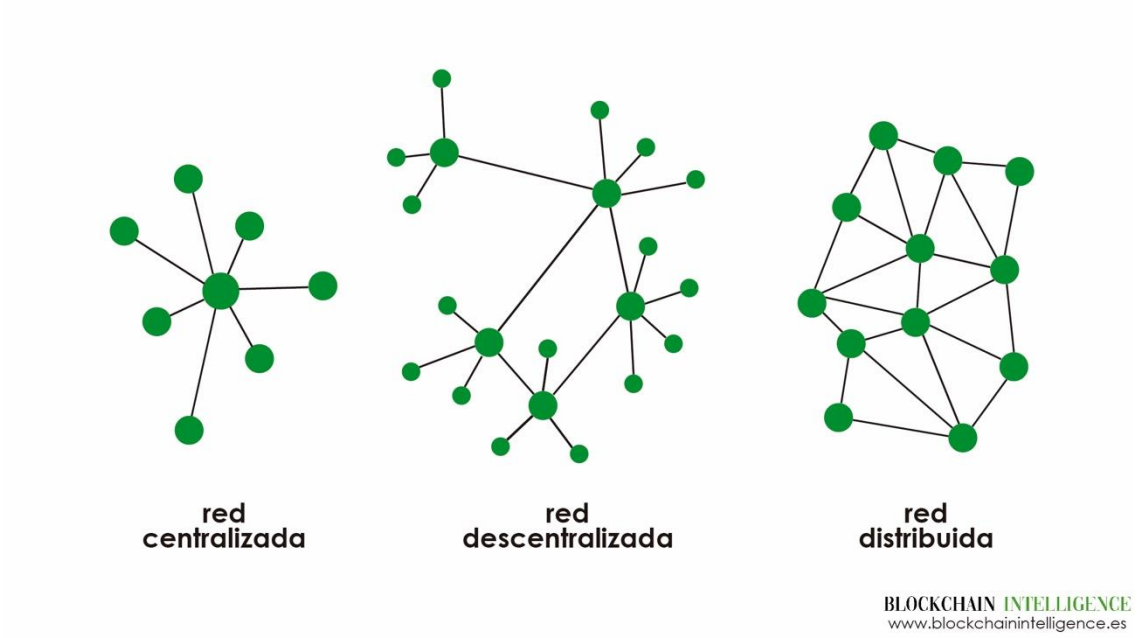

Figura 3. Redes distribuidas frente a redes descentralizadas y centralizadas (elaboración propia)

Conviene alertar, a la luz de la amplia gama de *blockchains* o DLTs que se han ido generando en los últimos años, de que no todas presentan características de diseño que permitan considerarlas redes distribuidas con los beneficios que se predican de *blockchain* (principalmente inmutabilidad). Si la red está compuesta por un número reducido de nodos o los sistemas de consenso son débiles o contienen algún tipo de centralización, no podremos decir que el contenido de esa *blockchain* es inmutable.

También se presentan retos en relación con las redes distribuidas. Algunos autores consideran en principio las *blockchains* menos eficientes por diseño que las bases de datos centralizadas (M. FINK, "Blockchain Regulation and Governance in Europe", 2019, 19) (especialmente en términos de sostenibilidad por consumo de energía). La naturaleza multinacional de las *blockchains* (especialmente las públicas) presenta cuestiones de índole jurisdiccional no siendo fácil definir el Derecho aplicable ni la adjudicación de responsabilidades a las partes intervinientes (M. FINK, M. "*Blockchain Regulation and Governance in Europe*", 2019, 182 y ss y producción académica de A. WALCH). Por otra parte, el entorno regulatorio actual está diseñado para redes centralizadas, siendo difícil su encaje y aplicación a entornos descentralizados. Es el caso por ejemplo del nuevo Reglamento General de Protección de Datos de la UE basado en un paradigma de control de las bases de datos por terceros identificados (bases de datos centralizadas). Pensemos que el origen criptoanarquista de *blockchain* (*Bitcoin*) parte de la idea de crear un sistema autónomo, autosuficiente y desvinculado de cualquier poder jurisdiccional. La frase "*Code is law*" refleja esta visión (criptoanarquista) en la que el acuerdo de las partes y su definición a través de código de programación autoejecutable haría innecesaria la aplicación de la ley y la existencia de un sistema jurisdiccional de resolución de conflictos. Sin embargo, la generalización del uso de *blockchain* en aplicaciones comerciales y sociales por empresas y personas que operan en el sistema institucional actual cumpliendo con la normativa vigente, hace necesaria la aplicación del Derecho a esta nueva realidad.

