

CAPÍTULO 10

INTERNET DE LAS COSAS Y *BLOCKCHAIN*: INTEGRACIÓN

INTRODUCCIÓN

Blockchain es una tecnología que ha comenzado a tener gran influencia significativa en el Internet de las cosas, mejorando la seguridad y potenciando la incorporación de un número creciente de dispositivos fiables al ecosistema de IoT. Las mejoras en la seguridad de los dispositivos de IoT facilitan la adopción más rápida de esta innovación revolucionaria y abrirá una amplia gama de posibilidades a las organizaciones y empresas en el futuro inmediato. *Blockchain* junto con las otras grandes tendencias que se han ido viendo en la obra, como Big Data e inteligencia artificial convergen en IoT y se ha convertido en una herramienta clave para la seguridad del Internet de las cosas y el Internet industrial de las cosas.

Ya existen bastantes plataformas de *blockchain*, algunas de ellas muy reconocidas como Hyperledger y Ethereum que están potenciando la integración con Internet de las cosas, creando nuevos modelos de negocios, y apoyándose en tecnologías específicas como *smart contracts* (contratos inteligentes), aplicaciones descentralizadas y en aplicaciones de gran eficacia en numerosos sectores agrícolas, financieros, seguros como la trazabilidad.

10.1. *BLOCKCHAIN* (CADENA DE BLOQUES): LA NUEVA REVOLUCIÓN DE INTERNET

Los orígenes históricos de la tecnología *blockchain* datan de la década de los ochenta, aunque fue a finales de los noventa, cuando empezó a desarrollarse materialmente en forma

embrionaria¹. En 1998, Nick Szabo describió un sistema de pago basado en el uso de técnicas criptográficas para facilitar la generación de unidades de valor virtual de forma estructurada, en un sistema conocido como *proof-of-work* (prueba de trabajo).

En 2008, Satoshi Nakamoto², una persona u organización misteriosa, cuya personalidad física se desconoce, publica un artículo de ocho páginas, donde propone una solución técnica para realizar transacciones entre dos agentes sin la necesidad de contar con una tercera parte con autorización que actuase como entidad validadora de la transacción.

Este documento se basó en investigaciones anteriores relacionadas con la prueba del trabajo y la criptografía, y lo combinó con el concepto de libro mayor virtual *virtual ledger* (es decir, la tecnología del libro mayor distribuido, *distributed ledger*) que registra las transacciones y facilita la transferencia de monedas virtuales de un usuario a otro. Una aplicación de esta tecnología de código abierto fue desarrollado y lanzado por Satoshi Nakamoto, en 2009, y se materializó en 2009 con el nacimiento de la red Bitcoin, la primera red conocida de *blockchain*.

En resumen, la infraestructura tecnológica *blockchain* o tecnología de registros distribuidos, es el resultado de numerosos años de investigación en criptografía y procesamiento distribuido, así como en técnicas para la creación de dinero digital. El artículo publicado en 2008 y la difusión y aceptación de la criptomoneda *bitcoin*, soportada por la tecnología *blockchain*, en 2009, supuso el punto de partida a la aceptación universal de la cadena de bloques. En la actualidad, *blockchain* es una tecnología con aplicaciones en multitud de campos con mayor penetración y difusión que las criptomonedas o monedas virtuales,

El 2017, fue el gran despegue de las tecnologías *blockchain*³ (cadena de bloques) a lo largo y ancho del mundo. Los años venideros hasta el 2020 se auguran como la gran expansión en todo tipo de sectores y con gran número de aplicaciones. Las tecnologías *blockchain* son el soporte de las criptomonedas a lo largo de todo el mundo, y en especial *bitcoin* (y otras como *Ethereum*), que han generado un nuevo ecosistema financiero. Cientos de bancos -centrales y privados—y corporaciones de todo el mundo apoyados en *blockchain* están invirtiendo miles de millones de euros en I+D+i que están cambiando las reglas de juego económicas y financieras. Además de esta gran transformación en el sector financiero, las tecnologías *blockchain* se están comenzando a aplicar en un gran número de sectores cuyos ámbitos aumentan de modo imparable: energía, telecomunicaciones, salud, alimentación, automoción, juegos virtuales, música, videos, medios de comunicación, voto electrónico, ciudades inteligentes, economía colaborativa, las ONG y, naturalmente en todas las grandes plataformas tecnológicas de impacto como Internet de las cosas, ciberseguridad, Big Data y analítica de datos, inteligencia artificial.

La tecnología *blockchain* fue uno de los temas candentes discutidos en el Foro Económico Mundial de 2018, donde la relevancia de esta tecnología se hizo cada vez más clara a medida que las iniciativas de gobiernos y organismos gubernamentales se han reforzado para impulsar la agenda de adopción del *blockchain*.

Nuevos consorcios y asociaciones entre las principales compañías de varias industrias resaltan el vínculo casi natural entre *blockchain* y la IoT. La generalización de *blockchain* traerá consigo una mayor seguridad en las transacciones, la economía digital o la protección de miles de millones de datos personales que impulsarán una administración más eficiente y

servicios de base para un gran número de cambios y el proceso de transformación digital. La convergencia de IoT y *blockchain* se ve reforzada con una tercera tecnología con lo cual se conforma una triada convergente: IoT, *blockchain* e IA.

El *blockchain* crea una cadena digital de registros con enlaces encadenados para formar un registro inmutable, único e irrepetible. Cada bloque de datos se eslabona al anterior para completar la cadena. Se consigue de este modo un registro distribuido, resistente a la sincronización, es decir, inmutable y permanente. Es muy útil para controlar la seguridad de la información, a través de protocolos para verificar y proteger las innumerables operaciones que se producen en su entorno. Es una base de datos que no permite borrar o modificar, solo permite una escritura bajo consenso. *Blockchain* permite comprobar si el documento generado ha sido alterado en algún momento posterior al registro.

“La inmutabilidad del *blockchain* puede entrar en conflicto con el derecho (Efren Diaz, 2018: 11) al olvido (art. 17 del RGPD) y la privacidad, al impedir la actualización o supresión de la información registrada en la cadena de bloques sin consenso de las partes implicadas”. El RGPD colisionará, según Díaz con el *blockchain* en su principal utilidad a punto fuerte que es su inmutabilidad e inalterabilidad; una vez que se introducen los datos no pueden ser borrados.

El derecho al olvido reconocido en Europa contraviene directamente la idea distinta de una tecnología que hace inmutable los datos registrados. El problema se agrava ante el esfuerzo inconmensurable que supondría la modificación, eliminación o de indexación de la información registrada en las bases de datos de cadena de bloques.

Los expertos plantean diversas soluciones que limiten el derecho al olvido en los sistemas *blockchain*. La aplicación efectiva del RGPD en entornos no monetarios ni financieros, requiere necesidades de una regulación moderna tales como: la veracidad jurídica de los documentos almacenados digitalmente y su preservación, la validez legal de los propios instrumentos financieros emitidos y las cuestiones relativas a la territorialidad y la responsabilidad en los contratos inteligentes y el desarrollo jurídico de IoT.

10.1.1. ¿CÓMO NACIÓ *BLOCKCHAIN*?

Tapscott (2017) señala que, coincidiendo con el hundimiento del sistema financiero global en 2008, fue en octubre de ese año cuando una persona o grupo de personas, con el pseudónimo de Satoshi Nakamoto publicó un artículo (octubre 2008) en el que se esbozaba el protocolo de un nuevo sistema de pago electrónico directo y entre iguales (*peer-to-peer* o P2P que usaba como aplicación de *blockchain* una criptomoneda llamada *bitcoin*).

Las criptomonedas o monedas digitales se diferencian de la moneda tradicional en que no las crean ni controlan los países. Este protocolo establece una serie de normas -en forma de computación distribuida- que garantiza la integridad de la información intercambiada entre los miles de millones de computadores que constituyen la red de *blockchain*, sin pasar por terceros. El protocolo es el fundamento de un creciente número de registros globalmente distribuidos llamados cadenas de bloque, el más grande de los cuales es *bitcoin*.

Nakamoto en ese artículo, detallaba el diseño de la primera cadena de bloques: “una base de datos pública y distribuida que se sincronizaría cada 10 minutos en miles de

computadores. Cualquiera podrá acceder a ella, pero nadie la podría piratear. ¿Su propósito? Proporcionar un registro de cambio blindado y descentralizado para una nueva moneda digital” (Pathak, 2018). Hasta ese momento como indica Pathak (2018) el problema con el dinero electrónico radicaba en que nadie podía asegurar que no se usaría dos veces. La cadena de bloques cambió eso, ya que cada transferencia -como se comentó anteriormente- se anota en un libro de contabilidad distribuido. Volviendo de nuevo a Tapscott, plantea que: “*blockchain* es un protocolo fiable soporte de una plataforma global en la que se puede operar de modo seguro, que no será el Dios Todopoderoso, pero sí es algo muy grande que llama protocolo fiable”.

10.2. FUNDAMENTOS DE *BLOCKCHAIN*

Blockchain es una base de datos, distribuida y escalable, en la que los usuarios independientes tienen acceso de forma segura. Se pueden digitalizar procesos de gestión global y los participantes colaboran estrechamente, sin comprometer detalles de privacidad o confidencialidad, minimizando la intermediación y el coste por actividad.

Una característica importante es la inmutabilidad de los datos ya que una vez inscritos es muy difícil cambiarlos (son inmutables).

- *Transparencia*. Proporciona una vista única de la información a todos los participantes.
- *Consenso*. Cuando hay que insertar un nuevo bloque se requiere el consenso de los actores del ecosistema. Al añadir el nuevo bloque a la cadena, la acción se puede verificar y tiene trazabilidad. Este proceso se puede verificar y tiene trazabilidad. Este proceso se puede automatizar total o parcialmente, utilizando algoritmos adecuados.

