Facultad de Economía, Empresa y Turismo
Universidad de La Laguna

MEMORIA DEL TRABAJO DE FIN DE GRADO

IMPACTO DE LA TECNOLOGÍA BLOCKCHAIN EN LA ACTIVIDAD PRODUCTIVA EMPRESARIAL

IMPACT OF BLOCKCHAIN TECHNOLOGY ON BUSINESS PRODUCTIVE ACTIVITY

AUTORAS:

Ainara García Hernández (54112301V)

Gema María Pérez Hernández (79089718D)

Laura Suárez Delgado (79086768A)

TUTOR:

Teodoro Ravelo Mesa

Grado en ADMINISTRACIÓN Y DIRECCIÓN DE EMPRESAS

FACULTAD DE ECONOMÍA, EMPRESA Y TURISMO

Curso académico 2018/2019

Convocatoria de Junio

En San Cristóbal de La Laguna, a 12 de junio de 2019

RESUMEN

El término blockchain está cobrando un protagonismo considerable en la economía actual. Las múltiples ventajas que ofrece esta tecnología, han despertado el interés de grandes empresas que buscan una mayor rentabilidad reduciendo costes y tiempos.

Con el objetivo de conceptualizar esta nueva herramienta y estudiar sus aplicaciones en los diferentes sectores, así como los principales motivos de la ralentización de su expansión, hemos consultado informes, manuales, blogs y artículos web entre otras fuentes.

Blockchain nace como una propuesta de registro de información distribuido, y opera de manera que cada uno de los ordenadores o servidores conectados tienen una copia del mismo. Su integridad se asegura por medio de la criptografía, lo cual nos permite prescindir de las terceras partes de confianza.

Son muchos los sectores productivos que han apostado por la incorporación de esta tecnología cuyas características aportan un indudable valor a sus procesos. Sin embargo, existen una serie de desafíos que frenan su adopción.

Palabras clave: blockchain, criptografía, registro de información distribuido, sectores productivos

ABSTRACT

The term blockchain is gaining considerable prominence in today's economy. The multiple advantages offered by this technology have aroused the interest of large companies seeking greater profitability by reducing costs and times.

With the aim of conceptualizing this new tool and studying its applications in different sectors, as well as the main reasons for the slowdown in its expansion, we have consulted reports, manuals, blogs and web articles among other sources.

Blockchain was born as a proposal for the registration of distributed information, and operates in such a way that each of the connected computers or servers have a copy of it. Its integrity is ensured through cryptography, which allows us to dispense with trusted third parties.

Nowadays, there are many productive sectors that have opted for the incorporation of this technology whose characteristics provide undoubted value to their processes. However, there are a number of challenges that hinder its adoption.

Keywords: blockchain, cryptography, distributed information register, productive sectors

ÍNDICE

ÍNDICE DE FIGURAS, TABLAS Y GRÁFICOS

CAPÍTULO 1. INTRODUCCIÓN

1.1. Desarrollo de la industrialización

Para hablar de la industria debemos remontarnos a mitad del siglo XVIII, cuando comienza la *Primera Revolución Industrial* en Europa, expandiéndose posteriormente al resto del mundo. Es entonces cuando parte de la producción empieza a dejar de ser manual para mecanizarse.

Los sectores del transporte y textil fueron los verdaderos pioneros en esta revolución.

En Reino Unido la industria textil, que ya tenía mucha importancia, evolucionó de pequeñas fábricas artesanales a grandes fábricas mecanizadas.

El transporte, tanto para personas como para mercancías, se vio revolucionado con la llegada de la máquina de vapor. Ésta dio paso a las locomotoras, siendo la primera patentada en 1769. El carbón tomó cada vez más relevancia, pues fue fundamental en esta primera revolución industrial como combustible para las nuevas máquinas de transporte que estaban surgiendo.

La comunicación dio también un giro en esta época con la aparición del teléfono y el telégrafo.

Casi un siglo después, en 1850, llegó la *Segunda Revolución Industrial* con el desarrollo de las industrias químicas, eléctricas y automovilísticas. El carbón como combustible quedó atrás para dar paso al petróleo, que empezó a usarse en los coches y aviones a los que se dio vida en esta época.

La industria eléctrica comenzó a desarrollarse y con ella evolucionaron los anteriormente mencionados telégrafo y teléfono, que, aunque su invención pertenece a la primera revolución industrial, su auge llegó en la segunda.

Los estudios del electromagnetismo consiguieron la primera transmisión de señales de telegrafía sin el uso de hilos. Estos hallazgos fueron de vital importancia para la posterior creación de la radio.

En 1876, Graham Bell patentó el teléfono. Fue entonces cuando su uso comenzó a expandirse por las ciudades llegando a cada hogar en el siglo posterior.

En la segunda mitad del siglo XX, llegó la *Tercera Revolución Industrial*, en la que destaca el uso de la electrónica y la tecnología de la información y las telecomunicaciones. Los avances conseguidos en esta tercera revolución en lo que respecta a la energía, es en lo que se basan las actuales búsquedas de un sistema energético más sostenible.

El petróleo sufre una gran subida de precio en esta época, por lo que se empieza a buscar alternativas. El vehículo eléctrico ya había sido diseñado en el siglo anterior, pero es ahora cuando gracias a la conciencia social y su desarrollo, vuelve a considerarse como una opción viable.

Las computadoras comenzaron su desarrollo con Alan Turing, produciéndose el gran avance en este campo en la década de 1960 con la creación de los primeros ordenadores personales, presentes actualmente en todos los hogares, haciendo de la comunicación un imprescindible en la actual vida diaria.

Internet llega en la década de los 80 con una conexión directa entre redes que crea un sistema global de comunicación descentralizada. En 1991 se registra el primer trabajo de cadena de bloques por Stuart Haber y W. Scott, siendo en 1992 cuando se introduce *el árbol de Merkle*.

Pocos años después aparece el *hashcash*, tecnología cuya finalidad era reducir el correo no deseado y los ataques de denegación del servicio; es la contrapartida al spam. Esta tecnología se populariza años más tarde por su implementación en el Bitcoin.

1.2. Desarrollo del Blockchain: del Bitcoin al Ethereum

A finales de 2008 una persona o grupo de personas bajo el pseudónimo de Satoshi Nakamoto, publicaron el primer documento sobre el Bitcoin.

Además de hablar por primera vez de este concepto, Satoshi desarrollo la primera versión del Bitcoin y fue el primer usuario de su propia moneda. Hoy en día sigue siendo una gran incógnita el verdadero nombre de Satoshi Nakamoto, y aunque este tema ha sido el centro de un gran debate y el núcleo de múltiples investigaciones, nadie ha podido confirmar su identidad a pesar de no faltar hipótesis al respecto. Lo que sí se sabe con seguridad, es que esta persona o grupo de personas, son actualmente consideradas de las más ricas del mundo, al acumular la cifra de 1.000.000 de Bitcoin que jamás han sido usados.

La historia del Blockchain comienza con la creación del primer bloque Bitcoin, denominado *"bloque génesis"*, que se elaboró el 3 de enero de 2009.

El valor de Bitcoin se mantuvo bajo y constante durante algunos años, hasta que en 2017 tuvo un gran crecimiento en valor y uso.

Cuando el Bitcoin comenzó a crecer, se convirtió en el objetivo de inversionistas, que aprovechaban las fluctuaciones constantes de la criptomoneda para comprar y vender generando altos beneficios. Su aumento de valor consiguió también llamar la atención de los hackers, que comenzaron a tener una gran relevancia en este mercado, ya que sus acciones estaban directamente relacionadas con el valor del Bitcoin en cada momento.

En 2013 se hizo pública la primera prueba de concepto de una nueva criptomoneda llamada *"Ethereum"*. A mediados de 2015 tuvo lugar el cálculo de su bloque génesis y, por tanto, el comienzo del uso de esta nueva criptomoneda que vino de la mano de los Smart Contracts (contratos inteligentes) que ayudaron a la creación de las ICOs (oferta inicial de moneda).

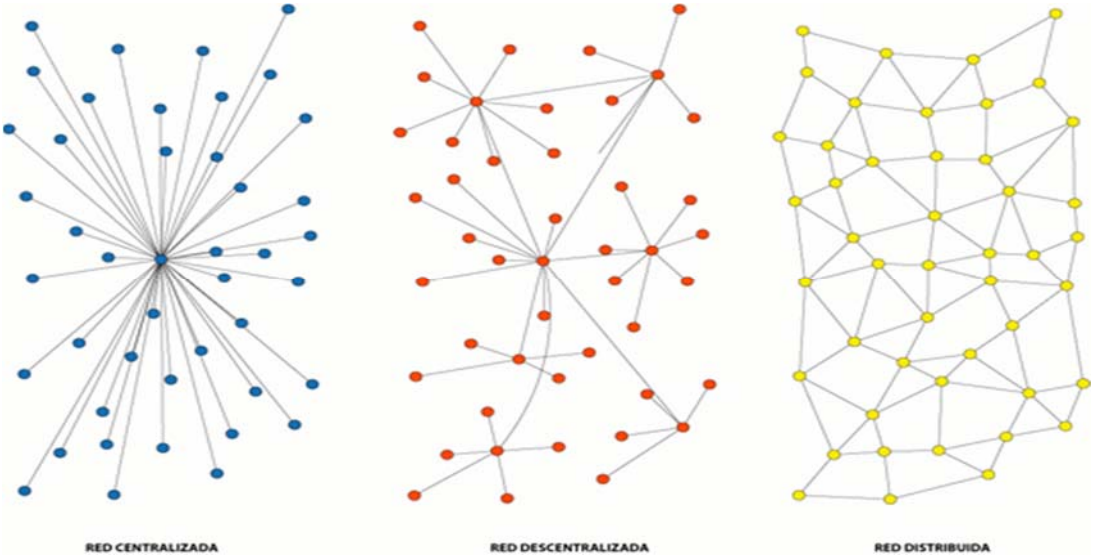
La simplicidad de estos dos nuevos conceptos hizo que las criptomonedas entraran en un nuevo periodo histórico, pues el lanzamiento de nuevas ICOs era diario y empezó a buscarse financiación para la creación de nuevas criptomonedas.