2.3.4. Consenso

El consenso garantiza que las transacciones registradas en la red son "válidas", contribuyendo a hacer en principio superflua la necesidad de intermediarios. Los protocolos de consenso garantizan la consistencia entre las distintas copias de un registro que se guardan en cada uno de los nodos de la red. Se consigue consenso cuando el protocolo puede asegurar que todos los nodos añaden los mismos nuevos bloques (con el mismo contenido) en su versión local de la *blockchain*. El hecho de que todos los participantes respeten las normas definidas en el protocolo para decidir cómo actualizar la base de datos, es la fuente de confianza en el sistema (M. FINK, "Blockchain regulation and governance in Europe, 2019, 20).

Para que los nodos acepten nuevos bloques, estos tienen que haber sido generados por mineros o nodos validadores, de acuerdo con el protocolo de consenso de cada red. Cuando un usuario de la red envía una transacción, esta se remite a los nodos para iniciar el proceso de registro y hacer posible la operación. Los mineros agrupan la transacción en un bloque junto con otras y la envían a la red. La ejecución de este servicio reporta beneficios (en el caso de *Bitcoin*, reciben el pago por bloque en *bitcoins* y las "propinas" que los usuarios pueden añadir a su transacción para incentivar el procesamiento más rápido de su operación). Sólo algunos nodos participaran en el minado (los mineros) pero todos los nodos participan en la validación de los nuevos bloques, contribuyendo a la distribución del nuevo bloque a los otros nodos, en su caso.

Cada *blockchain* define su mecanismo de consenso. En la actualidad existen múltiples protocolos. *Proof of work* es el más utilizado en redes públicas como *Bitcoin* y Etherium pero las dificultades que presenta han llevado a la propuesta de nuevos mecanismos de consenso como *Proof of Stake, Proof of Burn o Proof of Excellence* (C. PÉREZ SOLÁ, y J. HERRER-JOANCOMARTÍ, "Bitcoins y el problema de los generales bizantinos", 2014, 245).

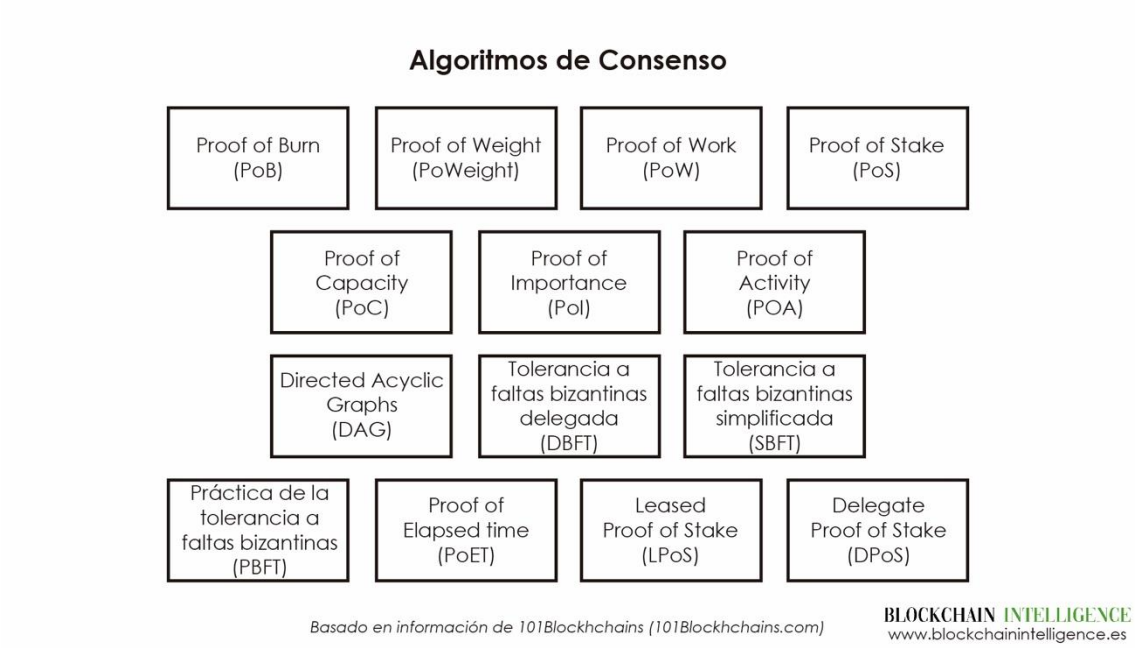

Figura 4. Algoritmos de consenso (elaboración propia basada en información de 101 Blockchains)