Cada bloque dispone de una marca de tiempo y un enlace con el bloque anterior, además de información sobre la aplicación específica. Cada bloque tiene un *hash* o identificador criptográfico único. Si se modifica su información, cambia su *hash*. Este se determina con un algoritmo y depende de la información contenida en ese bloque. Los mineros se encargan de encontrar nuevos *hashes*, para crear bloques y a cambio obtiene una retribución en criptomonedas.

En cada bloque existe un registro que contiene el *hash* del bloque precedente y permite la estructura secuenciada. Si alguien introduce un cambio no consensuado en la información, el *hash* cambiará y la cadena se romperá. Cambiar un *hash* significa tener que modificar todos los de los bloques existentes.

10.2.1. ¿QUÉ ES *BLOCKCHAIN*?

Blockchain es una base de datos distribuida que permite el almacenamiento de datos permanente, transparente y seguro. Es un enfoque innovador de las bases de datos distribuidas. La base de datos está distribuida entre diferentes participantes, protegida criptográficamente y organizada en bloques de transacciones relacionados entre sí, matemáticamente con algoritmos complejos.

Mantiene un listado de registros o bloques que está creciendo continuamente, pero con la característica de inmutabilidad de la información ya que está protegida criptográficamente y organizada en los citados bloques transaccionales relacionados entre sí con algoritmos matemáticos. No se puede cambiar la información contenida en un bloque, ya que cada bloque tiene una marca de tiempo y contiene un enlace a un bloque anterior; al estar descentralizada, ninguna persona u organización controla la entrada de datos o su integridad, pero el conjunto de la cadena de bloques se verifica continuamente por cada computadora miembro de la red de *blockchain*. En resumen, es una base de datos descentralizada que no se puede alterar.

En realidad, es un libro de contabilidad distribuido (*distributed ledger*) donde se anota cada transferencia de datos; en esencia, es una especie de hoja de cálculo que gracias a los algoritmos de matemáticas y de criptografía, es inalterable. El libro de contabilidad está integrado en una red de computadoras (computadores portátiles, servidores, teléfonos inteligentes) sin necesidad de una autoridad central. Los algoritmos matemáticos preservan la integridad de todas las fuentes de datos.

Don Tapscott, coautor de *Blockchain revolution* y uno de los grandes pensadores de la web del siglo XXI, define *blockchain* como un libro de contabilidad mundial que es capaz de albergar cualquier dato que requiera seguridad: historiales financieros, documentos de propiedad, certificados de identidad. Tapscott reseña que: “aunque el aspecto tecnológico de blockchain es complicado y la expresión blockchain suena rara, la idea es sencilla: las cadenas de bloques nos permiten enviar dinero de manera directa y segura de una persona a otra sin pasar por un banco, una tarjeta de crédito o PayPal”. En la práctica, lo que aporta *blockchain* es un protocolo fiable y seguro, siendo esta una de sus características más sobresalientes.

10.2.2. DEFINICIÓN DE *BLOCKCHAIN*

Una blockchain es una base de datos que se halla distribuida entre diferentes participantes, protegida criptográficamente y organizada en bloques de transacciones relacionados entre sí matemáticamente. Expresado de forma más breve, es una base de datos descentralizada que no puede ser alterada (Preukschat 2017: 23).

Una característica muy importante, es que, por definición, se trata de un sistema que permite que partes que no confían plenamente unas en otras puedan mantener un consenso sobre la existencia, el estado y la evolución de una serie de factores compartidos.

El consenso es una propiedad fundamental, y clave, de un sistema de *blockchain* porque es el fundamento que permite que todos los participantes puedan confiar en la información que se encuentra grabada. Blockchain -desde el punto de vista técnico- se basa en la confianza y el consenso, y se construye a partir de una red global de computadores que gestionan una base de datos de gran volumen.

10.3. *BLOCKCHAIN*: LA VISIÓN DEL NIST

En enero de 2018, el NIST, Instituto Nacional de Estándares y Tecnología (National Institute of Standards and Technology)⁴ una de las agencias más reputadas del mundo en el sector de las tecnologías, publicó un primer borrador del informe sobre tecnologías *blockchain* y que se ha convertido en una de las fuentes más prestigiosas donde consultar.

El documento *Draft NIST Interagency Report (NISTIR) 8202: Blockchain Technology Overview*⁵ es una guía muy completa de *blockchain* dirigida a empresas, directivos, profesionales y usuarios en general donde da recomendaciones de desarrollo y uso de la tecnología, y describe con gran fidelidad la tecnología, los componentes de la arquitectura de un sistema de cadena de bloques, los casos de usos (aplicaciones) más populares de *blockchain*, los beneficios y limitaciones de la tecnología.

Blockchain tal como se anunció en la presentación del informe es un nuevo paradigma muy potente y proporciona una visión general de la tecnología más disruptiva desde Internet. Además de la introducción a *blockchain*, describe los componentes de la cadena de bloques, la necesidad de modelos de permisos, contratos inteligentes, modelos de permisos de *blockchain* y una amplia gama de casos de usos, desde aplicaciones financieras -como criptomonedas- hasta aplicaciones no financieras tales como su integración en Internet de las cosas, y un caso muy importante como los edificios inteligentes o la aplicación en logística, en la administración de la cadena de suministro (SCM). Además de la descripción de la tecnología, sus raíces, amplía su estudio a las divisas digitales y criptomonedas.

El informe profundiza en conceptos esenciales como consenso y los diferentes modelos de consenso (*proof of stake* y *proof of works*), contratos inteligentes, categorización de *blockchain* y casos de uso. En el estudio también se describen los beneficios y limitaciones más importantes de la tecnología con el objetivo de ayudar a los administradores de tecnologías de la información a tomar decisiones bien informadas, sobre si las cadenas de bloques son la tecnología correcta para utilizar en una tarea determinada.

La primera conclusión práctica del NIST es que *blockchain* es un nuevo y potente paradigma para los negocios. Como todos los documentos oficiales del NIST, la publicación es un primer informe que se somete como borrador para todo tipo de propuestas y sugerencias

10.3.1. ¿QUÉ ES *BLOCKCHAIN* SEGÚN EL NIST?

La tecnología *blockchain* es, según el NIST:

Esencialmente, un libro de contabilidad (ledger) descentralizado que mantiene registros de transacciones en muchos computadores simultáneamente. Una vez que un grupo, o bloque de registros, se introduce en el libro mayor, la información del bloque se conecta matemáticamente o otros bloques formando una cadena de registros. Debido a esta relación matemática, la información de un bloque determinado no se puede alterar sin cambiar todos los bloques subsiguientes en la cadena y que se detectaría por otros usuarios de la red. De esta manera, la tecnología blockchain produce un libro de contabilidad fiable sin que los responsables de los registros se conozcan o confíen entre

sí que elimina los peligros que conlleva que un solo propietario mantenga los datos en una ubicación central

Versión final del NIST (2 de octubre, 2018)

El Instituto Nacional de Estándares y Tecnología (NIST) publicó en 2018 la versión final⁶ de su informe interinstitucional sobre tecnología de blockchain (NISTIR 8212. Blockchain Technology Overview: <https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf>). La descripción general de la tecnología blockchain es una versión actualizada de un borrador (Draft Blockchain Technology Overview), que fue publicado en enero del mismo año. El informe presenta el concepto de blockchain, como funciona la cadena de bloques, su uso en criptomonedas o monedas electrónicas, tipos de cadenas de bloques permitidas y sin permiso, componentes de las cadenas de bloques, modelos de consenso y sus aplicaciones más extendidas.

Las transacciones en la cadena de bloques se almacenan en un libro mayor bajo propiedad distribuida que minimiza la confianza, la seguridad y las preocupaciones de confiabilidad que pueden venir con la propiedad centralizada. En una red de *blockchain* distribuida, cada usuario mantiene una copia del libro de contabilidad, lo que dificulta la pérdida o destrucción. La resiliencia general de una red de *blockchain* heterogénea también es más fuerte porque los nodos se basan en software, hardware e infraestructura de red diferentes, por lo que no se garantiza que un ataque en un nodo funcione en otros.

Las cadenas de bloques se adaptan a aplicaciones donde los participantes que necesitan un sistema de propiedad criptográficamente seguro o un monitoreo de la actividad en tiempo real.

Blockchain es una base de datos distribuida. La información se almacena en innumerables computadores conectados entre sí a través de Internet. De modo práctico, es un tipo de libro de contabilidad al que pueden acceder todas las personas que registran y validan los datos.

Encadenamiento de bloques

Los bloques se encadenan (juntos) entre sí a través de cada bloque que contiene un hash a la cabecera del bloque anterior, formando la cadena de bloque. Si se cambiara un bloque publicado anteriormente, tendría un *hash* diferente. Esta acción, a su vez, produciría que todos los bloques subsiguientes también tengan *hashes* diferentes, ya que incluyen el *hash* del bloque anterior. Esta característica hace posible detectar y rechazar fácilmente cualquier cambio en los bloques publicados anteriormente.

Otras características de *blockchain*, sin embargo, pueden limitar su idoneidad en ciertas aplicaciones. Según el NIST, las preguntas a responder incluyen:

- Visibilidad de los datos: ¿Cuántos datos deben ser visibles en una red con permiso o sin él?
- Historial transaccional completo: ¿Cuántos datos transaccionales deben ser visibles para el público?

- Entrada de datos falsos: ¿Cómo pueden colocarse los controles para detectar la entrada de datos falsos?
- Datos de inviolabilidad y de invariabilidad: ¿Cómo se pueden mantener los datos del historial de transacciones?
- Transacciones por segundo: ¿Cuánto poder de cómputo es necesario para superar el lento procesamiento de transacciones?
- Cumplimiento: ¿Existen leyes o regulaciones que cambiarían la forma en que se diseña la cadena de bloques?
- Permisos: ¿Hay suficiente granularidad en roles de usuario específicos? ¿Quién puede administrar los permisos y con qué facilidad pueden ser revocados?
- Diversidad de nodos: ¿Cómo la diversidad de participantes de la red de *blockchain* contrarresta el riesgo?