Las redes peer-to-peer (P2P) fueron un gran hallazgo y cobraron gran importancia desde el mismo momento en el que surgieron, pues han sido fundamentales para el desarrollo tecnológico y son muy importantes en Bitcoin.

Las P2P dieron solución al mayor de los problemas de las redes centralizadas y descentralizadas. El principal problema de *las redes centralizadas* es que, al depender todos de un único servidor, si este falla, todo falla. En *la red descentralizada*, este problema se minimiza, pues la red central,

tiene varios servidores, de los que, a su vez, dependen otros servidores, por lo que si uno falla, solo falla una parte del sistema.

Figura 1: Redes de datos centralizadas, descentralizadas y distribuidas



Fuente: icommunity.io

Las P2P plantean una solución: *la red distribuida*. Todos los servidores están conectados entre sí, por lo que, si uno falla, no afecta a ningún otro.

Este tipo de red expone otros beneficios, como que la información de un nodo, no se elimina al suprimirlo, sino que ésta sigue en la red, pero en otro nodo diferente. Es decir, nada es imprescindible pues la información siempre es compartida.

CAPÍTULO 2. EL BITCOIN

2.1. Criptomonedas

Las criptomonedas son monedas virtuales que no están controladas por ningún ente gubernamental ni financiero y operan como cualquier otra divisa tradicional.

Se pueden considerar como una alternativa a las divisas tradicionales, pero se crearon como una solución al pago convencional.

El valor de la criptomoneda:

- No está vinculado con el comportamiento de la economía.
- Los cambios en el tipo de interés y el aumento de las reservas monetarias tienen un efecto indirecto al valor de la criptomoneda.
- El valor de estas dependerá del valor de los usuarios por mantener su precio al convertirlas en divisas tradicionales.

Por ello, actualmente, son tratadas como una materia prima.

2.1.1. Beneficios y riesgos de las criptomonedas

Beneficios:

- Visión global: Divisas globales que no son susceptibles a las economías o políticas de un país.
- Descentralización: No existe un mercado oficial, pueden estar operando todos los días.
- Volatilidad: Las criptomonedas pueden experimentar diferentes cambios en su precio de manera repentina. Como trading, estas fluctuaciones suponen una oportunidad.
- Transparencia: Todas las transacciones se registran en un libro compartido y se opera sobre un mecanismo que asegura que llegue al receptor la información que necesita el emisor.

Riesgos:

- Volatilidad: Como divisa, las inesperadas variaciones en el precio se convierten en un riesgo para las criptomonedas.
- Pérdidas: No existe ningún sistema implantado para la protección y compensación de posibles fraudes.
- Ampliación aceptación: Las criptomonedas tienen el valor que se les quiera dar.
- Cambios regulatorios: Exentas de regulación.

2.1.2. Divisa tradicional vs criptomoneda

Las criptomonedas se han presentado como una alternativa para las monedas tradicionales. El principal motivo de que las divisas digitales sean cada vez más populares, se debe a que se encuentran dentro de un sistema descentralizado cuya actividad no está regulada por ningún organismo público.

Es la diferencia más importante con respecto a las divisas tradicionales, ya que el valor de éstas siempre va a estar determinado por alguna entidad financiera.

Tabla 1: Diferencias entre divisa tradicional y criptomoneda.

Divisas tradicionales	Criptomonedas
Físicas	Digitales
Vinculadas a un país concreto o grupo de países	Globales
Emitida por el gobierno	Ofrecida a través de minería
Se inyectan en el sistema económico a través de bonos y otros títulos	Se inyectan directamente en el mercado de las criptomonedas
Oferta controlada por los bancos centrales	Oferta controlada por mineros y la tecnología de la minería
Reciben influencia de las tasas de inflación y de interés	Reciben poca influencia de políticas monetarias

Fuente: elaboración propia

2.2. El Bitcoin

El Bitcoin es una moneda virtual que sirve para intercambiar bienes y servicios. Se caracteriza por su eficiencia, seguridad y facilidad de intercambio. Es un sistema entre pares (peer-to-peer) distribuido. No existen ningún punto de control "central". Los Bitcoins se crean en el proceso de "minería", que se basa en buscar una solución a un algoritmo matemático a la vez que se procesan las transacciones.

El almacenaje y transmisión de valor entre los usuarios de Bitcoin se lleva a cabo por el uso de las unidades monetarias creadas por los mineros.

Los usuarios de la red se comunican entre ellos usando el protocolo bitcoin. La pila de protocolos bitcoin, disponible como software open source, se puede ejecutar desde diferentes dispositivos por lo que hace que sea una tecnología fácilmente accesible.

Los usuarios pueden transferir bitcoins a través de la red para realizar cualquier transacción que se pueda realizar con monedas convencionales. Los bitcoins se pueden comprar, vender o intercambiar por otras monedas en las casas de cambio especializadas.

Estas monedas están implícitas en las transacciones que se mueve el valor desde el remitente al destinatario. Todo usuario posee unas claves que permiten demostrar la propiedad de las transacciones en la red bitcoin. Estas claves suelen almacenarse en una cartera "Wallet" en la terminal de cada uno de los usuarios.

2.2.1. Orígenes del Bitcoin

El comercio de internet tradicionalmente ha venido a depender exclusivamente de instituciones financieras las cuales han servido de terceros confiables para el proceso de pagos electrónicos. El sistema ha funcionado generalmente bien a pesar de las debilidades inherentes del modelo basado en confianza. Por ello, en 2008 Satoshi Nakamoto hizo público un documento llamado "*Bitcoin: Peer-to- Peer Electronic Cash System*". En este documento se explicaba, a modo teórico, un medio de pago global sin intermediarios.

La existencia de las criptomonedas viene relacionada con el desarrollo de la criptografía. A finales de la década de los 80, muchos investigadores comenzaron a intentar utilizar la criptografía para realizar monedas virtuales. Estas primeras monedas virtuales iban respaldadas por alguna moneda nacional o por el oro. Estas monedas funcionaban, eran centralizadas y una "presa" fácil para los gobiernos o los hackers. Para ser fuerte frente a la intervención tanto del gobierno como de los hackers, era necesaria la existencia de una moneda digital descentralizada.

Bitcoin es ese sistema completamente descentralizado por diseño, y libre de cualquier autoridad central o punto de control que pueda ser atacado o corrompido. Este representa la culminación de las décadas de investigación en criptografía y sistemas distribuidos e incluye cuatro innovaciones reunidas en una combinación única y potente.

Se caracteriza por:

- Una red entre pares distribuida (el protocolo bitcoin)
- Un libro contable público (la cadena de bloques, o "blockchain" de la cual hablaremos en los próximos capítulos)
- Un sistema distribuido, matemático y determinístico de emisión de moneda (minería distribuida)
- Un sistema descentralizado de verificación de transacciones (script de transacciones)

2.2.2. Características del Bitcoin

- No pertenece a ningún Estado o País: Es una divisa que se puede utilizar en todo el mundo por igual.
- Se puede comprar bitcoin con cualquier moneda o divisas.
- No existen intermediarios: por lo tanto, las transacciones se realizan de persona a persona.
- Descentralizada: no es controlada por ningún gobierno, institución financiera o empresa.
- No es falsificable: a día de hoy no ha sido posible falsificarla o duplicarla esto es gracias a sistema criptográfico.
- Las transacciones son irreversibles.
- Preserva la identidad: No es necesario revelar la identidad de los usuarios a la hora de realizar alguna transacción.
- El dinero no puede ser intervenido por nadie.

2.2.3. Beneficios y riesgos del Bitcoin

El bitcoin presenta los siguientes beneficios:

- *Libertad de pago*: Se podrá enviar y recibir cualquier cantidad de dinero de manera instantánea independientemente del lugar y del momento.
- *Tasas muy bajas:* Los pagos con Bitcoin actualmente se pueden realizar con tasas muy bajas o sin tasas. Se puede incluir una tasa en todas las transacciones para que éstas tengan prioridad sobre las demás.
- *Menores riesgos para los comerciantes:* Las transacciones con bitcoin son seguras e irreversibles y no contienen ni datos personales ni privados de los comerciantes.
- *Seguridad y control:* Los usuarios de la red Bitcoin tienen el completo control sobre las transacciones que realizan. Los pagos con Bitcoin pueden realizarse sin estar asociados a datos personales. Esto ofrece un alto nivel de protección contra el robo de identidad. Además, los usuarios de Bitcoin pueden proteger su dinero con copias de seguridad y encriptación.
- *Neutral y transparente:* Toda la información referente al Bitcoin se puede encontrar en la cadena de bloques para que cualquiera la pueda verificar y usar. Nadie puede controlar o manipular el protocolo bitcoin porque es criptográficamente seguro
- Sin embargo, tiene como desventajas:
- *El grado de aceptación:* Actualmente, no son muchas las personas ni comercios que conocen el Bitcoin.
- *La volatilidad:* Es de suponer que a volatilidad irá disminuyendo a medida que el mercado y la tecnología Bitcoin maduren.
- *Desarrollo en curso:* A día de hoy aún se están desarrollando herramientas, características y servicios para hacer que Bitcoin sea más accesible y seguro.