En todos los casos, se trata de generar incentivos (económicos) a las partes para realizar el trabajo de validación dentro de esa comunidad de la red y a la vez garantizar el acuerdo de todos los participantes sobre la validez de los datos incluidos en ese registro (dificultando cualquier intento de manipulación). En las redes privadas pueden darse otro tipo de estructuras de consenso e incentivos, incluso sin minado. Por ejemplo, existen *blockchains* privadas en las que determinados nodos se comprometen contractualmente a validar transacciones aplicando un mecanismo de rotación, de forma que se garantiza la contribución de todos los nodos a la tarea pero no simultáneamente, evitando gasto energético excesivo.

El análisis de los mecanismos de consenso es muy relevante a la hora de elegir una *blockchain* sobre la que desarrollar aplicaciones o realizar transacciones porque de ellos depende en gran medida que sea verdad la tan refererida "inmutabilidad" que suele predicarse de la tecnología *blockchain*. Si en una *blockchain* privada tenemos pocos nodos validadores y/o los intereses o incentivos de algunos de estos nodos están muy alineados, se diluirá de forma incluso definitiva el carácter "inmutable" de los registros. Se plantean retos similares en los entornos de *blockchain* pública por la concentración geográfica de mineros o nodos con posibles intereses comunes.

2.3.5. Autenticación

Otro elemento importante en el uso de *blockchain* para el intercambio de valor es la posibilidad de vincular transacciones con usuarios. De esa manera podremos saber quién ha transferido un activo digital a quién. La criptografía asimétrica hace posible esta función de autenticación. El sistema genera pares de claves vinculadas: una pública (puede ser conocida por todos) y otra privada (sólo conocida por una parte). Lo que cifra una solo lo puede descifrar la otra. Si el dueño de una clave privada envía un mensaje, cualquier persona con la clave pública vinculada podrá descifrar el mensaje. Esta acción es lo que se considera la firma electrónica y permite comprobar el origen fidedigno de un mensaje o transacción. La efectividad de los algoritmos asimétricos depende de funciones matemáticas de un solo sentido, que requieren relativamente poca potencia de cálculo para ejecutarse, pero muchísima potencia para calcular la inversa.

Para enviar un mensaje seguro a una persona, éste se codifica con la clave pública del destinatario. El sistema garantiza que el mensaje resultante sólo puede ser descodificado con la clave privada del destinatario. Dado que se tiene la certeza de la identidad de dicho destinatario gracias a su clave pública, aseguramos que el mensaje llega al destinatario correcto. De este modo se consigue autenticación garantizando confidencialidad.

Dependiendo de la *blockchain* se utilizarán sistemas de pseudoanonimato de manera que las transacciones se puedan acceder a través de sistemas criptográficos de clave pública y privada sin necesidad de conocer la identidad detrás de dichas claves, pero pudiendo vincular la transacción a un solo usuario.

Este fue un elemento distintivo y clave en las *blockchains* públicas, cuyo origen y fundamento vinculado a la filosofía criptoanarquista tenía como uno de sus objetivos principales generar un sistema de intercambio garantizando la privacidad de las personas, evitando la dependencia de sistemas institucionales y de grandes compañías controladoras de los datos. El manifiesto criptoanarquista declara que la combinación de protocolos criptográficos y encriptación haría posible la revolución socio-económica y alteraría completamente la naturaleza de la regulación del gobierno, el poder fiscal y control de las interacciones económicas, la capacidad de mantener secreta la información e incluso alteraría la naturaleza de la confianza y la reputación (M. FINK, 63). Si bien esta garantía de privacidad tiene claros beneficios iniciales en términos de libertad individual, presenta también riesgos de uso fraudulento o criminal. Además, limita el uso generalizado y no estrictamente "cripto" al hacer difícil la combinación de este

mundo virtual con estructuras sociales preexistentes como pueden ser las judiciales. Pensemos que *bitcoin* es *per se* inembargable precisamente porque es imposible acceder a los *bitcoins* sin la colaboración de la persona a cuya clave privada se vinculan (a diferencia del dinero FIAT, custodiado generalmente por entidades bancarias sometidas al cumplimiento de una orden judicial).