10.4. FUNCIONAMIENTO DE *BLOCKCHAIN*

Aunque a nivel popular, y a medida que se populariza el término de cadena de bloques, se suele confundir *blockchain* y *bitcoin*, no es así y tienen que clarificarse estos conceptos. El *bitcoin* es un tipo de criptomoneda y la cadena de bloques es la técnica que hace posible el protocolo *bitcoin*; es decir: una infraestructura que permite mantener un registro de todo tipo de transacciones. El *blockchain* existe sin el *bitcoin*, pero no a la inversa. El *bitcoin* es una aplicación -la más popular por ahora- que se ejecuta sobre una cadena de bloques, de forma un tanto similar a como la red o la web se ejecuta sobre Internet. De hecho, *bitcoin* fue el primer sistema de contabilidad distribuida que no necesitaba el respaldo de un servidor centralizado ni de una organización y continúa siendo de los mayores. Pablos (2018) señala que, en noviembre de 2017, almacenaba más de 120 gigabytes de información, tamaño que aumenta con cada transacción.

El sistema de *blockchain* se construye a partir de una red global de computadores que gestionan una base de datos de gran volumen, que se basa, fundamentalmente, en la confianza y el consenso de las partes. Todas las cadenas de bloques (al igual que las usadas en *bitcoin*) están distribuidas, es decir, se ejecutan en computadores que ofrecen voluntariamente personas y organizaciones de todo el mundo; en consecuencia, no hay una base de datos central que en caso de peligro pueda atacarse.

La *blockchain* puede ser pública o privada. La *blockchain pública* está abierta a todas las personas que lo deseen y todo el mundo pueda verla cuando quiera porque reside en la red, no en una determinada organización que se encargue de auditar las transacciones y llevar registros. La *blockchain privada* está limitada a solo algunos usuarios. De cualquier forma, no se necesita una entidad central para supervisar o validar los procesos a realizar. Además, la *blockchain* está encriptada con claves públicas y privadas que garantizan una seguridad total.

En el caso de *bitcoin*, *Ethereum*, u otras criptomonedas, no se guardan en archivos que estén en un lugar determinado, sino que está representado por transacciones que se registran en una cadena de bloques que al igual que una hoja de cálculo o registro, usa los

recursos de una red amplia entre iguales (P2P) para verificar y aprobar todas y cada una de las transacciones hechas en *bitcoin*.

10.4.1 PROCESO DE LAS TRANSACCIONES EN UNA CADENA DE BLOQUES

Numerosos medios de comunicación de prestigio mundial, *Scientific American*, *The Economist*, *Forbes*, *Financial Times* junto con los más prestigiosos a nivel español como *El País*, *El Mundo*, *La Vanguardia*, *ABC*, *Expansión*, *Cinco Días*, *El Economista* han analizado y en muchos casos publicado infografías donde se muestra el proceso y funcionamiento de una cadena de bloques en muchos casos con aplicación a transacciones de criptomonedas o de otros documentos de importancia. Un modelo del funcionamiento de una cadena de bloque publicado por la prestigiosa revista científica *Scientific American*⁷ consta de las siguientes etapas:

- *Inicio de la transacción*. Una parte acuerda enviar datos a otra parte (los datos pueden ser cualquier cosa, criptomonedas, contratos, título de propiedad, título académico, propiedad, certificado médico, certificado de nacimiento).
- *Difusión de la transacción*. La transacción se difunde por la red de computadores (nodos) que operan el *blockchain*. Se crea un bloque con las transacciones en la cadena de bloques. Cada nodo dispone de algoritmos para comprobar la validez de la transacción.
- *Bloques y huella digital (hashing)*. Se crea una huella digital del nuevo bloque mediante una función criptográfica (*hash*) y una huella digital que apunta al bloque anterior.
- *Validación de la transacción (minería)*. Ciertos nodos denominados mineros comienzan a evaluar las transacciones mediante algoritmos criptográficos. Cuando existe consenso entre ellos, la transacción se considera válida y el bloque validado se añade a la cadena que ya no puede ser modificada, con la huella digital en la que también se codifican las huellas validadas de los bloques previos.
- *Ejecución de la transferencia*. El bloque se crea definitivamente y la información o unidad de valor se transfiere de la cuenta de la parte A la cuenta de la parte B.

10.4.2 COMPONENTES DE *BLOCKCHAIN*: FUNCIONAMIENTO

El *bitcoin* o cualquier criptomoneda no se guarda en archivos que se sitúan en un lugar concreto, sino que está representada por transacciones que se registran en una cadena de bloques (un registro u hoja de cálculo) que usa los recursos de una amplia red de computadoras entre iguales para verificar y aprobar todas y cada una de las transacciones realizadas en *bitcoin*.

Todas las cadenas de bloques -incluidas las de *bitcoin*- están distribuidas; es decir, se ejecutan las computadoras que ofrecen voluntariamente personas de todo el mundo. No existe una base de datos central sobre la que se pueda actuar. Cada diez minutos, se comprueban, ordenan y almacenan todas las transacciones en un bloque que se une al

bloque anterior, creándose una cadena. Cada bloque ha de referirse al anterior para ser válido. Esta estructura registra exactamente el momento de las transacciones y las almacena, evitando que nadie pueda alterar el registro. Si alguien quiere robar un bitcoin, ha de reescribir toda la cadena de bloques, en presentica de todos, situación prácticamente imposible.

Las cadenas de bloques son un registro distribuido y suponen la conformidad de la red con todas las transacciones que se han realizado. Es un registro de computación global del valor de un registro distribuido que todo el mundo puede descargar y ejecutar en su computador personal

Este registro digital de transacciones económicas se puede programar para utilizar prácticamente cualquier cosa que tenga valor e importancia en la sociedad:

- Partidas de nacimiento, defunción y permisos de matrimonio
- Escrituras y títulos de propiedad
- Grados y certificaciones académicas
- Informes financieros
- Procedimientos y tratamientos médicos
- Demandas de seguros
- Votos
- Origen de los alimentos
- Cualquier cosa que se pueda codificar

El especialista, Tapscott (2017: 29) lo define como Internet de todo, es decir, necesita “un registro de todo”. El libro de registro digital es una tecnología que permite que computadoras distribuidas en diferentes lugares almacenen información actualizada de modo permanente con todas las copias sincronizadas.

Plataformas de *blockchain* para empresas

- Ethereum
- Hyperledger Fabrics
- R3 Corda
- Ripple
- Quorum
- Canton
- Cardano

Hyperledger: Una plataforma modelo de *Blockchain*

En 2015, Linux Foundation creó el proyecto Hyperledger, con el objetivo de crear un estándar abierto cross-industry para el desarrollo de tecnologías utilizando *blockchain*. Son más de 130 miembros de distintas industrias, incluyendo TI, finanzas, salud y transporte (IBM, Intel, J. P. Morgan, American Express). Este consorcio tiene la función de desarrollar proyectos de código abierto en torno a la tecnología *blockchain*. Uno de estos proyectos es Hyperledger Fabric que es la red *blockchain* corporativa utilizada por IBM para la implementación de soluciones de negocios con sus clientes.

Hyperledger es, en realidad, un conjunto de tecnologías *blockchain* con diferentes características cuyo objetivo principal es la construcción de *blockchain* privadas. La plataforma Hyperledger ofrece la posibilidad de integrar la aplicación con softwares más conocidos para la gestión empresarial, para así realizar una implementación sencilla y rápida sin tener que realizar cambios en la propia empresa y la gestión de datos.

10.5. ¿CUÁLES SON LAS PRINCIPALES APLICACIONES DE LA TECNOLOGÍA *BLOCKCHAIN*?

Las tecnologías de *blockchain* pueden convertirse en la espina dorsal de una nueva Internet más segura y cambiar el mundo que conocemos desde la perspectiva de una nueva revolución de Internet. En un futuro no muy lejano, *blockchain* gracias al protocolo fiable que plantea Tapscott, se puede convertir en una plataforma global con la que se puede operar de modo seguro y será algo muy grande.

Tapscott plantea que más que un *Internet de la información*, las cadenas de bloques convertirán a Internet en un *Internet del valor o del dinero*, basado en que: «la plataforma permite a todo el mundo saber de lo que es verdad, al menos con respecto a la información que se registre de manera estructurada. En su forma más básica, es un código fuente libre [...] y como tal, nos da la posibilidad de crear infinidad de aplicaciones nuevas y de cambiar muchas cosas». Este Internet del valor producirá un gran cambio social y tecnológico que impactará en todas las facetas de la vida como sucedió con la aparición y despliegue universal de la red Internet y de la web.