2.3. El Ethereum

Vitalik, un programador y escritor ruso conocido principalmente por ser el cofundador de Ethereum y Bitcoin Megazin, lanzó un documento teórico donde se establecieron nuevas funcionalidades. Se plantea que la red no fuera solo una entidad para almacenar y validar transacciones, sino que también, actuara de intermediario de ejecución de contratos. De aquí nació el concepto *"Smart Contract"*.

Los contratos inteligentes *(Smart Contracts)* se comenzaron a desarrollar desde 1993 por el criptógrafo Nick Szabo. Éste, desarrolló un programa informático que ejecuta los acuerdos celebrados entre dos o más partes asegurándose que ciertas acciones sucedan como resultado de que se cumplan una serie de condiciones específicas.

Los objetivos principales de los Smart Contracts son:

- Creación de un estado de seguridad superior al de los contratos tradicionales.
- Reducción de costes.
- Reducción del tiempo asociado a estas interacciones.

Es un programa capaz de ejecutarse automáticamente, sin necesidad de la intervención de terceros.

Estos contratos se caracterizan por ser:

- *Públicos:* Se almacenan en la Blockchain y cualquiera puede acceder.
- *Inmutables:* Una vez almacenados no se pueden cambiar.
- *Configurables:* Solamente los dueños, mediante claves, puede cambiar ciertas variables.
- *Comunicativos:* Se pueden alegar entre ellos.
- *Distribuidos:* Son los mineros los que lo ejecutan independientemente del país en el que se encuentre.

"Cabe destacar que, los Smart Contracts, no son exclusivo del Ethereum, sino que en el Bitcoin ya se desarrollaban. Ethereum transforma los smart contracts de bitcoin a otro nivel. Ethereum, que es uno de los proyectos más famosos en el sector de los smart contracts, es una plataforma de computación distribuida basada en una blockchain pública como Bitcoin y que además permite ejecutar contratos inteligentes P2P (entre los nodos, sin servidores centrales) en una máquina virtual descentralizada llamada *Ethereum Virtual Machine (EVM).*

Se basa en toda la teoría de Bitcoin en cuanto a estar distribuido, tener su propia criptomoneda, mineros e incluso su propio blockchain entre otras cosas pero, a diferencia de Bitcoin, Etherum ha creado un intérprete de lenguaje de programación mucho más extenso (*Turing completo*), permitiendo añadir lógica mucho más compleja dentro del blockchain. Es decir, se podría asemejar a un ordenador distribuido, el cual utiliza su criptomoneda *(el ether)* como la "gasolina" que necesita el contrato para que los mineros puedan ejecutarlo. Es decir, ahora con Ethereum los contratos son programas con muchas más funcionalidades y posibilidades. Aunque para ello, y esto es algo que mucha gente les critica, han tenido que crear toda una nueva red de cero, renunciando a la red de Bitcoin (la más potente del mundo).

Todas las aplicaciones funcionan en una blockchain con una potencia de cómputo muy alta que permite a los desarrolladores crear aplicaciones descentralizadas (DAPPS): Organizaciones Autónomas Descentralizadas (DAO), Mercados de intercambio, …" (Fuente: https://academy.bit2me.com)

CAPÍTULO 3. LA TECNOLOGÍA BLOCKCHAIN

Desde que Bitcoin incorporó el uso de la tecnología blockchain, el interés por la misma ha ido creciendo exponencialmente. El éxito obtenido en el campo de las criptomonedas ha tenido repercusión a nivel global motivando el interés por descubrir su potencial para ofrecer soluciones en múltiples áreas. Blockchain es una herramienta útil que va más allá de las bases de datos centralizadas en las que los datos se almacenan en un único lugar físico.

Hoy en día vivimos en un mundo que necesita producir, gestionar, almacenar y compartir información certificada continuamente. Blockchain nace como una propuesta de registro de información distribuido, y opera de manera que cada uno de los ordenadores o servidores conectados tienen una copia del registro.

Esta tecnología, que hace pocos años parecía indeleble unida a la creación de monedas criptográficas, está asumiendo el papel de guardián en la emergente "economía de confianza".

3.1. Blockchain: definición y propiedades

El término inglés blockchain significa cadena de bloques, los cuales pueden contener diferentes tipos de información como por ejemplo: transacciones, contratos, identidades, activos o cualquier cosa que pueda ser descrita en forma digital.

Dado su protagonismo en el híper-ciclo de Bitcoin, puede haber alguna confusión sobre qué es esta tecnología y el valor que potencialmente puede ofrecer a los negocios. A grandes rasgos, podemos definir la blockchain como *una contabilidad pública que mediante una red distribuida de ordenadores proporciona una forma de registrar y compartir información con toda una comunidad sin la participación de terceros que actúen como intermediarios*.

Si desglosamos esta definición, podemos observar algunas de las propiedades más importantes que sustentan la red Blockchain.

"Una contabilidad pública…" El carácter público de esta red permite que la actualización o validación de la información pueda ser vista por todos los participantes de la misma.

"… que mediante una red distribuida de ordenadores…" la cadena de bloques funciona como una red *P2P (peer-to-peer)* formada por un conjunto de ordenadores interconectados llamados "nodos"

"…proporciona una forma de registrar y compartir información con toda una comunidad…" Cada participante de esta comunidad tiene su propia copia de la información y todos los miembros tienen que validar colectivamente cualquier actualización.

"…sin la participación de terceros que actúen como intermediarios" esta red tiene un carácter descentralizado puesto que el intercambio se realiza de usuario a usuario sin que un ente principal controle ese tráfico de datos en la red.

Además de las anteriores, esta tecnología presenta otras propiedades que son cruciales para entender su funcionamiento:

- Irreversibilidad e inmutabilidad: Una vez que se ha grabado un dato o se ha realizado una transacción en la cadena de bloques, es imposible de eliminar. Esto sólo sería posible si el resto de participantes estuviese de acuerdo.

- Criptografía y seguridad: la criptografía es la técnica de codificar información con claves secretas, de tal forma que lo escrito solamente sea inteligible para quien sepa descifrarlo. Blockchain la emplea para garantizar la seguridad en las transacciones de sus miembros.

- Privacidad y transparencia: La cadena de bloques proporciona verificabilidad pública de su estado general sin filtrar información sobre el estado de cada participante individual.

- Cronología: cada bloque tiene una marca de tiempo que dota a todas las transacciones de ese bloque con ese registro temporal.

- Rapidez a bajo coste: La blockchain hace posible que las transacciones se realicen de forma más rápida que a través de una entidad central como los bancos. Asimismo, también influye en los costes ya que, si se eliminan los intermediarios, se abarata el proceso de realizar transacciones en la red.

3.2. Fundamentos principales para entender su estructura y funcionamiento

Para comprender mejor esta tecnología es necesario conocer los elementos básicos que la respaldan.

El primer elemento a considerar son *los nodos*, equipos informáticos que sostienen su infraestructura y almacenan el libro de cuentas como un libro mayor de contabilidad. Estos nodos son unidades iguales entre sí y generan una red entre pares P2P.

A medida que va aumentando la necesidad de almacenar nueva información, es necesario actualizar el sistema. Cada actualización conlleva la creación de un nuevo bloque. Esta labor corresponde a un subgrupo de nodos que constituyen un elemento clave dentro la red blockchain: *los mineros.*

Los mineros son los nodos que se encargan de crear bloques a través de la resolución de un problema matemático complejo que requiere de una gran potencia de computación. Básicamente resuelven puzles criptográficos de enorme y deliberada complejidad (López y López, 2017). Por su contribución, los mineros reciben una compensación económica normalmente en criptomonedas.

Una vez hallada la solución, ésta es compartida con el resto de la comunidad para su validación en un proceso llamado *"proof of work"*, siendo este otro factor relevante en el proceso. Digamos que proof of work (*prueba de trabajo* en español) es una especie de *captcha*[1] para sistemas

[1] **Captcha** *(Completely Automated Turing test to tell Computers and Humans Apart)* es una **medida de seguridad implementada en la mayoría de páginas web**, o más bien en sus formularios de registro o introducción de datos para detectar si quien los rellena es realmente una persona o un bot automatizado. Se le suele identificar por ser un sistema que lanza una pregunta por responder, o que exige introducir una serie de palabras o incluso señalar fotografías.

informáticos. Actualmente es una pieza fundamental en las criptomonedas como Bitcoin, permitiendo alcanzar el consenso dentro de una red Blockchain.

Otro elemento a destacar de su estructura, son los ***bloques*** por los está compuesta. Tal y como mencionábamos anteriormente, la red blockchain está compuesta por diferentes bloques que contienen diversos tipos de información. Estos bloques están interconectados con su predecesor y su sucesor por medio del ***hash***, formando así una cadena.