La criptografía asimétrica hace posible operar en determinadas *blockchains*, por ejemplo *Bitcoin*, de forma pseudoanónima. Las claves privadas nos permiten acceder a nuestros registros y por tanto poder operar con nuestras criptomonedas sin necesidad de desvelar otros elementos de nuestra identidad real (nombre, biometría, número de pasaporte, etc.).

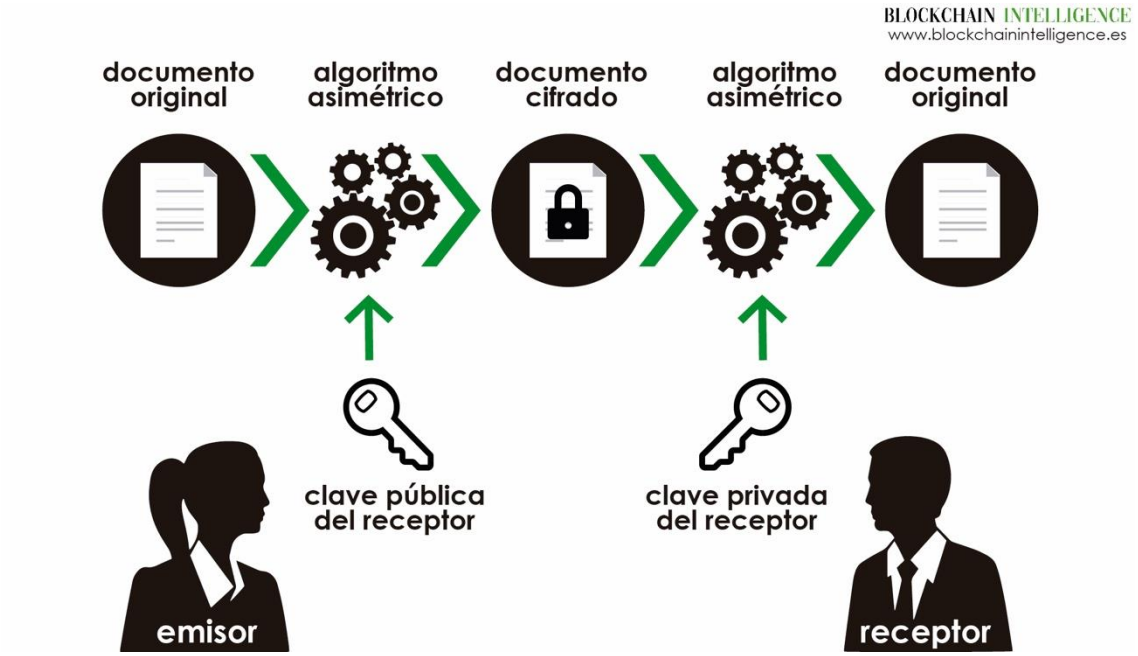

Figura 5. Elaboración propia

Otras *blockchains* (privadas o permisionadas) pueden vincular las claves privadas con identidades "reales" o institucionales.

3. TIPOS DE BLOCKCHAIN Y SUS FUNCIONALIDADES

3.1. BLOCKCHAINS PÚBLICAS VS BLOCKCHAINS PRIVADAS

Bitcoin hizo posible por primera vez el intercambio de valor entre desconocidos a través de internet, creando la primera *blockchain*. Esta *blockchain*, el protocolo, incorporaba determinadas características (en parte referidas arriba). Se trata de una red pública (se puede consultar por cualquier persona aunque no forme parte de la red), de acceso abierto sin condiciones, descentralizada (varios participantes conectados gracias a un protocolo común, generan el consenso y "operan" la red entre todos) y pseudónima (no es necesario identificarse para participar porque se puede colaborar con claves pública y privada). Desde entonces se han ido desarrollando multitud de otras *blockchains* cada una con sus características (número de nodos, gobernanza y normas de participación, mecanismo de consenso, definición de responsabilidades, etc.). Algunas de ellas son de naturaleza abierta, "*blockchains* públicas", otras son "*blockchains* privadas" y otras son "*blockchains* públicas permisionadas".