Las posibilidades de las tecnologías *blockchain* son todas aquellas en donde existan transacciones de datos. La seguridad, transparencia, consenso y la confianza son propiedades fundamentales en cualquier negocio y soporte de las cadenas de bloques. En consecuencia, las tecnologías de *blockchain* son idóneas en multitud de sectores y las aplicaciones irán emergiendo; y camino del horizonte 2020 habrán aparecido tanto a nivel de investigación como de negocios, industria, salud, docencia. Un listado casi innumerable con infinidad de aplicaciones como Tapscott predice en su obra de impacto en campos como:

- Salud (sanidad y farmacia)
- Automoción
- Energía
- Trazabilidad de alimentos

- Gestión de bienes digitales
- Gestión energética
- Ciberseguridad
- Análisis de Big Data y aplicaciones de Open Data
- Registro de certificados académicos
- Votaciones o democracia participativa. Voto electrónico
- Trazabilidad para logística
- Sistemas de venta y alquiler
- Servicios de auditoría o consultoría
- Gestión de la propiedad intelectual
- Economía colaborativa
- Redes de dispositivos e Internet de las cosas
- Autenticación y pruebas de existencia
- Viajes
- Turismo
- Juegos virtuales
- Organizaciones no gubernamentales (ONG)

10.6. TIPOS DE *BLOCKCHAIN*: PÚBLICA, PRIVADA E HÍBRIDA

BLOCKCHAIN PÚBLICA

Está abierta a la participación de cualquiera que lo desee. Todo el mundo la puede ver porque reside en la red y no es una determinada institución que se encargue de auditar las transacciones y llevar los registros. Además, está encriptada: una encriptación que incluye claves públicas y privadas (en lugar de los sistemas de dos claves de las “cajas fuertes”) que garantizan una seguridad total. Ejemplo de redes públicas son: Bitcoin y Ethereum. La primera *blockchain* pública que ha existido ha sido la criptomoneda *bitcoin* lanzada en 2019. En su funcionamiento juega un rol importante la “minería” como proceso computacional necesario que opera para asegurar su red *prueba de trabajo*.

Características

- *Públicas*, cualquier persona -no se requiere ser usuario- puede acceder y consultar las transacciones realizadas.

- *Abiertas*. Cualquier persona se puede convertir en usuario y adoptar un protocolo común.
- *Descentralizadas*. Todos los usuarios tienen las mismas responsabilidades y los nodos son iguales.
- *Pseudoanónimas*. Los propietarios de las transacciones no son identificables personalmente, pero sus rastros tienen carácter público. La mayoría de las cadenas de bloques no pueden ser anónimas, excepto aquellas expresamente diseñadas.

BLOCKCHAIN PRIVADA

La *blockchain* privada se denomina con frecuencia *Distributed Ledger Technology* (DLT, Tecnología de Libro Mayor Distribuido). La *blockchain* privada es distribuida en el sentido de que es una base de datos repartida en varios nodos. La *blockchain* pública es descentralizada ya que no se controla quien participa en la misma.

Características

- *Privadas*. No todos los datos inscritos en la cadena de bloques tienen difusión pública, y solo los usuarios o participantes pueden acceder y consultar todas o alguna de las transacciones realizadas.
- *Cerradas*. Solo las personas invitadas a participar adquieren la condición de usuario o registradores de las transacciones.
 - El protocolo predeterminado podrá incluir distintos niveles de acceso a los usuarios, de modo que unos puedan tener la capacidad de registrar la información y otros tener vetada esta opción. El diseño depende de los objetivos conseguidos.
 - *Distribuidas*. El número de nodos puede estar limitado al número de participantes o una parte de ellos, pero los nodos se conocen entre sí. Los nodos son protegidos por los participantes que se comprometen a mantener la estabilidad del sistema. Esta es una característica importante que puede compensar la inestabilidad de las cadenas públicas.
 - *Anónimas*. Una cadena de bloques privada puede establecer el nivel de anonimato que considere conveniente para realizar o proteger transacciones.

Los usuarios de una cadena de bloques privada están sujetos a un protocolo determinado que los autoriza a participar en el registro de las anotaciones y/o verificar los cambios introducidos en la cadena. Por ello la base de datos puede estar más centralizada y el número de nodos se puede limitar a un número de usuarios establecido por los promotores, aunque las anotaciones realizadas seguirán siendo inalterables.

TIPOS DE *BLOCKCHAIN* SEGÚN PERMISOS

En una cadena de bloques pública, cualquier usuario puede participar en ella, esto implica un bloque sin permiso (*permissionless*). En una cadena de bloques privada, la posibilidad de

participar no está al alcance de todo el mundo, aunque el código utilizado sea público. La persona debe ser invitada a participar, por esta razón se la denomina *blockchain* con permiso (*permissioned*)

10.7. CONTRATOS INTELIGENTES

El término “contrato inteligente” (*Smart City*) fue definido por primera vez por Nick Szabo⁸ en 1994, jurista y criptógrafo; su doble formación permitió introducir principios de perspectiva jurídica y aplicación de algoritmos matemáticos criptográficos a los contratos inteligentes. La definición de smart contract de Szabo es: “*un conjunto de promesas, especificado en forma digital, que incluye protocolos dentro de los cuales las partes cumplen con estas promesas*”.

Al principio del lanzamiento del concepto no se pudo aplicar ya que las infraestructuras tecnológicas del momento no hacían visible la solución ya que no existían plataformas que permitieran su implementación. Fue, en 2015, con el lanzamiento de Ethereum cuando comenzó a ganar en popularidad el concepto de contrato inteligente, ya que Ethereum es una blockchain pública que incorpora, como innovación principal los contratos inteligentes, que, a su vez es una innovación muy potente al estilo de la criptomoneda *bitcoin*. La creciente popularidad se apoya también en que Ethereum dispone de su propia criptomoneda, el *ether*, por lo que no requiere el uso de *bitcoin*.

ETHEREUM

En su sitio oficial (www.ethereum.org), Ethereum se define como la blockchain programable del mundo y es de software abierto (open source). Al contrario que otras cadenas de bloques y como gran atractivo, Ethereum es programable lo que significa que los desarrolladores pueden utilizar la plataforma para construir nuevos tipos de aplicaciones. “Su principal objetivo es proporcionar la infraestructura necesaria para el desarrollo de aplicaciones descentralizadas cuya lógica de negocio reside enteramente en la blockchain en forma de contratos inteligentes” (Vilarroig 2018: 66)

Ethereum, es un proyecto global que actual como una comunidad y que es accesible por cualquier persona o entidad con independencia de lenguaje o nacionalidad y que incorpora como principal innovación, respecto a la criptomoneda *bitcoin*, los contratos inteligentes.

Cualquier programa que se ejecuta (o corre) en la Máquina Virtual de Ethereum, **EVM** (*Ethereum Virtual Machine*) se conoce comúnmente como un “*Smart Contract*” (contrato inteligente)⁹. Los lenguajes más populares para escribir contratos inteligentes en Ethereum son, el sitio web oficial: 1. *Solidity*, inspirado en los lenguajes de programación C++, Python y JavaScript; 2. *Vyper* basado en el lenguaje de programación Python. Está reconocido que el lenguaje más popular para trabajar en Ethereum es *Solidity*, aunque además de *Vyper* existen otras opciones.

¿Qué es un contrato inteligente?

El término contrato inteligente se refiere en general al uso de computadores u otros medios automáticos para ejecutar un contrato entre partes (Vilarroig 2020: 67). En esencia, un contrato inteligente es un código o protocolo informático que facilita verificar y hacer cumplir un contrato de manera automática. Un ejemplo típico de contrato inteligente puede ser el de una máquina expendedora de alimentos y bebidas, donde la máquina está diseñada para establecer una relación entre el diseño/proveedor de la máquina y el consumidor o usuario que realiza la compra de un alimento o bebida. Ethereum es la plataforma de *smart contracts* más destacada de la red.

Un contrato inteligente o *smart contract* es un código o protocolo informático que facilita verificar y hacer cumplir un contrato de manera automática (algoritmo computerizado que realiza los términos del contrato). El programa o las líneas de código (normalmente escritos en *Solidity*, aunque pueden ser otros lenguajes de programación) permiten facilitar el intercambio de dinero, contenidos, propiedad, acciones o cualquier cosa de valor. Una vez escrito y añadido a la Blockchain, un contrato inteligente se convierte en un programa de computador que se ejecuta automáticamente cuando se cumplen determinadas condiciones.

Estos contratos funcionan en la cadena de bloques y, a priori, no necesitan la intervención de las personas para comprobar y ejecutar su cumplimiento. Se almacenan dentro de una cadena de bloques para hacer todo tipo de transacciones incluidas las monetarias, para que se ejecute tal y como se programó sin posibilidad de censura, tiempo de inactividad, fraude o interferencia de terceros.

El modelo de contrato inteligente actual fue creado por Ethereum, donde un contrato inteligente es código escrito en un lenguaje de programación -el más utilizado *Solidity*. La plataforma **Ethereum**, en su origen, se creó específicamente para desarrollar contratos inteligentes con *blockchain*

CONTRATO INTELIGENTE VERSUS CONTRATO ORDINARIO

Un contrato ordinario, el usual en el mundo actual, es un acuerdo entre dos o más partes, requiere de una redacción que prevea las diferentes cláusulas de lo que es cumplimiento o no, y necesita un marco regulatorio con juristas, tribunales, notarios... Es decir, existen unas reglas de juego que permiten a todas las partes que lo aceptan entender en que va a consistir la interacción que van a realizar. Los contratos son documentos verbales o escritos. Los contratos escritos son documentos sujetos a las leyes y jurisdicciones territoriales y, normalmente requieren el uso de notarios.

El contrato inteligente elimina los intermediarios y se autoejecuta de manera autónoma a través del cumplimiento de determinadas acciones establecidas en el contrato, no escrito, sino basado en algoritmos en los que el cumplimiento de las partes acciona la siguiente fase. Un smart contract sólo necesita el acuerdo entre las partes para ser válido y no tiene por qué estar sometido a ninguna autoridad. En síntesis, un contrato inteligente es un código informático escrito en un lenguaje de programación (como se ha comentado anteriormente, *Solidity* de Ethereum, es el más utilizado) y es capaz de ejecutarse y hacerse cumplir por sí mismo, de manera autónoma y automática, sin intermediarios ni mediadores.

Un contrato inteligente puede ser creado y llamado por personas físicas y/o jurídicas, pero también como comentamos al principio, por máquinas u otros programas que funcionan de manera autónoma. Un contrato inteligente tiene validez sin depender de autoridades, debido a su naturaleza: código visible por todos y que no se puede cambiar al existir integrado en la tecnología *blockchain*. Esta característica le confiere un carácter descentralizado, inmutable y transparente.