El hash, es un número único e irrepetible que identifica cada bloque. Podemos utilizar el término *"huella digital"* como símil para hacernos una idea de su función. Este número se genera conforme a la información contenida en cada bloque, por lo que cada uno tiene el suyo propio.

El hash y la visión de toda una comunidad, son los dos motivos principales que hacen que esta red sea "inhackeable". Por un lado, si un usuario alterase la información de un bloque, su hash cambiaría y no encajaría con su predecesor y su sucesor. En consecuencia, la cadena quedaría invalidada. Por otro lado, en esta comunidad, cada usuario mantiene su propia copia de la información, y todos los miembros tienen que validar colectivamente cualquier actualización. La distribución de los mineros significa que el sistema no puede ser hackeado por una sola fuente. Si alguien intenta manipular la información de un libro mayor con fines maliciosos, los nodos estarán en desacuerdo con la integridad de ese libro y rechazarán la incorporación de esa modificación a la cadena. Por tanto, podemos decir que la seguridad de este sistema se la dan sus propios usuarios.

Un último apunte sería diferenciar los tipos de blockchain que existen en función del grado de acceso: *las públicas, las federadas y las privadas.*

Las blockchain públicas son aquellas en las que cualquier persona o entidad puede integrarse libremente y cuya información se distribuye por igual entre los nodos, teniendo así un carácter descentralizado.

Las federadas han ido surgiendo con la idea de servir como registros descentralizados que permiten generar confianza en entornos complejos con entidades con diferentes intereses. En general no son públicos, sino que un número determinado de organizaciones, entidades o compañías se encargan de administrar la red y mantener copias sincronizadas del blockchain. El acceso generalizado es en este caso mediante una interfaz web que estos administradores ponen a disposición de los usuarios.

A diferencia de las anteriores, las blockchain privadas presentan un carácter más jerarquizado y el usuario debe ser invitado para formar parte de ella.

3.3. Funcionamiento de la red Blockchain

Teniendo en cuenta los múltiples elementos descritos en el epígrafe anterior, explicaremos de forma muy general el funcionamiento de la cadena de bloques:

El primer paso es acceder a la red. Los futuros usuarios que quieran formar parte de la red tienen dos opciones según el tipo de blockchain que se vaya a utilizar: descargarse la app correspondiente que les convierte en un nodo con los mismos derechos que los demás, o acceder vía una interfaz web.

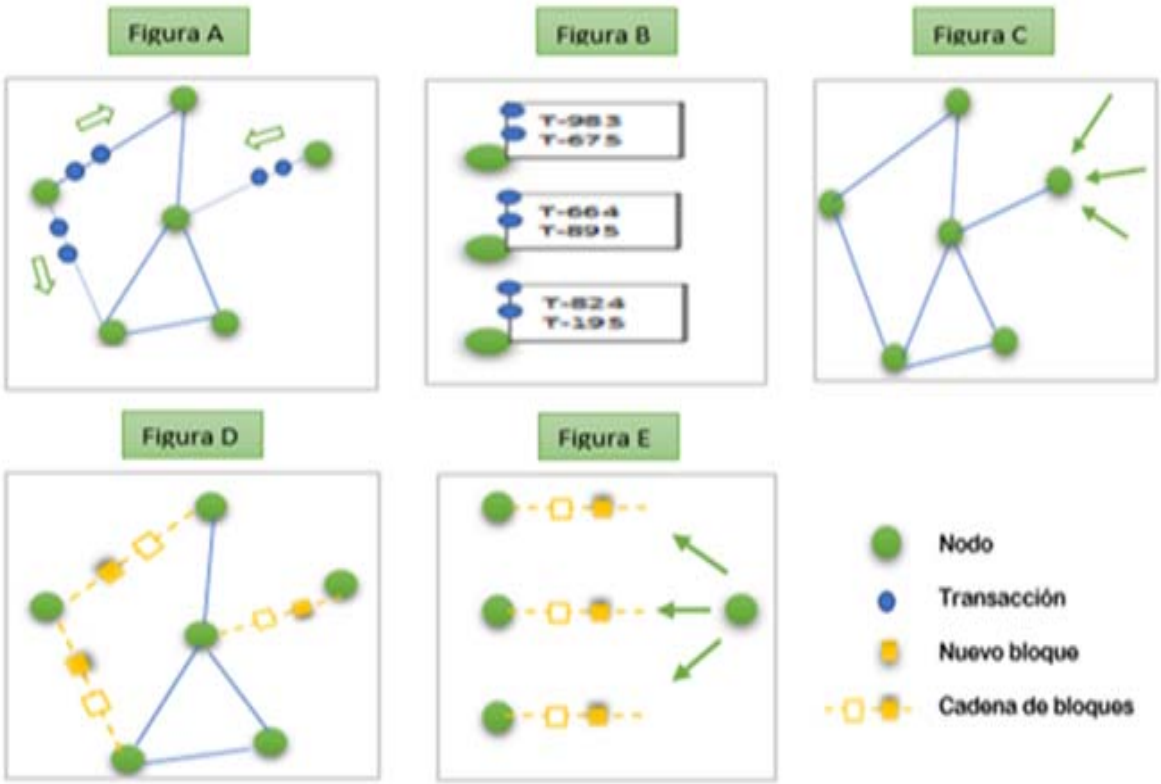
Una vez los participantes están conectados a la cadena, el siguiente paso consiste en enviar información en forma de transacción *(Figura 2-A).* Es decir, cuando un nodo quiere realizar una transacción, envía la información sobre ésta a los nodos con los que está conectado y cada uno de ellos comprobará la validez de la misma -por ejemplo, que no se esté intentando transferir un dinero que ya haya sido gastado-. En caso de que la transacción sea correcta, cada nodo la añade a su lista de transacciones ***"pool"*** y la reenvía a los nodos a los que cada uno de ellos está conectado. De esta forma, cada nodo va llenando su pool con las transacciones que va escuchando. *(Figura 2-B)*

Cada cierto tiempo, -que dependiendo de la blockchain puede variar desde unos pocos segundos hasta varios minutos-, un nodo es escogido aleatoriamente en un proceso conocido como ***"protocolo de consenso"*** para proponer un bloque. *(Figura 2-C)*

El usuario seleccionado propone un bloque nuevo con las transacciones que ha ido "escuchando" y registrando en su pool. Antes de ser enviado a los demás nodos, este bloque ha de ser validado con un hash. El sistema solo acepta el bloque si tiene un hash válido*. (Figura 2-D)*

Finalmente, en caso de resultar correcto, el resto de nodos verifican que todas las transacciones también sean correctas y actualizan su copia de la cadena con esta nueva versión contenida en el nuevo bloque. *(Figura 2-E)*

Figura 2: Funcionamiento de la red Blockchain

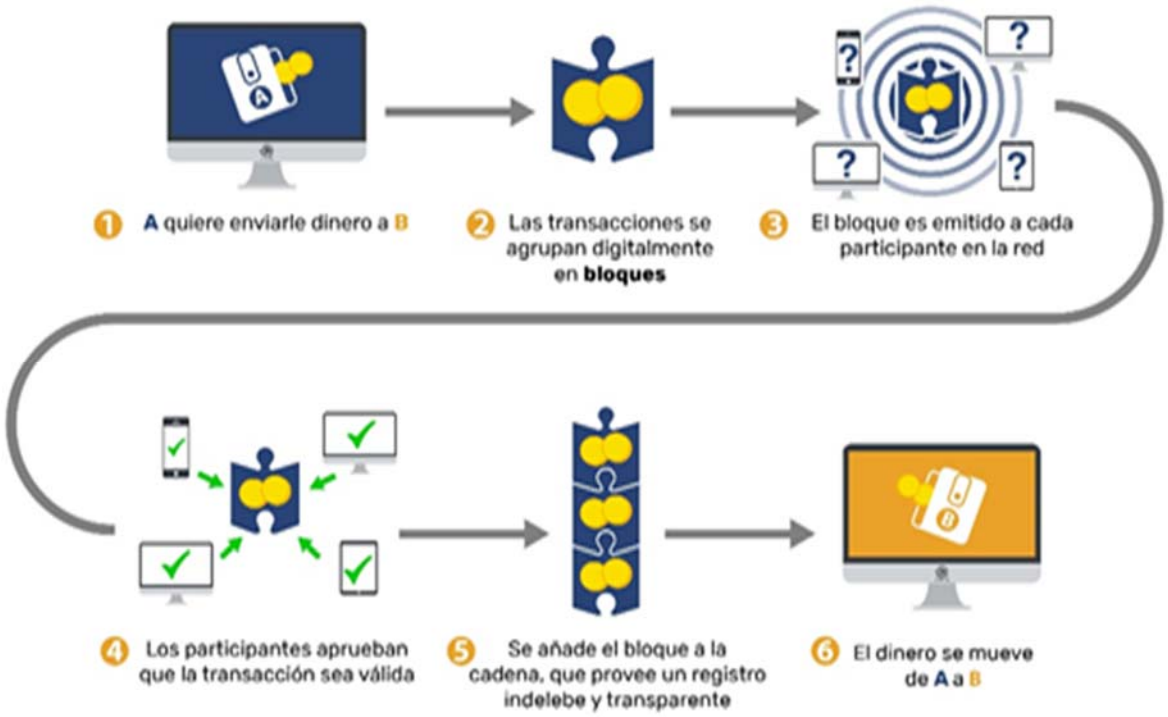


Fuente: elaboración propia partiendo de Allende y Colina (2018)

Para tener una visión más completa del funcionamiento de esta red, veamos un ejemplo:*(Fig. 3)*

Supongamos que los participantes A y B tienen acceso a una billetera digital que les permite enviar o recibir monedas. A quiere transferir cierta cantidad a B. El usuario A, al tomar esta decisión, envía una instrucción de cambio a la base de datos informando que parte de sus unidades valor ahora pasan a pertenecer al usuario B. Esta orden es difundida en la red y se verifica si A tiene recursos para efectuar la transferencia y, si es correcto, esta instrucción se agrupa en un bloque junto con otras transacciones que han tenido lugar en un mismo intervalo de tiempo determinado, imaginemos que en los últimos 10 minutos. Este bloque mezcla la información de las partes involucradas de cada transacción, la cantidad, el tiempo y lo procesa a través del hash. Una vez validado, el bloque se añade al final de la cadena con la nueva actualización dando lugar a la transferencia de A a B.