3.2. BLOCKCHAINS PÚBLICAS

Las *blockchains* públicas, como *Bitcoin*, son aquellas cuya participación es abierta y libre. El protocolo está basado en código abierto y cualquier persona puede descargarlo en su ordenador y participar en la cadena. Esta naturaleza hace necesario que los mecanismos de consenso incluyan incentivos económicos para que algunos participantes en la red se decidan a realizar el trabajo de validación (que supone elevados costes energéticos derivados del trabajo de cálculo vinculado en el caso de uso de *Proof of Work* como protocolo de consenso). Es la forma de conseguir que el sistema funcione sin controles, de forma descentralizada y sin obligar a los participantes a mantenerse en la red durante un tiempo determinado. Recordemos que los nodos de las redes públicas, lo son porque han decidido en un momento, libremente y sin previo aviso o autorización ser parte de la red. Asimismo, dejan de ser nodos cuando eliminan el *software* de su ordenador.

Como hemos visto, el funcionamiento de estas redes se basa en la combinación de criptografía e incentivos basados en teoría de juegos, dando lugar a lo que se ha dado en llamar "criptoeconomía" y permitiendo el desarrollo de sistemas descentralizados en los que el mantenimiento del registro se realiza entre los participantes, sin entidad central de control responsable y de forma pseudónima. (V. BUTERIN

define criptoeconomía como "*any descentralised criptographic protocol that uses economic incentives to ensure that it keeps going and does´nt go back in time or incur any glitch*", V. BUTERIN, Visions, Part I, *The value of blockchain technology*, 50).

3.3. BLOCKCHAINS PRIVADAS

Las *blockchains* privadas son aquellas en las que la participación se define entre los miembros o los originadores de forma privada. Las partes intervinientes definirán los requisitos para formar parte de la red y la gobernanza de la misma. Entre otros elementos se deberán definir los mecanismos de adaptación del protocolo en caso de necesidad o conveniencia tecnológica, número mínimo de nodos, mecanismos de consenso, previsión en caso de desaparición de la red, responsabilidad de los intervinientes, nivel de identificación de los participantes, etc. La definición de estos elementos, harán apta esa *blockchain* o DLT para determinados usos y de ellos dependerá la robustez y fiabilidad de cada *blockchain* como mecanismo de garantía de registro, en principio, inmutable.

3.4. BLOCKCHAINS PÚBLICAS PERMISIONADAS

Por último, las *blockchains* públicas permisionadas son un tipo de *blockchain* en las que las partes definen las características y requisitos de participación y gestión, pero cualquier parte que cumpla con las condiciones predefinidas podrá participar en esa red.

4. IMPACTO DE BLOCKCHAIN EN LOS NEGOCIOS, LA ECONOMÍA Y LA SOCIEDAD

4.1. BLOCKCHAIN EN LA INDUSTRIA: EFICIENCIA Y NUEVOS MODELOS

Blockchain dota, en principio, de confianza a las relaciones entre partes que no necesariamente confían entre sí. La posibilidad de trabajar con registros fiables, así como de digitalizar activos y programar su uso a través de *Smart Contracts*, automatizando su transferencia y eliminando intermediarios, abre un enorme abanico de posibilidades en el desarrollo de las relaciones humanas y comerciales. Estas posibilidades afectan a todos los sectores productivos (sistema financiero, logística, gestión de propiedad intelectual, turismo, administración pública, manufacturas, seguros, *compliance*, auditoría, supervisión, educación y recursos humanos, etc.) y tienen aplicaciones en distintos estadios de la cadena de valor (tanto *back-office* como *front-office*).