APLICACIONES DE LOS CONTRATOS INTELIGENTES

Los contratos inteligentes tienen una cantidad innumerable de casos de uso, integrados en el catálogo general de aplicaciones de las cadenas de bloques, aunque por sus características específicas existen casos de usos específicos. Un conjunto grande de casos de uso, recopilado de numerosas fuentes, es el siguiente:

- *Servicios financieros y bancarios*
 - Préstamos
 - Seguros y microseguros; reclamos de seguros
 - Establecimientos de hipotecas
 - Pagos de cupones y bonos
 - Depósitos de garantía
 - Herencias
 - Sector inmobiliario
 - Automatización de pagos y donaciones
- *Servicios de salud*
 - Expedientes médicos
 - Acceso a los datos sanitarios de la población
 - Seguimiento de la salud personal
- *Servicios del sector público*
 - Controlar el suministro y pago de servicios de electricidad, gas y agua potable en el hogar
 - Votaciones
 - Apuestas, loterías, ocio
 - Estaciones autónomas de recarga de vehículos eléctricos
- *Servicios legales*
 - Registro de la propiedad
 - Propiedad inteligente

- Firma digital y verificación de identidades
- Notarios

10.8. TRAZABILIDAD

La trazabilidad es una de las aplicaciones de mayor y eficiente uso de *blockchain*. El diccionario de la Real Academia Española (DRAE) al definir *trazabilidad*, destaca su origen como término adaptado del inglés *traceability* y derivado de *to trace* “rastrear”, y considera las siguientes acepciones:

- Posibilidad de identificar el origen y las diferentes etapas de un proceso de producción y distribución de bienes de consumo.
- Reflejo documental de la *trazabilidad* de un producto.
- Propiedad de un resultado de medida que permite relacionarlo con una referencia superior mediante una cadena documentada de calibraciones.

En consecuencia, la trazabilidad de un producto es la posibilidad de conocer el origen de un producto y seguir su curso a lo largo de su cadena de transformación y distribución. Las reglas de trazabilidad están definidas por normas emitidas por organismos de control nacionales o internacionales, que varían según la naturaleza de las mercancías. En la Unión Europea, la trazabilidad de los productos alimenticios está bajo el control de la Autoridad Europea de Seguridad Alimentaria (EESA).

Según la EESA, la trazabilidad de un producto consiste en la capacidad de decir qué subproductos lo componen y las cantidades, conocer el proveedor de las materias primas con las que se ha elaborado un lote, y al cliente al que se le han suministrado en productos.

Dentro de un producto, existen varios tipos de trazabilidad.

- *Trazabilidad externa hacia atrás*. Trata de conocer el origen o componente utilizado para producir el nuestro dentro de la cadena de suministro.
- *Trazabilidad interna*. Consiste en poder obtener un estado pasado o inicial de un elemento que ha sido procesado dentro de una organización en su conjunto de elementos.
- *Trazabilidad externa hacia adelante*. Se trata de poder obtener los estados de un elemento una vez se ha enviado al cliente.

Otro término sinónimo de trazabilidad es la *rastreadibilidad*. Uno de los objetivos que busca conseguir el registro de la trazabilidad, es la capacidad de rastrear con rapidez y eficiencia ciertos datos referentes a la elaboración de un producto. En ese sentido, *blockchain* es una tecnología eficiente en la resolución de problemas de trazabilidad y logística.

- La trazabilidad de los alimentos: trazabilidad alimentaria
- Trazabilidad de los medicamentos

- Trazabilidad en el sector de alimentación y distribución (los grandes almacenes Carrefour aplica la tecnología *blockchain* en la trazabilidad)
- Trazabilidad aplicada a la agricultura
- Trazabilidad en Logística (caso de la consultora y desarrolladora de software, Indra)
- Trazabilidad de industrias cárnicas
- Trazabilidad en el sector bebidas
- Trazabilidad de productos farmacéuticos
- Trazabilidad en la cadena de suministro (SCM)

Numerosas grandes empresas del sector de distribución y alimentación han lanzado iniciativas de trazabilidad apoyadas en *blockchain* (El Corte Inglés, Alcampo, Walmart, Nestlé, Dole, Unilever, Carrefour).

CASOS DE ESTUDIO

La cadena multinacional Carrefour¹⁰, empresa francesa, especializada en la distribución de alimentos y con un gran número de supermercados desplegados a nivel mundial, anunció en noviembre de 2018 que empezaría a prestar servicios con un nuevo sistema de trazabilidad de alimentos basado en la cadena de bloques de Hyperledger Fabric de la plataforma IBM Food Trust.

Carrefour es la primera vez que usa la cadena de bloques para hacer seguimiento a uno de sus productos. Una primera aplicación iniciada es “monitorear únicamente la comercialización del pollo campero criado sin tratamientos antibióticos”. Los consumidores pueden consultar información detallada sobre el producto: fecha de nacimiento del ave, modalidad de crianza, alimentación, ubicación de la granja, proceso de envasado y fecha en la que llegó a los almacenes de Carrefour. El comprador podrá verificar “calidad y origen”. La etiqueta incluye en el producto un código QR que se escanea y presenta la información en el teléfono inteligente.

Carrefour ha lanzado la primera *blockchain* agroalimentaria de Europa para garantizar la trazabilidad de su cadena de pollos de granja: incubación, cría, alimentación, sacrificio, almacenamiento y ventas. Cada etapa de la producción, transformación y almacenamiento de las aves de corral se registra y constituye un elemento de la *blockchain*, que permite:

- Garantizar la transparencia en toda la cadena de suministro.
- Consultar todos estos datos de modo inmediato gracias a un código QR situado en la etiqueta del producto. De este modo conocerá con total precisión el origen de los productos que consume la ruta que han realizado hasta llegar a la estantería del almacén.
- Acceder al historial completo del producto que han comprado y verificar la autenticidad de sus compras, al escanear un chip NFC o un código QR integrado en cada artículo.

- Conocer información relativa al producto, al escanear el código QR que incluye la etiqueta del alimento: fecha de nacimiento del pollo, modo de cría, la ubicación de la granja, el alimento que ha recibido, el proceso de envasado o la fecha en la que han llegado a los almacenes de Carrefour.

Ventajas

- Para el consumidor: accesibilidad inmediata a la información, control y eficacia (calidad y origen).
- Para el proveedor: Tener una visión global de 360° de todo el proceso de distribución y poder garantizar la calidad del producto.

Plataforma IBM Food Trust

Tiene como objetivo implementar un estándar global de trazabilidad de los alimentos en todas las etapas de la cadena de suministro. Carrefour es miembro fundador de la plataforma IBM Food Trust y cuenta con los servicios de IBM y en España, la empresa gallega Coren.

Caso de éxito: La empresa del sector agroalimentario Angulas Aguinaga fue de los primeros fabricantes de alimentación en unirse a la plataforma IBM Food Trust, sistema de trazabilidad basado en tecnología que permite controlar el proceso desde la producción hasta su llegada al punto de venta. Ha implantado la tecnología de bloques en la trazabilidad alimentaria de sus productos, como el famoso pescado/marisco, angulas y gulas de Aguinaga.

Mirror

Aplicación para la trazabilidad *blockchain* personalizable: almacenamiento y rastreo de la información, que se basa en Hyperledger. Mirror se puede integrar a la mayoría de los sistemas actuales como SAP, Oracle, Joomla, WordPress y sistemas IoT, sin alterar el flujo de trabajo y productividad, pudiendo manejar los datos desde dispositivos iOS o Android, o cualquier PC con conexión a Internet. Mirror ofrece aplicaciones en:

- *Sector agroalimentario.* Ofrece seguridad y certificación de cualquier alimento, pudiendo visualizar su crecimiento, tratamiento y colocación en venta, para garantizar las características hasta que llegue al cliente.
- *Sector sanitario.* El cliente puede consultar todo su historial clínico: enfermedades, alergias y percances, expedientes de los centros donde se hayan recibido tratamiento y datos básicos de la salud.
- *Sector académico.* De modo fiable, accesible y seguro se puede disponer de todo el historial académico, títulos de grado, notas de cada curso y otros documentos.
- *Sector industrial.* El fabricante puede disponer de la información real y única de cada etapa de la producción hasta que el producto llega al cliente final, garantizando la calidad y la posibilidad de disponer información real de compra, y obteniendo una mejora en su propio servicio y la satisfacción del cliente.
- *Sector del arte.* Certificar la autenticidad de una obra de arte o la propiedad de un bien concreto.

10.9. IDENTIDAD DIGITAL

La creación de una identidad digital permite identificar los productos de origen y añadir a la red de información que los concierne. Existen desarrollos conjuntos de sistemas de trazabilidad específicos en redes *blockchain* según las necesidades de un sector determinado, p. e. sistemas de trazabilidad de alimentos¹¹ o de bienes de gran valor.

IBM y Walmart están desarrollando un sistema de trazabilidad de alimentos en cadenas de bloques que permitirá a los consumidores obtener información muy diversa sobre los productos que adquieran en el supermercado como su origen, modo de producción, días hasta la caducidad.

Se requiere una seguridad jurídica en el intercambio de datos, y eso ha hecho fortalecer los mecanismos y sistemas de gestión de la identidad digital que posibilitan la acreditación y autenticación de la personalidad del usuario cuando opera en espacios de Internet y de Internet de las cosas, en particular. Ibáñez (2018: 83) define la identidad digital como: “la información electrónica y telemática asociada a una persona física o jurídica conforme a reglas específicas configuradoras de un sistema de identidad”. También considera que el sistema de identidad debe usarse para dos finalidades fundamentales: autenticar o demostrar frente quienes operan en la red que quien introduce los datos es quien pretende ser respecto a ellos y autorizar a quien ha sido autenticado para realizar operaciones, transacciones o, en el orden jurídico, negocios jurídicamente válidos, contratos o actos unilaterales con los efectos prevenidos por la ley.