Figura 3: Transacciones de dinero en la red Blockchain



Fuente: plus58minning.org

CAPÍTULO 4 ACCIONES CONCLUYENTES Y APLICACIONES INNOVADORAS DE LA TECNOLOGÍA BLOCKCHAIN

Tras la revisión de los fundamentos de la tecnología blockchain, podemos decir que actualmente, constituye una herramienta fundamental de innovación y desarrollo dentro del presente proceso de digitalización de la actividad productiva y de las futuras perspectivas de la industria 4.0.

Los diferentes sectores productivos están empezando a considerar el gran potencial y los posibles beneficios que puede ofrecer a sus negocios y, aunque ha sido el sector financiero el pionero en detectar la utilidad y las ventajas de su incorporación, otros sectores como el industrial, el asegurador, el sanitario, el sector medioambiental y el sector público, valoran como esta innovadora tecnología puede cambiar su forma tradicional de actuación.

4.1. Aplicación en el sector financiero

El sector financiero, ha tardado en darse cuenta del valor que brinda el sistema blockchain. Sin embargo, a día de hoy, son muchos los bancos que han invertido importantes sumas de dinero en su desarrollo. Este creciente interés puede estar motivado por lo disruptiva que es esta tecnología para el sector, especialmente si simplifica los procesos bancarios y reduce considerablemente los costos.

La tecnología blockchain puede cambiar potencialmente la forma en la que se relacionan los bancos con sus clientes. Destacamos algunos beneficios como:

- *Reducción de costes.* Blockchain obvia la figura del intermediario, como son las cámaras de compensación. De esta forma, se eliminaría las tarifas que éstos cobran por sus servicios. Podemos decir que esta significativa reducción en los costes provocaría una mejora en la posición de los bancos desde un punto de vista de capitalización.

- *Un sistema de pagos efectivo.* Mediante un sistema de bloques optimizado orientado al usuario, un pago puede ser efectivo en unos segundos. Este hecho reducirá el tiempo y los costes relacionados con la transacción.

- *La creación de una identidad digital.* Blockchain permitiría la verificación independiente de los clientes por parte de una organización. Comprobaría la documentación que éste aporta y el banco podría compartir esta información en la cadena de bloques. Cada vez que se proporcione nueva información, se añadirá como un nuevo bloque a la cadena. Ese hecho también beneficiará al resto de identidades, ya que podrán acceder a esta información a tiempo real. De este modo, se crea una identidad digital del cliente que se utilizará para futuras transacciones. No obstante, deben considerarse leyes como el Reglamento General de Protección de Datos.

- *La disminución de delitos económicos.* Las instituciones financieras y las empresas de transferencia de dinero se enfrentan a casos de delito económico, es decir el fraude. Para combatirlo la mayoría de bancos se sustentan en una base de datos centralizada que los hace vulnerables a los propensos ataques de hackers. En los últimos tiempos la seguridad cibernética se ha convertido crucial, por lo que todas las instituciones financieras están siendo alentadas a reforzar sus sistemas. Blockchain puede eliminar o reducir significativamente las transacciones fraudulentas, usando una contabilidad distribuida en la que cada bloque tenga su marca de tiempo y esté vinculado con el bloque anterior. Ante una acción fraudulenta, los bloques no encajarían y dicha modificación quedaría invalidada.

En España, parte del sector financiero junto con empresas e instituciones de diferentes sectores, han creado *Alastria*, la primera red española regulada basada en blockchain. Esta iniciativa, según el artículo *"La banca se suma al Blockchain"* publicado en *elEconomista.es*, permitirá a los usuarios unificar todas sus identidades digitales de forma más segura y decidir con quién compartirla.

Santander, BBVA, CaixaBank o Bankia, son algunas entidades financieras que forman parte de este consorcio basado en blockchain y cada uno de ellos realiza diferentes prácticas que apoyan su implementación.

En el pasado año, el Banco Santander afianzaba las bases de su apuesta por el blockchain desde dentro, donde sus propios accionistas votaron por primera vez las propuestas de su consejo de administración mediante esta tecnología. Casi un año después, blockchain se ha convertido en pieza clave de la estrategia digital de la entidad, que actualmente es socio fundador de la Enterprise Ethereum Alliance (EEA) junto con otros grandes bancos internacionales y otras empresas. "Para Santander, 2019 es un año clave en el impulso blockchain". (InnovaSpain, febrero 2019)

Por su parte, BBVA forma parte del grupo de bancos internacionales para explorar los potenciales beneficios que ofrece su incorporación y han confiado a una start up americana *R3 CEV* el desarrollo de aplicaciones empleando esta tecnología en el sector financiero.

Este proyecto incluye varios bancos entre los que se encuentran *BBVA, Bank of America, Barclays, Goldman Sachs, HSBC, JP Morgan, Morgan Stanley, Société Générale, BNP Paribas, Canadian Imperial Bank of Commerce, ING, Commerzbank, UBS*…

Tal y como se recoge en un artículo web de noticias de la propia entidad publicado en el mes de abril, "el responsable de economía y relaciones institucionales de BBVA, ha aprovechado la reunión del IIF ('*Institue of International Finance*') en Washington, para defender un marco regulatorio del sector financiero que fomente los beneficios potenciales de la tecnología *DLT* (tecnologías de registro distribuido o *'Distributed Ledger Technology*')" entre las que se encuentra el blockchain.

Además, BBVA es uno de los socios fundadores de la *Asociación Internacional de las Aplicaciones Blockchain de Confianza* o *INATBA* (su acrónimo en inglés). Esta asociación promovida por la Comisión Europea, agrupa a 105 organizaciones para tratar de definir un marco global más transparente, predecible y de confianza que permita la adopción de blockchain y la tecnología DLT.

Bankia también ha puesto en marcha un laboratorio blockchain en colaboración con *Innomnia* y está trabajando en varios proyectos usando esta tecnología. La entidad ha creado la plataforma "*stockmind",* con la que se puede *"tokenizar*[2]*"* cualquier tipo de activo y facilitar la creación de mercado, mediante la puesta en contacto entre vendedores y compradores.

Por último, mencionar que CaixaBank, participa en la alianza bancaria internacional formada por UBS, IBM o Commerzbank, con la intención de impulsar la plataforma *"Batavia"* para dar apoyo financiero a operaciones de comercio internacional a través de "blockchain".

[2] ***Tokenizar*** es el proceso de sustitución de un elemento de datos sensibles por un equivalente no sensible, denominado token, que no tiene un significado o valor extrínseco o explotable.

4.2. Aplicación de la tecnología blockchain en la logística y trazabilidad

Las características que sostienen la red blockchain, permiten la creación de plataformas descentralizadas sobre las que realizar la trazabilidad de la historia de un producto, del proceso de fabricación y de la cadena logística, potenciando así la confianza y colaboración entre todos los miembros sin que exista un ente central que controle el proceso.

Todos los agentes que intervienen (proveedores, productores, operadores de logística, minoristas…) podrían crear una huella digital que se iría actualizando cada vez que se interactúa con un elemento en su camino hacia el consumidor final.

Esta plataforma, funcionará en conjunción con elementos de IoT[3](sensores, transponders, códigos QR…) y utilizará smart contracts para fundamentar acuerdos entre las diferentes partes, garantizar que éstos sean satisfechos o controlar el cumplimiento de las regulaciones.

Algunos ejemplos serían: el control del cumplimiento de la cadena de frío, las regulaciones ambientales o la automatización de transacciones de mercancías.

Una plataforma así, presenta una capacidad para mejorar la eficiencia y reducir los costes en los distintos ámbitos de operación. El uso de un registro inmutable permite garantizar quién es el responsable en cada momento del producto transportado. Por otro lado, el mayor grado de integración entre los participantes a nivel de stocks e inventario, puede mejorar los procesos desde una visión más amplia, sincronizando y automatizando la relación entre flujos de inventario, flujos financieros y de datos para conseguir una optimización a nivel de costes y una mejor evaluación de riesgos.

En el ámbito de la logística y transporte de mercancías también se está apostando por la adopción de la tecnología blockchain como palanca de cambio.

Aunque aún se encuentra en una fase muy inicial de adopción con respecto a otros sectores, en el informe *"Cómo impacta Blockchain en la logística 4.0"* de Minsait, se afirma que actualmente se están llevando a cabo diferentes propuestas las cuales agrupamos en los siguientes campos o iniciativas para su incorporación.