A más corto plazo, *Blockchain* se presenta como la tecnología que facilita el ahorro de costes y mejora de la eficiencia. A más largo plazo, se plantea la posibilidad de desarrollo de nuevos modelos de negocio (en parte descentralizados) que pueden ser tan disruptivos como los vividos recientemente en la era internet (pensemos como ejemplo en la posibilidad de desarrollar sistemas de navegación GPS descentralizados en los que un *software* recibe los datos anonimizados de los participantes y genera el servicio que hoy en día ofrecen empresas centralizadas). Uno de los grandes beneficios del uso de *blockchain* es que genera una capa de interoperabilidad entre partes distintas por encima de los sistemas tecnológicos de cada parte. El hecho de que el protocolo esté diseñado para que los nodos se comuniquen, presenta grandes oportunidades de automatización de procesos entre operadores distintos (como la posibilidad de automatizar y abaratar los pagos internacionales que hoy en día necesitan algún proveedor de pagos, como SWIFT como sistema común de conexión entre bancos, y complejos mecanismos de liquidación interbancaria).

El sector financiero fue uno de los primeros en abordar la tecnología *blockchain*. La carrera por la digitalización y gestión del cambio derivadas de la crisis financiera por un lado y las amenazas generadas por nuevos participantes en el mercado (*fintechs* y *big techs*) han favorecido el abordaje de nuevas tecnologías por las entidades financieras más tradicionales. Por otro lado, se ha desarrollado un tejido *fintech* de aplicaciones *blockchain* y más recientemente las grandes empresas tecnológicas han lanzado criptomonedas y otros productos financieros basados en esta tecnología. El poder disruptivo de *blockchain* es muy intuitivo para gran parte de la actividad financiera

tanto en *front office* como en *back office* y actividad supervisora. Por un lado, se presentan oportunidades, ya en mercado, en la generación de nuevos servicios o el abaratamiento de productos actuales como los pagos, servicios de *trade finance* como la carta de crédito (donde el peso administrativo y la confianza entre bancos es esencial), emisiones de bonos o préstamos con mayor seguridad y agilidad. Desde la perspectiva de la gestión interna (*back office*) y uso de la tecnología en el entorno supervisor/regulador (*regtech/suptech*), es claro el potencial de agilización y mejora de procesos de cumplimiento normativo y auditoría, desarrollo de DAOs, votos digitales, así como las posibilidades de establecer sistemas de control más automatizados por el supervisor que puede tener acceso directo a las informaciones relevantes sin necesidad de acceder a través de la propia entidad supervisada.

Las posibilidades de desarrollo del sector asegurador a través del uso de *Smart Contracts* es otro de los grandes campos de desarrollo de aplicaciones. Por otra parte, el ámbito industrial y empresarial se presenta como el gran beneficiario de esta tecnología por las posibilidades de mejora de la gestión de la cadena de distribución, logística y los negocios desarrollados de forma colaborativa o multiparte.

Ha surgido una importante corriente de creación de consorcios de grandes y medianas empresas con el objetivo de crear *blockchains* con las características más adaptadas a sus propósitos comerciales, compartiendo los costes de infraestructura para luego competir en el entorno de aplicaciones.

4.2. Apoyo institucional al desarrollo de la tecnología blockchain

Los retos tecnológicos del uso de la tecnología *blockchain* se unen a los regulatorios y jurídicos. Sin embargo, la involucración institucional en el apoyo al desarrollo de esta tecnología hace pensar que tanto la interpretación de la normativa actual como futuros desarrollos tratarán de favorecer la adopción de esta tecnología. Cabe mencionar especialmente la labor de la Unión Europea con iniciativas como el Observatorio *Blockchain*, INATBA, su participación en el *European Blockchain Partnership* y la inversión de programas Horizonte 2020 relacionados con tecnología *Blockchain* (como el proyecto *Blockcers*). Autoridades regulatorias también han trabajado sobre la adaptación de la regulación y supervisión de determinados fenómenos, productos o mercados que han surgido como consecuencia del uso de *Blockchain*. Por ejemplo, la *European Securities and Markets Authority* -ESMA- ha publicado un documento en el que trata la aplicación a los criptoactivos de la normativa relativas a mercado de valores

(https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf).

Por su parte, la *European Banking Authority* -EBA- en su informe de 9 de enero de 2019 (https://eba.europa.eu/documents/10180/2545547/EBA+Report+on+crypto+assets.pdf) aborda también el tema de los criptoactivos desde la perspectiva de la aplicación de la normativa financiera como la relativa al dinero electrónico, servicios de pago, prevención de blanqueo de capitales y otras normativas aplicables a instituciones de crédito).