En consecuencia, Ibáñez ve que la contribución mayor de *blockchain* en el área de la identidad, es “la consecución plena de una autonomía individual que refuerza extraordinariamente la privacidad y que se concreta en la construcción de las denominadas plataformas de identidad digital soberanas (SSI, *Self-coverage Identity*)”.

Trazabilidad de bienes inmateriales

Una vez creada la “identidad digital” de la obra sería posible acreditar su autenticidad, identificar el autor, registrar sus sucesivas transmisiones, sus actos de explotación, conocer el alcance y asegurar la validez de las licencias obtenidas.

10.10. *BLOCKCHAIN* EN INTERNET DE LAS COSAS

Las tecnologías de cadenas de bloques han comenzado a tener una influencia significativa en el IoT mejorando la seguridad, potenciando la incorporación de un número creciente de dispositivos en el ecosistema. Las empresas pueden utilizar las cadenas de bloques para gestionar los datos de los dispositivos en los bordes, activos basados en IoT, códigos de barras, exploración de códigos QR o información de dispositivos.

Existen muchas ventajas de la construcción de máquinas inteligentes para comunicar y operar vía *blockchain*.

- IOTA. Ha sido una de las primeras *startups* enfocadas en IoT. No es, realmente, una cadena de bloques. Funciona en una estructura de datos llamada un grafo dirigido acíclico (*direct acyclic graph*) conocido como “thetangle” en la IoT.
- *The tangle* (el enredo). Es parecida o similar a una cadena de bloques y cae dentro de la categoría de la tecnología de contabilidad distribuida, pero presenta una estructura de consenso diferente. De modo notable, la estructura de *tangle* hace que la plataforma sea muy rápida.

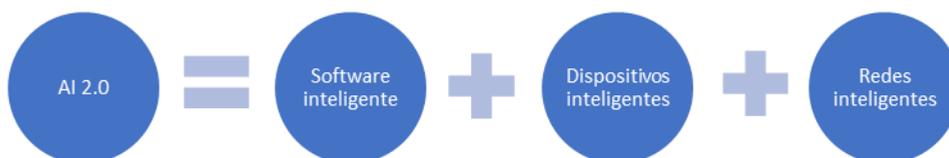
Los bloques se agregan al libro de contabilidad al hacer referencia a una matriz de transacciones previas interconectada: de ahí, procede el nombre *enredo*, en lugar de la secuencia única de una cadena de bloques normal. El rendimiento reciente de la red ha conseguido unas 1000 transacciones por segundo, lo cual supone una mejora enorme sobre las tasas estándar del *blockchain*.

Blockchain mejorará la conectividad de Internet de las cosas

El análisis de los datos recibidos por los dispositivos de IoT, potenciado por *blockchain* y la inteligencia artificial potenciará el desarrollo de software, extrayendo conocimiento útil y accionable para la toma de decisiones en las organizaciones y las empresas.

Inteligencia artificial 2.0

Pathak (2018) define una nueva tendencia que denomina Inteligencia 2.0 y que se compone de la integración de la tecnología cognitivas o el software inteligente (AI), los dispositivos inteligentes (Internet de las cosas) y las redes inteligentes (*blockchain*).



AI 2.0 es una combinación de AI (software inteligente), IoT (dispositivos inteligentes) y Blockchain (red inteligente). Fuente: Pathak y Bhandari (2018:19) [adaptada]

Aplicación de AI 2.0 Smart Lean Manufacturing

Las prácticas de fabricación se han convertido en altamente optimizadas. Los dispositivos de IoT se pueden utilizar para monitorizar máquinas y su entorno. La analítica inteligente de datos puede aplicarse sobre la monitorización de los datos recolectados para generar conocimiento y ayudar a la optimización en los procesos de fabricación. *Blockchain* puede ayudar a asegurar y dar fiabilidad para la distribución de parámetros optimizados en una cadena de plantas de fabricación. La cadena de suministro puede también ser gestionada eficientemente utilizando *blockchain*.

Casos de estudio. Seguro de automóviles

Los datos de la actividad de un conductor son capturados por su vehículo inteligente. Se vuelcan luego en los servidores de la compañía de seguros que los activará en casos específicos (como el de un accidente) y los enviará en forma automática a los usuarios que lo necesiten. La función de cadenas de bloques en este caso es dar transparencia y perpetuidad a esa información, para que los datos recogidos por el auto sean la única fuente de información y que se conecten de forma eficaz (Interxion)¹².

Según Interxion, el rápido proceso de desarrollo de IoT y *blockchain* producirá grandes cambios en el modo de vivir y conectarse, siempre que se mantengan los objetivos de proteger la privacidad y los datos de los usuarios.

Existe un vínculo natural entre cadenas de bloques e Internet de las cosas. El ya mencionado Tapscott, uno de los grandes pensadores a nivel mundial sobre el impacto de las tecnologías en los negocios y en la sociedad, anunciaba en su obra como *blockchain* e Internet de las cosas contribuirán de modo colaborativo a la transformación de gran número de aplicaciones y de industrias completos. IoT sin *blockchain* se enfrenta a problemas de escalabilidad y de punto a punto.

Blockchain servirá como la columna vertebral de la confianza digital y la seguridad para las interacciones en las aplicaciones de IoT y de grandes organizaciones. La tecnología *blockchain* se combinará con IA y con IoT para responder al desafío de la escalabilidad, punto importante de falla, sellado de tiempo, registro, privacidad, confianza y confiabilidad de un modo muy consistentes.

10.10.1. EL INTERNET DE LAS COSAS: UN REGISTRO DE TODAS LAS COSAS

El Internet de las cosas como señala Tapscott (2017: 224) requiere un registro de todas las cosas, un modo de compartir información distribuida, fiable y segura, de captar datos y de automatizar acciones y transacciones en Internet, gracias a la tecnología de *blockchain*:

La tecnología blockchain nos permite identificar dispositivos inteligentes con información básica relevante y programarlos para que actúen en determinadas circunstancias sin riesgo de error ni manipulación. Como la blockchain es un archivo incorruptible de todos los intercambios de información que se producen en la red y crecientes en el tiempo, el usuario puede estar seguro de que los datos son exactos y fidedignos.

Existe amplio consenso entre las empresas tecnológicas de que el sistema de cadena de bloques es esencial para desarrollar el potencial del IoT.

10.10.2. APLICACIONES DEL REGISTRO DE TODAS LAS COSAS

El registro de todas las cosas, creado dentro de la IoT tiene grandes posibilidades en numerosos e importantes sectores. Las ventajas y las oportunidades de negocio serán específicas de cada aplicación, pero de gran impacto en el mercado y modelos de negocio

actuales. Citando de nuevo a Tapscott (2017: 229-236) sintetiza las categorías de impacto y la revolución que supondrá en los siguientes doce sectores principales:

- Transporte
- Gestión de infraestructuras
- Gestión de energía, residuos y agua
- Extracción de recursos, agricultura y ganadería
- Control medioambiental y servicios de emergencia
- Atención sanitaria
- Servicios financieros y seguros
- Archivos de documentos y registros
- Administraciones de edificios y propiedades
- Operaciones industriales: la fábrica de las cosas
- Gobierno de la casa
- Operaciones y ventas al por menor

El IoT basado en *blockchain* tiene un gran potencial. La primera razón que aporta Tapscott es “porque da vida al mundo físico”. Una vez cobran vida en el registro, los objetos pueden percibir, responder, comunicarse y actuar. Los dispositivos se pueden buscar, encontrarse, usarse y pegarse unos a otros según manden los contratos inteligentes, creando así nuevos y revolucionarios mercados como ha hecho Internet con las personas y todo tipo de contenido digital.

Un ejemplo destacado citado por Tapscott es la economía circular: gestión de energía, residuos y agua, es el caso de empresas de servicios tradicionales tanto de los países desarrollados como países en vías de desarrollo que pueden usar el IoT con *blockchain* para controlar la producción, la distribución, el consumo y la recogida de bienes y residuos. Menciona el caso de empresas nuevas sin gran infraestructura incorporada que utilizan las tecnologías de *blockchain* para crear mercados y modelos completamente nuevas (microrredes de suministro comunitario).

Otra aplicación original que cuenta Tapscott es la extracción de recursos, agricultura y ganadería. Cita, el caso de las vacas que pueden convertirse en dispositivos de *blockchain* permitiendo a los ganaderos saber lo que comen, con qué se medican y todo su historial sanitario. Una aplicación más descrita por Tapscott es el uso de la tecnología para ayuda a controlar maquinaria costosa y muy especializada, y hacer que esté más disponible para un uso puntual y sea más amortizable; también mejorar la seguridad de mineros, agricultores y ganaderos mediante el etiquetado de los equipos de seguridad y listas de control automatizadas (para cerciorarse de que el equipo se usa indebidamente).

10.11. CONVERGENCIA DE *BLOCKCHAIN* Y LA INTELIGENCIA ARTIFICIAL EN INTERNET DE LAS COSAS

Según IDC, en 2019, el 20 % de todos los despliegues de IoT tendrán habilitados niveles básicos de servicios de *blockchain*. La convergencia de la cadena de bloques y el Internet de las cosas está en la agenda de muchas empresas y existen implementaciones, soluciones e iniciativas en diferentes áreas, externas de IoT y también los servicios financieros.

La rápida convergencia de IA, IoT y *blockchain* está aportando un gran valor a las empresas y las personas que utilizan estos nuevos servicios. IoT lleva el análisis en tiempo real a los procesos automatizados (de los cuales la AI forma parte). A medida que se ofrecen servicios personalizados a empresas es probable que se necesite acceder o almacenar grandes cantidades de información personal, lo que requiere una arquitectura de seguridad mucho más fuerte a la que se tiene con el modelo centralizado.