4.2.1. Comercio Internacional

Existen varias iniciativas en este ámbito, ya que el comercio internacional representa un escenario perfecto para su aplicación, especialmente en el caso de las operaciones portuarias.

Este entorno presenta un alto grado de complejidad operacional por el elevado número de participantes, la cantidad de procesos a realizar y las necesidades de supervisión y coordinación en los mismos. Por tanto, un modelo que permita reducir la fricción e incrementar la confianza entre sus participantes, supone un aporte de valor.

La logística en el transporte marítimo internacional viene exigiendo desde hace tiempo mejoras en sus procesos. IBM y Maersk, iniciaron una colaboración en junio de 2016 y crearon *Tradelens* como propuesta de solución.

[3] **IoT:** Internet of Things

Tradelens es una plataforma basada en blockchain con la capacidad real de revolucionar el comercio internacional. Es una herramienta eficaz que cuenta con el apoyo de varias organizaciones.

Al emplear esta tecnología como soporte de las cadenas de suministro digitales, los socios comerciales pueden colaborar creando una única vista compartida de una transacción sin comprometer la confidencialidad o la privacidad de la misma. Además, fomenta una mayor eficiencia en la forma en la que sus participantes (líneas navieras, operadores de puertos y terminales, autoridades aduaneras…) interactúan a través del acceso a tiempo real a los documentos de envío de datos.

Por otro lado, mediante el uso de los smart contracts, la plataforma permite la colaboración digital entre las partes involucradas en el comercio internacional.

Esta plataforma estuvo sometida durante un año a una prueba piloto, donde sus fundadores trabajaron con varios socios del sector para detectar amenazas y oportunidades, así como mejorar las posibles debilidades del proyecto. Como resultado, se demostró un 40% de ahorro y 154 millones de eventos comerciales gestionados con éxito.

4.2.2. Transporte terrestre de mercancías

Las iniciativas dentro de este ámbito tienen en común el propósito de fomentar la colaboración y transparencia entre los agentes de la cadena logística. Se orientan a enfoques de negocio desintermediados en el que una plataforma blockchain conecte a los transportistas con los clientes finales.

- *A2b Direct* es una empresa de logística que ha desarrollado una plataforma cuyo servicio proporciona una interacción directa entre transitarios y los propietarios de la carga. Mediante ésta, proporciona servicios de gestión de la identidad de los transportistas, así como rankings basados en datos registrados en blockchain y opiniones de los clientes.

- *PassLfix* plantea el transporte de objetos de forma descentralizada y segura ya que combinando la tecnología blockchain e IoT. se puede probar la transmisión de activos sin necesidad de un tercero de confianza. Con estos ingredientes, PassLfix propone una nueva forma de transferir bienes, usando Smart contracts para gestionar las entregas, y activos digitales para el pago de tasas y depósitos.

- *Hagglin* nace como el primer mercado peer-to-peer del mundo que adopta un sistema de logística peer-to-peer. Con el auge de marketplaces desintermediados y de plataformas de desintermediación para el envío de mercancías, Hagglin pretende facilitar una plataforma única y global cuyo objetivo es que cualquiera pueda comprar, vender o intercambiar cualquier cosa, en cualquier momento, y desde cualquier lugar, y que dichos bienes se entreguen mediante los propios miembros de la comunidad.

4.2.3. Trazabilidad de producto

Blockchain está despertando gran interés en este campo. Debido a la creciente demanda de transparencia por parte de los consumidores y la necesidad de seguridad y control desde el punto de vista de la salud pública, el uso de esta tecnología resulta atractivo para proporcionar valor.

- *Provenance* está desarrollando un sistema de trazabilidad y productos con el objetivo de garantizar que la información que se almacena es segura, auditable, inmutable y accesible. Los productos podrán incorporarse al sistema de trazabilidad a través del etiquetado, Smart tags o código en un sitio de comercio electrónico, y la plataforma blockchain (basada en tecnología Ethereum) actuará como un sistema descentralizado en el que formarán parte los participantes de la cadena de suministro. En algunos mercados como Japón, Estados Unidos y Reino Unido, ya se han realizado pruebas con blockchain para la trazabilidad de la cadena de producción y suministro de alimentos.

- *Ripe.io* plantea un nuevo nivel de transparencia en cuanto al origen de los alimentos y su viaje hasta el consumidor final, aspirando así a crear la blockchain de los alimentos y transformar la cadena de suministros de alimentos frescos. Armonizando esta tecnología e IoT, pretende incrementar la recopilación y la visibilidad de los datos en los procesos permitiendo nuevas analíticas, mayor automatización y diferentes modelos de negocio.

4.2.4. Reparto de "última milla"

Además de los tres campos de aplicación ya descritas, se están llevando a cabo otras iniciativas relacionadas con la aplicación de blockchain en el reparto final, conocido como "última milla".

En esta ocasión, destacamos a *Walmart*, líder en retail, que está aplicando blockchain en el desarrollo de nuevos sistemas de gestión de entregas. Sus desarrollos se orientan a la automatización de la logística en procesos de entrega de paquetes con drones y a las capacidades de blockchain para gestionar la identificación de los drones al aproximarse a los puntos de reparto.

Además, hacemos mención a los *servicios postales* de diversos países, como EE. UU, Canadá o Australia, quiénes están explorando las capacidades de blockchain para distintos usos, que van desde la prestación de servicios de verificación de identidad digital, al tracking de los envíos, pasando por servicios financieros como giros postales o envíos internacionales de dinero, en los que su uso puede incrementar la eficiencia.

4.3. Aplicación de la tecnología blockchain en el medioambiente

En la reunión sobre el cambio climático celebrada en 2017 en Bonn (Alemania), la *Convención Marco de las Naciones Unidas Sobre el Cambio Climático (UNFCCC)* resaltó el potencial que la tecnología blockchain puede ofrecer a este sector.

En este comunicado, la UNFCCC destaca tanto las ventajas que supondría su adopción, como su capacidad para aplicar soluciones que contribuyan al cumplimiento de los compromisos del *Acuerdo de París sobre el Cambio Climático*.

Basándose en esta tecnología, señala cuatro vías para lograr sus objetivos:

- *Mejorar el comercio de emisiones de carbono:* una base de datos distribuida, podría utilizarse para mejorar el sistema de transacciones de carbono. *IBM y Energy blockchain Lab*, cooperan para desarrollar una plataforma basada en blockchain con el fin de hacer más transparentes, seguras y líquidas las transacciones de activos de carbono. En su proyecto, han demostrado que éstas podrían llegar a ser un 30% más eficiente.

- *Facilitar el comercio de energía limpia: Solarcoin* es un ejemplo de cómo la tecnología p2p puede funcionar para el comercio de energía renovable mediante plataformas blockchain. En 2014 nace la SolarCoin como una criptomoneda pensada para promover la generación de electricidad mediante energía solar fotovoltaica, más limpia y eficaz que cualquier combustible fósil.

  Otro proyecto de la UNFCCC es que los consumidores puedan comprar, vender o intercambiar energía renovable entre sí, y que los tokens o los activos digitales puedan ser negociables y representen cierta cantidad de producción de energía.

- *Flujos mejorados de financiación climática:* la tecnología blockchain contribuye a que la financiación que se asigne a proyectos que apoyan la acción ecológica sea más transparente. Al mismo tiempo, estimula el desarrollo de sistemas de *crowdfunding* para micro empresas o proyectos de más envergadura.

  El artículo web *"Convención sobre el Cambio Climático reconoce el potencial de blockchain en sus objetivos"* publicado en Criptonoticias, expone como ejemplo la iniciativa de Dubái, que construyó un gran fondo de inversión para startups enfocadas en la salud, el transporte y la vialidad, energía renovable, sostenibilidad, educación, seguridad y planeamiento urbano.

- *Mejor seguimiento de los gases de efecto invernadero (GEI):* Las propiedades de blockchain, podrían facilitar el seguimiento y el informe de las reducciones de emisiones previniendo el doble conteo. Esto supondría un monitoreo efectivo en la implementación de las *Contribuciones Determinadas Nacionalmente* (NDCs) bajo el Acuerdo de París, al igual que serviría para monitorear los objetivos de cada empresa.

4.4. El Sector Sanitario

Blockchain brinda la oportunidad de optimizar los servicios de atención al paciente, fomentando una mayor transparencia y control sobre los datos.

Está tecnología permitiría a los pacientes tener un registro de su salud (visitas médicas, intervenciones, enfermedades, tratamientos…). Del mismo modo, permitiría mantener la privacidad y confidencialidad del historial médico de cada paciente a la par que agilizaría el proceso de intercambio de documentación entre los proveedores de salud y aseguradoras.

Por otro lado, también podría aplicarse a la industria farmacéutica, ya que, con la descentralización de los datos, existiría un mayor control sobre la cadena de producción de los medicamentos y, por tanto, tendríamos la garantía de tener información fiable sobre su origen y elaboración. De esta forma, se evitarían posibles falsificaciones.

4.5. El Sector Público

La administración pública, también podría sumarse a este proceso de aplicación y aprovecharse de sus ventajas. La cadena de bloques podría tener un gran impacto en la Hacienda Pública evitando el fraude y el blanqueo de capitales, por ejemplo. Por otro lado, los DNI podrían evolucionar hacia una tecnología blockchain que garantice los derechos fundamentales de los individuos, por ejemplo, en procesos electorales.