Grupos de trabajo están reflexionando sobre la adecuada aplicación de normativa europea a este nuevo fenómeno. Un ejemplo es el esfuerzo que varios grupos realizan sobre la aplicación del Reglamento General de Protección de Datos a la realidad *blockchain* [el art. 29 Working Party, Opinion 04/2014 on Anonymisation Techniques, 0829/14/EN, 20 llegó a la conclusión de que los datos transaccionales encriptados con procesos de *hashing* podrían considerarse datos personales de acuerdo con el Reglamento de Protección de Datos (GDPR)+.

4.3. Blockchain para la administración y el desarrollo

Cabe también destacar el interés y actividad por parte de las administraciones públicas por el potencial uso de *blockchain* tanto para la mejora de su propia gestión como en relación con los administrados (evolución de la identidad digital pública, introducción de *blockchain* en los procesos de licitación pública, etc.). En este marco, destacamos también la actividad de los bancos centrales en el desarrollo de moneda digital de Banca Central con tecnología *blockchain*. Podemos esperar que estos desarrollos potencien y faciliten el uso de la tecnología *blockchain* en la industria. Por otra parte, la naturaleza digital y descentralizada convierte a *Blockchain* en una tecnología muy interesante desde la perspectiva del desarrollo, pudiendo ser un elemento impulsor de la inclusión social, especialmente en países con baja confianza institucional o menos estructuras sociales capaces de dar acceso equitativo a servicios y productos. Por ejemplo, finanzas inclusivas. Esta es la razón por la que la mayoría de las instituciones multilaterales de desarrollo están trabajando en el potencial uso de la tecnología *blockchain* para el cumplimiento de sus objetivos (Naciones Unidas, Banco Interamericano de desarrollo, Banco Europeo de Inversiones, entre otras).

4.4. Blockchain y la economía descentralizada

Además de las posibilidades de transformación de la industria, *blockchain* es por excelencia la tecnología capaz de desarrollar la economía descentralizada porque hace posible el intercambio con efectos patrimoniales entre particulares que no se conocen (economía P2P) y favorece el desarrollo de la economía colaborativa.

4.5. Blockchain y una nueva sociedad

El impacto de las nuevas tecnologías, como *blockchain* entre ellas, en las actuales estructuras sociales, es claro y capital. Es ineludible el abordaje de retos vinculados con su adopción como el desarrollo del futuro del trabajo, el riesgo de control social, el impacto geopolítico o el impacto medioambiental. Es crítico el diseño de estructuras que garanticen que el impacto de la tecnología en nuestro modelo de sociedad está alineado con los valores de consenso que vertebran nuestra convivencia.

REFERENCIAS

BECK, R. ET AL., OPPORTUNITIES AND RISKS OF BLOCKCHAIN TECHNOLOGIES, 2016, DAGSTUHL REPORTS 99, 119.

BUTERIN V., VISIONS PART I: THE VALUE OF BLOCKCHAIN TECHNOLOGIY, EHEREUM BLOCK, 13 ABRIL 2015. 50 [HTTPS://BLOG.ETHERIUM.ORG/2015/04/13/VISIONS-PART-1-TH-VALUE-OF-BLOCKCHAIN-TECHNOLGY/] "BLOCKCHAIN IS A MAGIC COMPUTER THAT ANYONE CAN UPLOAD PROGRAMS TO AND LEAVE THE PROGRAMS TO SELF-EXECUTE, WHERE THE CURRENT AND ALL PREVIOUS STATES OF EVERY PROGRAM ARE ALWAYS PUBLICLY VISIBLE, AND WHICH CARRIES A VERY STRONG CRYPTOECONOMICALLY SECURED GUARANTEES THAT PROGRAMS RUNNING ON THE CHAIN WILL CONTINUE TO EXECUTE IN EXACTLY THE WAY THAT THE BLOCKCHAIN PROTOCOL SPECIFIES".

DE FILIPI, P. WRIGHT, A., "BLOCKCHAIN AND THE LAW. THE RULE OF CODE", CAMBRIDGE MASSACHUSSETTS, HARVARD UNIVERSITY PRESS, 2018, 33 Y SS.

DOMBROVSKI, V. [HTTP://EUROPA.EU/RAPID/PRESS-RELEASE_SPEECH-18-1242_EN.HTM] ("PARA MANTENER LA COMPETITIVIDAD, EUROPA DEBE APOYAR LA TECNOLOGÍA [BLOCKCHAIN]").