2019 fue el año de la convergencia. La vulnerabilidad de la seguridad de la IoT es lo que ha favorecido el uso de la *blockchain* en convergencia con IoT. Con IoT cada dispositivo conectado es, en sí, un punto vulnerable de entrada y con IA tomando decisiones por los usuarios, los riesgos son muy significativos. Una plataforma soportada por *blockchain*, es escalable, segura y fácilmente examinada, creando un alto nivel de seguridad. Las tres tecnologías pueden configurar un ecosistema seguro y estable. Los chips NFC y RFID, y *blockchain* configuran una nueva identificación personal y potenciarán las criptomonedas.

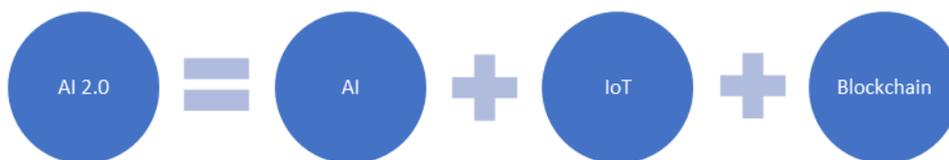
Para que el IoT sea adoptado con confianza necesita protocolos para verificar y proteger las innumerables operaciones que se producen en su entorno. *Blockchain* puede cumplir con estos requerimientos y está alcanzando niveles de eficacia que resultan muy atractivos para las empresas. La escalabilidad que ofrece también es un factor decisivo a la hora de acumular enormes cantidades de registros y transacciones. Ya existen casos de aplicación de las cadenas de bloques en el desarrollo de Internet de las cosas.

En ese sentido, Pandia (2019)¹³ considera que:

El concepto mismo del IoT -Internet de Todo- es que a las máquinas, objetos, sensores, personas y más se les pueden proporcionar identificadores únicos y la capacidad de transferir datos a través de una red centralizada a una red descentralizada. Esta transferencia se produciría con o sin interacción de persona a persona o de persona a computadora, y requeriría no solo nuevas capacidades tecnológicas y no tecnológicas, sino también la convergencia de blockchain y AI / ML.

Pathak (2018) [apartado 10.10] definió:

Inteligencia Artificial 2.0 como la integración de Internet de las Cosas, Blockchain y la propia Inteligencia Artificial



10.11.1. HACIA UN MODELO DE CONVERGENCIA DE *BLOCKCHAIN-IOT-AI*¹⁴

Dado que la arquitectura del ecosistema actual de IoT se basa en un modelo centralizado conocido como el modelo servidor/cliente donde todos los dispositivos se identifican, autentican y conectan a través de servidores en la nube que admiten capacidades de almacenamiento y procesamiento colosales, parece que los servidores/granjas de servidores pueden ser costosos, y también hacer que las redes de IoT sean vulnerables a los ataques cibernéticos.

A medida que surgen aplicaciones para tareas delicadas e infraestructuras críticas, esto puede afectar los ecosistemas evolutivos de IoT; lo cual nos lleva a un punto de análisis vital: ¿es necesario que la descentralización sea parte de la ecuación de IoT? El Internet de las cosas, o los dispositivos que se comunican entre sí, se distribuyen por naturaleza. Como resultado, es razonable que la tecnología de libro mayor descentralizado y distribuido, como *blockchain*, juegue un papel vital en la forma en que los dispositivos se comunicarán directamente entre sí o con los responsables de la toma de decisiones. Ahora, dado que todos los dispositivos de IoT deberán etiquetarse, también se deberá documentar el rastro de los dispositivos de IoT, con qué interactúan, ya que, sin duda, jugará un papel definitivo más allá de Internet. Comprensiblemente, el paradigma de seguridad está cambiando.

Ahora, la tecnología *blockchain* probablemente permitirá la creación de redes de malla seguras, donde los dispositivos de IoT podrán interconectarse de manera confiable y evitar las amenazas cibernéticas. Con cada nodo auténtico que se registra en la cadena de bloques, los dispositivos de IoT en la red podrán identificarse y autenticarse entre sí sin la necesidad de autorización humana. Como resultado, la red de autenticación será escalable para admitir miles de millones de dispositivos sin la necesidad de recursos humanos adicionales.

Aprovechar *blockchain* para datos de IoT ofrece nuevas formas de automatizar procesos en todos los niveles sin configurar una infraestructura de tecnología de almacenamiento y autenticación centralizada complicada y costosa. Se cree que esta es una solución clave para las redes en las que existe una potencia informática creciente en el borde: en sensores, dispositivos y otros dispositivos distribuidos. *Eso nos lleva a una pregunta importante: ¿es la tecnología blockchain el vínculo que falta para resolver los problemas de seguridad, privacidad y confiabilidad de la evolución del ecosistema de Internet de las cosas?*

Debido a que la generación, el almacenamiento, el análisis y la comunicación de datos, información e inteligencia son fundamentales para el ecosistema de IoT, existe la necesidad de proteger los datos a lo largo de su ciclo de vida.

CASO PRÁCTICO

La rápida convergencia de *Blockchain*, IoT e IA, está aportando un gran valor en las empresas y las personas que utiliza estos nuevos servicios.

- *IA*. Componente fundamental de la automatización, y mejora de las experiencias al elevar los niveles de eficiencia de las empresas
- *IoT*. Su función principal es analizar en tiempo real, los procesos automatizados. El IoT genera un flujo de trabajo para personalizar las experiencias que las empresas ofrecen a sus clientes.
- *Blockchain*. Al ofrecer servicios personalizados, se suele necesitar acceder o almacenar cantidades grandes de información personal, que no requiere una arquitectura de seguridad mucho más fuerte que la tradicional del modelo centralizado. Como arquitectura distribuida utiliza criptografía y permite mejorar la validación de algunos datos sin alterar las bases de datos existentes, las cuales cumplen con varios requerimientos de cumplimiento.

CASO DE USO

Turgeon¹⁵ muestra el beneficio de un caso de uso donde convergen la IA, IoT y *Blockchain*. Es una aplicación de ciencias de la salud. Un paciente lleva puesto un dispositivo que monitorea su ritmo cardíaco y nivel de ejercicio todos los días. El dispositivo inteligente contiene toda su información personal (identidad incluyendo reconocimiento facial y de huella digital, información de contactos; datos sobre su médico, medicamentos, alergias, tratamiento). Por razones de seguridad, las funciones biométricas cifradas se almacenarían en una arquitectura de bases de datos.

Su aseguradora médica controla con rigurosidad su salud y constantemente monitorea los diferentes aspectos de su salud a lo largo del día mediante los dispositivos *wearables* que usted ha registrado con ellos. *Blockchain* será la columna vertebral de la confianza digital para muchas organizaciones de gran tamaño.

Asiste a un evento y su dispositivo *wearable* reporta un ritmo cardíaco anormal. La IA a través del análisis, determina que esa anomalía es un precursor de un ataque cardíaco. Se activa, inmediatamente un evento para notificar a su médico, su estado y proporcionarle todos los datos relevantes de los últimos días. Su médico observa una situación grave y envía una ambulancia por usted para llevarlos al hospital.

Sus dispositivos *wearables* por geolocalización indican su ubicación exacta al equipo de respuesta de emergencia para que lo atiendan. Cuando llega al hospital, el sistema enlazado a su criptomoneda (*bitcoin*) que también utilizan *blockchain*, le permite ingresar y pagar una habitación privada. El proceso activado por IA brindó una experiencia completamente automatizada que le salvó la vida.

RESUMEN

La tecnología *blockchain* (cadena de bloques) fue uno de los temas centrales destacados y debatidos en el Foro Económico Mundial en enero de 2018 (WEF 2018) con lo que fortalecía la tecnología como componente central de la economía de los años futuros.

- Existen un gran número de consorcios y asociaciones de empresas e industrias que coordinan, analizan y dirigen las estrategias nacionales e internacionales para el desarrollo y despliegue de *blockchain*.
- En España, **ALASTRIA**, es una asociación -sin ánimo de lucro- de gran prestigio a nivel nacional e internacional con un elevado número de asociados: organizaciones, empresas, fundaciones, universidades... Sus objetivos son liderar y dar normas, reglas, metodologías, técnicas de *blockchain* con la finalidad de ayudar a todos sus asociados y cualquier otra entidad interesada en el conocimiento, desarrollo y despliegue de técnicas de cadenas de bloques, aplicaciones y usos en los innumerables sectores donde tienen impacto.
- Al igual que en otras tecnologías la prestigiosa organización NIST de Estados Unidos ha publicado un buen número de informes que ayudan a conocer, desarrollar y desplegar tecnologías *blockchain* y como organización sin ánimo de lucro todos ellos gratuitos y recomendables su análisis y descargas.
- Los tipos de *blockchain* más populares son: pública, privada e híbrida.
- Aplicaciones y conceptos muy importantes de gran impacto en el sector *blockchain* son: Contratos Inteligentes, Trazabilidad y Identidad Digital.
- La década 2020 se caracteriza por la convergencia de *blockchain*-IoT-IA y con soporte de infraestructuras de la nube (*cloud*, *edge*, *fog*) y el ecosistema de Big Data.

BIBLIOGRAFÍA

ALLENDE, Marcos (2018). *Blockchain. Cómo desarrollar confianza en entornos complejos para generar valor de impacto social*. IE/IPS TechLab BLD Banco Interamericano de Desarrollo. Licencia Creative Commons. Disponible en línea en: <https://webimages.iadb.org>.

BAMBARA, Joseph I. y Paul R. ALLEN (2018). *Blockchain. A Practical Guide to Developing Business, Law, and Technology Solutions*. New York: McGraw-Hill.