4.6. El Sector Asegurador

Este sector, sigue con atención el desarrollo de blockchain y valora las diversas áreas de aplicación. Una plataforma respaldada con esta tecnología, podría ofrecer beneficios a la industria a distintos niveles al igual que podría habilitar nuevos modos de operación. Algunos beneficios son:

- Reducción del fraude: con una red distribuida, se podría detectar reclamaciones y patrones de comportamiento relacionados con el fraude
- Valores añadidos en conjunción con IoT: activación o desactivación de seguros de viaje, vehículos, hogar…
- Automatización de creación de pólizas, reclamaciones y pagos a través de Smart contracts
- Empoderamiento de los clientes en la gestión de sus datos e historial de usuario distribuido, agilización de trámites de alta, y mejora de la evaluación de riesgos.

CAPÍTULO 5 LIMITACIONES DE LA TECNOLOGÍA BLOCKCHAIN

En el capítulo anterior observamos las múltiples ventajas que ofrece la red Blockchain y lo disruptiva que supone su aplicación en los diferentes sectores. Sin embargo, a pesar de su indudable potencial, podemos decir que esta tecnología se encuentra en una fase práctica muy inicial y presenta diversas barreras que debe afrontar para alcanzar la madurez y lograr una adopción a mayor escala.

A continuación, citaremos algunos desafíos que necesita superar esta tecnología para conseguir su objetivo:

La terminología empleada y el vocabulario que se ha introducido con su desarrollo, han hecho de Blockchain una tecnología bastante sofisticada y compleja de entender, lo cual supone un obstáculo para aquellos individuos que no están familiarizados con esta jerga técnica. Esta complejidad supone un freno para los negocios limitando el grado de implementación en los mismos.

El consumo de energía se convierte en otro desafío ya que, para mantener esta red, se necesita un consumo elevado que cada vez va en aumento. La mayor parte de la tecnología Blockchain sigue la infraestructura del Bitcoin y utiliza el PoW (proof of work) como un algoritmo de consenso que multiplica continuamente la potencia informática necesaria para computar un nuevo bloque. Según el artículo *"Blockchain – basics and beyond"* publicado en la revista digital *ABB Review*, se estima que el consumo de energía actual es del orden de la capacidad de producción de dos plantas nucleares (véase gráfico 1).

La seguridad, constituye un reto crucial para esta tecnología y así lo expresan los autores del mismo artículo: "La inmutabilidad de Blockchain es sólida, pero hay muchos posibles modos de ataque: por ejemplo, las billeteras de bitcoin están expuestas al robo, los paquetes pueden espiarse, podrían organizarse ataques de denegación de servicio distribuidos, etc. Es más, no hay modo de evitar que un atacante que controle más del 50 por ciento de la potencia informática de la Blockchain controle la propia red. Éste podría, incluso, deshacer transacciones antiguas".

La rigidez del sistema hace que modificar los protocolos subyacentes sea casi imposible. Si unos participantes actualizan sus protocolos y otros no, aparecen realidades diferentes que dan lugar a conflicto. Por tanto, la coordinación de los participantes es vital para este sistema. Esta falta de flexibilidad repercute, además, en el tiempo de respuesta dado que, cualquier cambio, necesita la verificación del conjunto de nodos, lo cual indica que no podemos esperar una solución rápida.

En la publicación *"La cadena de bloques y los cinco vectores del progreso"* por la compañía Deloitte, se señala que "como medios de procesamiento de transacciones, los sistemas basados en la cadena de bloques son comparativamente lentos". "En contraste con algunos sistemas heredados de procesamiento de transacciones capaces de procesar decenas de miles de transacciones por segundo, la cadena de bloques de bitcoin puede manejar solo entre tres y siete transacciones por segundo" *(véase gráfico 3)*. Esto supone una preocupación para las empresas cuyos sistemas requieren de un elevado rendimiento y cortos tiempos de respuesta, por lo que muchos consideran que la tecnología Blockchain no es viable para aplicaciones a gran escala.

Los problemas regulatorios son otra barrera importante que dificultan la adopción de la cadena de bloques según el mismo informe. Este tipo de tecnología, emplea diferentes conceptos y métodos como firmas criptográficas o contratos inteligentes cuya regulación no se encuentra recogida en ninguna normativa actual, y en ocasiones, su aplicación va en contra de las prácticas que ésta estipula.

Otro desafío al que se enfrenta, es la ***falta de estándares e interoperabilidad*** entre varias plataformas. La tecnología será de poca utilidad en un escenario mayor si no puede ser fácilmente conectada con los sistemas existentes de las empresas. En un artículo web publicado en Criptonoticias, el vicepresidente de la compañía estadounidense de servicios financieros, *Depository Trust & Clearing Corporation* (DTCC), Larry Thompson, destaca la necesidad de una estandarización para no complicar aún más las estructuras y favorecer la adopción global de Blockchain. El discurso que presentó en el taller llamado *"Sharing the Challenge"* (Compartiendo el Desafío) señala la importancia del trabajo en equipo por parte de los grandes reguladores en medidas que permitan la estandarización de esta red en el área de las finanzas.

"Sin coordinación para establecer un conjunto en común de estándares aplicables a la tecnología de contabilidad distribuida que sea usado a nivel mundial, corremos el riesgo de repetir lo pasado y crear a conciencia un nuevo sistema que no interactúe entre sí. Necesitamos aumentar la conciencia de la necesidad de estándares tecnológicos armonizados y mejorar las practicas a los efectos de la integración y la interoperabilidad." (Larry Thompson)

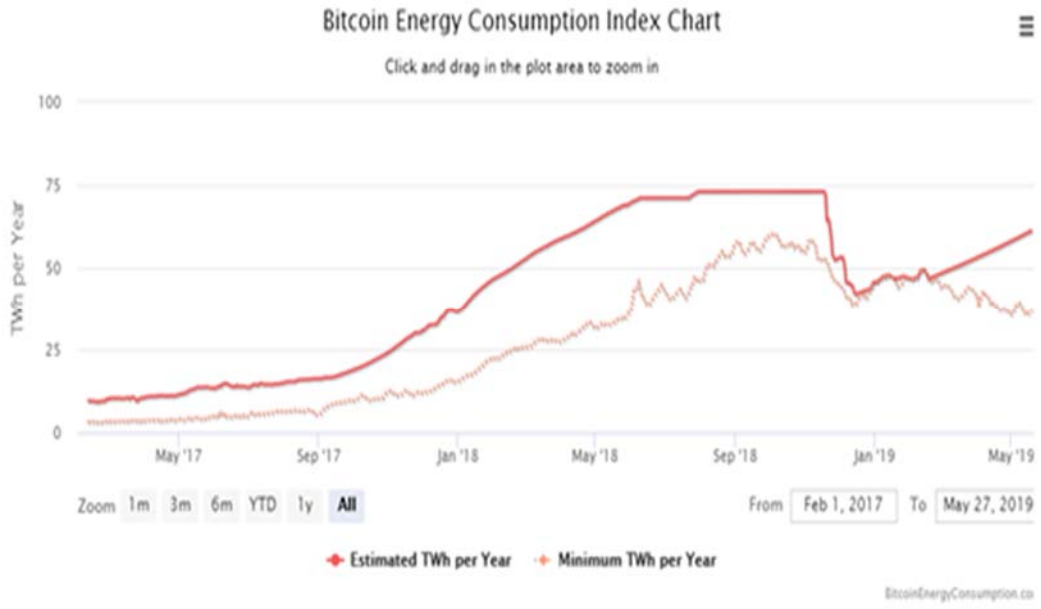
Por su parte, las criptomonedas también se enfrentan a una serie de limitaciones que impiden su plena aceptación, algo que, a su vez, frena la implementación de la cadena de bloques y el futuro de su tecnología.

Desde un punto de *vista ecológico*, y según señala un estudio elaborado por Max J. Krause y Thabet Tolaymat, publicado en la revista *Nature Sustainability*, el desarrollo de las criptomonedas podría suponer un ***riesgo para el medioambiente***.

En su análisis se pudo afirmar que, entre el primer semestre de 2018 (véase gráfico 1), el minado de criptodivisas demandó más energía que la necesaria para la extracción física de metales como el cobre, el oro o el platino. Asimismo, apuntan que la potencia de computación que se necesita equivale a la cantidad de electricidad anual consumida en países como Hong Kong o Irlanda.

Los autores analizaron, al mismo tiempo, las posibles repercusiones sobre el calentamiento global y, las investigaciones mostraron como las criptodivisas *Bitcoin, Etherum, Litecoin y Monero* generaron entre 3 y 15 millones de toneladas de emisiones de carbono, lo que evidencia una posible contribución al incremento del calentamiento global.