FINK, M. "BLOCKCHAIN REGULATION AND GOVERNANCE IN EUROPE", CAMBRIDGE, CAMBRIDGE UNIVERSITY PRESS, 2019, 19, 20, 63, 182 Y SS.

GONZÁLEZ MENESES, M., ENTENDER BLOCKCHAIN, UNA INTRODUCCIÓN A LA TECNOLOGÍA DE REGISTRO DISTRIBUIDO, ARANZADI, 2017, 40.

GÓMEZ DE LA CRUZ, A., "ANÁLISIS SOBRE LA REGULACIÓN DE CRIPTOACTIVOS EN EUROPA", [HTTPS://GALLERY.MAILCHIMP.COM/56C5FD402137885A0463B5950/FILES/907B3982-A834-4212-9EDC-D7FF4A50E8AD/ESMA_EBA_INFORME_4_.PDF?MC_CID=FC57AECE4F&MC_EID=5C9461E56C]

LAWRENCE CARTER AND WEGMAN, "UNIVERSAL CLASSES OF HASH FUNCTIONS", JOURNAL OF COMPUTER AND SYSTEM SCIENCE 18, NO. 2, 1979, 143-154.

MATZUT R. ET AL, "A QUANTITATIVE ANALYSIS OF THE IMPACT OF ARBITRARY BLOCKCHAIN CONTENT ON BITCOIN", 26 FEB. 2018 [HTTPS://FC18.IFCA.AI/PREPROCEEDINGS/6.PDF].

NAKAMOTO, S. (PSEUDÓNIMO), "BITCOIN: A PEER-TO-PEER ELECTRONIC CASH SYSTEM",

[HTTPS://BICOIN.ORG/BITCOIN.PDF] ("AN ELECTRONIC PAYMENT SYSTEM BASED ON CRYPTOGRAPHIC PROOF INSTEAD OF TRUST, ALLOWING ANY TWO WILLING PARTIES TO TRANSACT DIRECTLY WITH EACH OTHER WITHOUT THE NEED FOR A TRUSTED THIRD PARTY").

PÉREZ SOLÁ, C. Y HERRER-JOANCOMARTÍ, J. "BITCOINS Y EL PROBLEMA DE LOS GENERALES BIZANTINOS", RECSI 2014, 2-5 SEPTIEMBRE 2014, 245.

WALCH, A. "IN CODE(RS) WE TRUST: SOFTWARE DEVELOPERS AS FIDUCIARIES IN PUBLIC BLOCKCHAINS REGULATING BLOCKCHAIN", EN "TECHNO-SOCIAL AND LEGAL CHALLENGES", ED. PHILIPP HACKER, IOANNIS LIANOS, GEORGIOS DIMITROPOULOS & STEFAN EICH, OXFORD UNIVERSITY PRESS, 2019. TAMBIÉN DISPONIBLE EN: [HTTPS://PAPERS.SSRN.COM/SOL3/PAPERS.CFM?ABSTRACT_ID=3203198].

INFORMES DE AUTORIDADES PÚBLICAS Y REGULACIÓN:

REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS, REGULATION (EU) 2016/679 ON THE PROTECTION OF NATURAL PERSONS WITH REGARD TO HTE PROCESSING OF PERSONAL DATA AND ON THE FREE MOVEMENT OF SUCH DATA, 2016, OJ L 119/1.

ART. 29 WORKING PARTY, OPINION 04/2014 ON ANONYMISATION TECHNIQUES, 0829/14/EN, 20.

DOCUMENTO DE LA EUROPEAN SECURITIES AND MARKETS AUTHORITY -ESMA- SOBRE LA APLICACIÓN A LOS CRIPTOACTIVOS DE LA NORMATIVA RELATIVAS A MERCADO DE VALORES [HTTPS://WWW.ESMA.EUROPA.EU/SITES/DEFAULT/FILES/LIBRARY/ESMA50-157-1391_CRYPTO_ADVICE.PDF].

INFORME DE LA EUROPEAN BANKING AUTHORITY -EBA- DE 9 DE ENERO DE 2019 [HTTPS://EBA.EUROPA.EU/DOCUMENTS/10180/2545547/EBA+REPORT+ON+CRYPTO+ASSETS.PDF]