BASHIRAN, Imran (2017). *Mastering Blockchain*. Birmingham: Packt Publishing.

BOAR, Andrei (2018). *Descubriendo el bitc oin. C omo funciona, c omo comprar, invertir, desinvertir*. Profit Editorial.

DOLADER, Carlos, Juan Bel ROIG y Jos  Luis MU OZ TAPIA. "La Blockchain: Fundamentos, aplicaciones y relaci n con otras tecnolog as disruptivas", en UPC. N mero 405, pp.: 33-40.

DOMINGO, Carlos (2018). *Todo lo que querías saber sobre Bitcoin, Criptomonedas y Blockchain y no te atrevías a preguntar*. Barcelona: Planeta.

IBÁÑEZ, Javier Wenceslao (2018). *Blockchain: Primeras cuestiones en el ordenamiento español*. Madrid: Dykinson.

MOUGAYAR, William (2017). *La tecnología BLOCKCHAIN en los negocios. Perspectivas, práctica y aplicación en Internet*. Madrid: Anaya Multimedia.

NAKAMOTO, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System. Artículo original de creación de Bitcoin". Disponible en línea en: <www.bitcoin.org>.

NORTON, Jared (2016). *Blockchain. Easiest Ultimate Guide to Understand Blockchain*.

PATHAK, Nishith y Anurag BHANDARI (2018). *IoT, AI, and Blockchain for .NET. Building a Next-Generation Application from the Ground Up*. Apress.

PORXAS, Núria y María CONEJERO (2018). "Tecnología BLOCKCHAIN: Funcionamiento, aplicaciones y retos jurídicos", en *Actualidad Jurídica Uría Menéndez*, 48-2018, pp. 24-36.

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

SANTOS, Maximiliano y Enio MOURA (2019). *Hands-On IoT Solutions with Blockchain*. Packt Publishing.

TAPSCOTT, D. y A. TAPSCOTT (2017). *La revolución Blockchain*. Barcelona: Deusto.

TUR, Carlos (2018). *Smart contracts. Análisis jurídico*. Madrid: Editorial REUS.

VILLAROIG, Ramón y Sampere PASTOR (dir.) (2018). *Blockchain: Aspectos tecnológicos, empresariales y legales*. Pamplona: Aranzadi.

ZHU, Liehvang y Keke GAI, Meng LI (2019). *Blockchain Technology in Internet of Things*. Springer.

RECURSOS

DYLAN, Yaga; Peter MELL, Nil ROBY y SCARFONE, Karen (2018). *Blockchain Technology Overview. NISTIR 8202. NIST. Versión final, octubre 2018*. Disponible en línea en: <https://csrc.nist.gov/publications/detail/nistir/8202/final>

DYLAN, Yaga; Peter MELL, Nil ROBY y SCARFONE, Karen (2018). *Draft Blockchain Technology Overview. NISTIR 8202. Versión Borrador, enero 2018*. Disponible en: <https://csrc.nist.gov/CSRC/media/Publications/nistir/8202/draft/documents/nistir8202-draft.pdf>

[GitHub.com](https://github.com)

[Hbr.es](https://hbr.es)

[IBM \(ibm.com/developerworks\)](https://ibm.com/developerworks)

miethereum.com

Medium (*medium.com*)

Myethereum.es

Technologyreview.es

Theblockchain.es

GLOSARIO

Nodo. Un computador conectado a una red P2P (peer-to-peer) con diferentes capacidades de cómputo. Las criptomonedas como bitcoin y ethereum se componen de miles de nodos repartidos por todo el mundo. Todos los nodos han de poseer el mismo software y protocolo para comunicarse entre sí. En una blockchain pública los nodos no tienen por qué identificarse, mientras que en una blockchain privada, los nodos se conocen entre sí y pueden ser iguales entre ellas.

Redes igual a igual (P2P, peer-to-peer). Red descentralizada de computadores conectados directamente entre ellos que se pueden comunicar entre sí directamente, sin pasar por un servidor central ni por un administrador. Napster fue una de las primeras redes P2P, y en la actualidad BitTorrent es una de las más populares.

Libro de contabilidad distribuido (distributed ledger). Lista de transacciones con marcas de tiempo que se difunde, copia y confirma simultáneamente a través de múltiples computadores de una red P2P.

Bloque. Agrupación de transacciones individuales en una cadena de bloques. En el caso de la criptomoneda bitcoin todas las transacciones se comprueban, ordenan y almacenan en un bloque que se une al bloque anterior, creándose así una cadena. Cada bloque debe referirse al bloque anterior para ser válido. Esta estructura registra fielmente el momento de las transacciones y las almacena evitando que nadie pueda alterar el registro.

Cadena de bloques. Es un conjunto de computadores o servidores denominados nodos, que conectados en red utilizan un mismo protocolo o sistema de comunicación con el objeto de validar y almacenar la información registrada en una red P2P.

Criptomoneda. Moneda virtual que utiliza técnicas de criptografía para controlar cuándo se generan las unidades de la divisa y garantizar la transferencia segura de fondos.

Minería. Proceso computacional necesario que opera para asegurar su red. Los nodos de una red de criptomoneda compiten entre sí para añadir de modo seguro nuevos bloques a la cadena.

Método aleatorio o dispersión (hash/hashing). Método criptográfico que usa una función llamada hash que resume cualquier cantidad de datos en una cadena alfanumérica de longitud fija. La transformación de una cadena de caracteres en un valor normalmente más corto, de longitud fija, o una clave que representa la cadena original (similar a la creación de un acortador de direcciones URL de la web como bitly.com).

Sistema descentralizado. Todos los computadores conectados a la red son iguales entre sí y controlan dicha red. No existe una jerarquía entre los nodos en el caso de una *blockchain* pública, pero si puede existir jerarquía en una *blockchain* privada. En un sistema centralizado, toda la información está controlada por un único computador o servidor.

Contrato inteligente: Programa de computadora que controla directamente la transferencia de monedas o activos digitales entre partes bajo ciertas condiciones, almacenados en la tecnología *blockchain*.

NOTA

¹ En el artículo, “Virtual Currencies and Blockchain Technology. Irish Departmento Finance. Discussion Paper” (2018). Disponible en línea en: <www.finance.gov.ie/wp-content/uploads/2018/03/Virtual-Currencies-and-Blockchain-Technology-March-2018.pdf>. En la página 3, se puede leer una historia muy contrastada y fiel de las monedas virtuales y la tecnología *blockchain*, junto con una descripción muy completa, rigurosa y actualizada de ambas tecnologías.

² Satoshi Nakamoto (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Disponible en línea en: <<https://bitcoin.org/bitcoin.pdf>>.

³ En España, se creó en 2017 el consorcio Alastria, constituido por un gran número de organizaciones, grandes y pequeñas empresas, centros de investigación, fundaciones y universidades, cuyo objetivo principal es el estudio, investigación y desarrollo de tecnologías *blockchain* para contribuir a su difusión y despliegue y contribuir a su penetración social.

⁴ Es la agencia no regulatoria del Departamento de Comercio de los Estados Unidos, y cuyo objetivo principal es promover la innovación y la competitividad industrial. El NIST en su origen Oficina Nacional de Normas (NBS), se creó en 1901, y en 1988 cambió su nombre por el actual NIST. El progreso e innovación tecnológica de los Estados Unidos dependen de las habilidades del NIST, especialmente en: biotecnología, nanotecnología, tecnologías de la información y fabricación avanzada. Los trabajos del NIST tienen impacto a nivel mundial en tendencias tecnológicas. Un caso por recordar son las definiciones y marcos regulatorios de la computación en la nube.

⁵ Disponible en línea en: <<https://csrc.nist.gov/news/2018/nistir-8202-blockchain-technology-overview>
<<https://csrc.nist.gov/CSRC/media/Publications/nistir/8202/draft/documents/nistir8202-draft.pdf>>.

⁶ Sara Friedman. Artículo sobre el informe final del NIST disponible en línea en: <<https://gcn.com/articles/2018/10/03/nist-blockchain-overview.aspx>>.

El informe final fue publicado por el NIST. Disponible en línea en: <<https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf>>. En

enero de 2019, el sitio web oficial del NIST se encontraba cerrado por razones de “cierre de organismos nacionales de los Estados Unidos”.

⁷ Pavlus, John (2018) “The World Bitcoin created”, en *Scientific American*, pp. 28-33. La versión española, en su número de febrero 2018 de Investigación y Ciencia, publicó la traducción del dossier y el artículo citado anteriormente de Pavlus.

⁸ “Smart Contracts: Building Blocks for Digital Markets,” 1996, www.alamut.com/subj/economics/nick_szabo/smartContracts.html.

⁹ <https://ethereum.org/developers/#getting-started>

¹⁰ Carrefour. 11 de noviembre de 2018.

¹¹ Disponible en línea en:

<Ibm.com/blockchain/supply.chain>.

¹² Disponible en línea en:

<Interxion.com/es/blogs/2017/04/blockain-se-prepara-para-integrarse-en-el-internet-de-las-cosas-iot>.

¹³ Jayshree Pandya (2019). “A Changing Internet: The Convergence Of Blockchain, Internet Of Things, And Artificial Intelligence”, en revista *Forbes*. Disponible en línea en:

<<https://www.forbes.com/sites/cognitiveworld/2019/07/05/a-changing-internet-the-convergence-of-blockchain-internet-of-things-and-artificial-intelligence/#c4287137c58f>>.

¹⁴ El blog en español de la multinacional DellEMC, también traduce, recoge y amplía los conceptos de la experta Jayshree Pandya comentados anteriormente. Disponible en línea en:

<<https://blog.dell EMC.com/es-es/un-internet-cambiante-la-convergencia-del-blockchain-internet-de-las-cosas-y-la-inteligencia-artificial/>>.

¹⁵ Turgeon, Jean. *Dossier Blockchain IoT*.