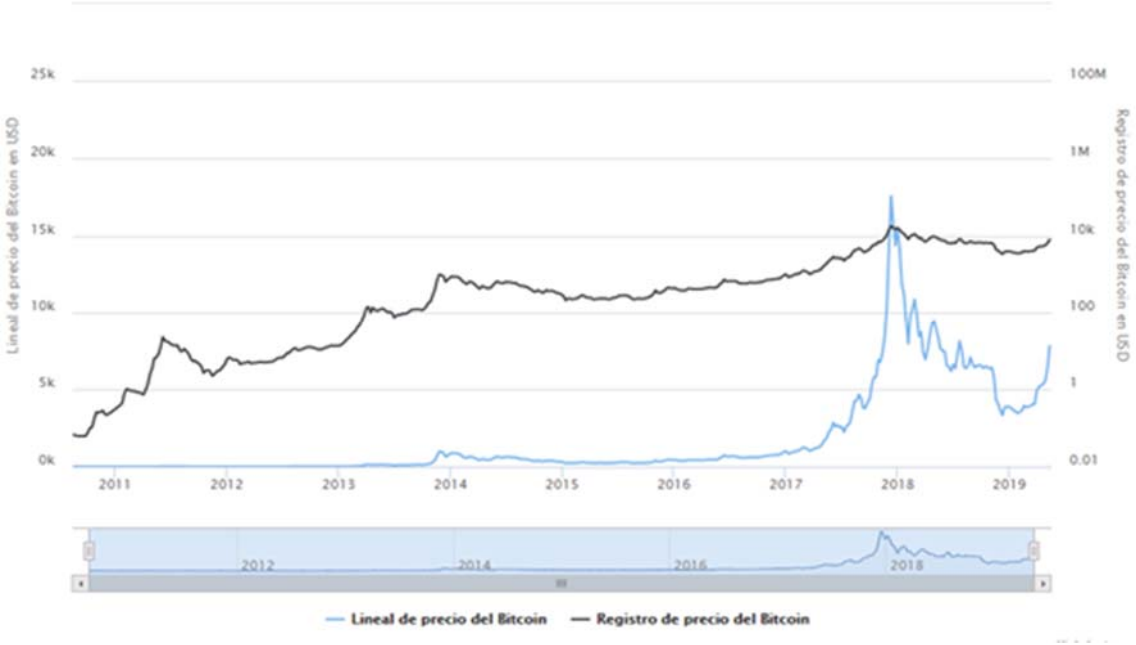
Gráfico 1: Diagrama de consumo de energía de Bitcoin



Fuente: www.digiconomist.net

La alta volatilidad y la escasa regulación, han hecho que las criptomonedas sufran un retroceso respecto al 2017, donde, por ejemplo, el Bitcoin, alcanzó su valor máximo (véase gráfico 2). Esta regresión desencadena un clima de incertidumbre que influye en la aceptación y adopción tanto de las criptomonedas como de la tecnología que las respalda, por lo que conviene prestar atención a este aspecto.

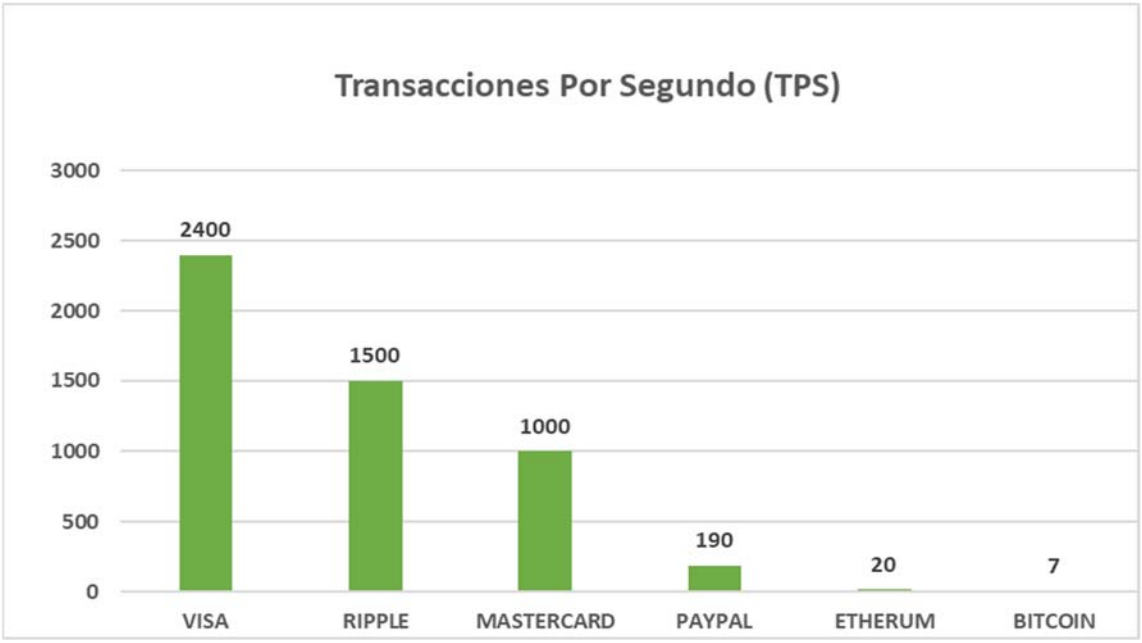
Gráfico 2: Historial del precio de Bitcoin.



Fuente: www.buybitcoinworldwide.com

El volumen de transferencia, es otro de los retos que nos plantean las criptomonedas. Las transacciones de criptodivisas son muy lentas, en el caso del Bitcoin para que cada bloque de transacción se haga efectivo debe pasar unos 10 minutos, y existe, además, una gran lista de espera (*mempool*) debido a que todas las transacciones que ocurren en ese plazo de tiempo no caben en un mismo bloque. Este hecho siembra la duda sobre la viabilidad de su aplicación para iniciativas que impliquen grandes volúmenes de transferencias, tal y como apuntamos en los desafíos de la Blockchain (véase gráfico 3).

Gráfico 3: Número de transacciones por segundo en diferentes plataformas de pago



Fuente: Elaboración propia partiendo del artículo de Elías Rodríguez García (2018).

Como se puede apreciar en el gráfico 3, las cifras de las operaciones con Bitcoin son muy escasas por lo que podemos asegurar que no es el mejor medio de pago y que los individuos no terminan de aceptar.

La inmadurez de las criptomonedas se encuentra presente en diferentes campos que afectan de forma directa a la evolución de la tecnología Blockchain:

En el ámbito legal, como bien mencionábamos en el epígrafe anterior, actualmente no contamos con una legislación sólida que regule los aspectos que introduce esta tecnología, como por ejemplo las criptomonedas. Este vacío legal permite que agentes malintencionados actúen y dejen sin garantías a los usuarios.

En el plano económico, la inestabilidad, ya comentada, tiene su origen en la inmadurez de la moneda electrónica.

Y, por último, dentro del *ámbito tecnológico*, la tecnología Blockchain necesita proyectos reales y tangibles que funcionen y sean rentables para que las grandes empresas se fijen y sigan apostando por ella. Si no se consigue tener proyectos con nombres y apellidos basados en el Blockchain pronto se considerará como una tecnología de nicho, una utopía no rentable y hará que el interés por la misma disminuya.

Finalmente, destacamos el *exceso de oferta* como otra barrera a superar. Cada día nacen más ICOs, surgen nuevos forks y nuevas propuestas de criptomonedas que hacen que la diversidad y la oferta crezca sin control. Cualquier usuario que participe en esta red puede lanzar al mercado nuevas criptomonedas modificando y mejorando las existentes o creándolas desde cero, lo que acarrea como resultado:

- La mayoría de monedas que se crean no aportan nada nuevo tecnológicamente, ya que en lugar de hacer una propuesta de mejora y evolución de la ascendiente, realizan pequeñas matizaciones.
- Hace que aparezcan las monedas de nichos, esto es, los usuarios cogen únicamente el código fuente de una criptomoneda popular y la adapta a sectores concretos (sanidad, educación, tecnología…)

En la actualidad, no existen suficientes recursos monetarios para respaldar a todas estas criptomonedas. Por lo que debemos prestar atención, apostando por novedades coherentes y estudiando bien dónde y cómo invertir el dinero.

CONCLUSIÓN

No cabe duda que el impacto que esta tecnología causará en nuestras vidas va ser tan significativo como el impacto que tuvo en su momento la aparición de Internet.

Esta red posee un gran potencial y podemos afirmar que, definitivamente, está aquí para quedarse. En este documento, hemos observado algunas de sus aplicaciones más características y el valor que podrían brindar a las empresas, lo que nos lleva a pensar que la cadena de bloques supondrá un cambio radical tanto a nivel económico como a nivel social.

Sin embargo, a día de hoy existen varios retos como la regulación y la seguridad que conviene superar, ya que son dos de las debilidades que más incertidumbre y desconfianza generan a las empresas y, por tanto, frenan su aceptación.

Podemos concluir señalando que, aún queda un largo camino para alcanzar una adopción generalizada por los distintos sectores económicos, pero es probable que en los próximos años veamos los frutos de su desarrollo que motivarán el paso a una *Cuarta Revolución Industrial: la Industria 4.0.*

GLOSARIO

Árbol de Merkle: Dentro de cada bloque de la red Bitcoin nos encontramos con una estructura llamada "Árbol de Merkle", esta estructura busca relacionar una serie de datos separados con un único hash para reducir el tiempo y los recursos empleados en verificar la integridad de una cantidad de información.

Ataque del 51%: Se produce cuando una persona o un grupo de individuos posee el 51% del poder de cómputo de la red. Es decir, este grupo o individuo dispone de más capacidad de cálculo que el resto de participantes de la red, algo que puede afectar de manera negativa al sistema electrónico distribuido, alterando el funcionamiento de la red de forma temporal.

Crowfunding: Mecanismo de financiación en el que un promotor solicita financiación para un proyecto públicamente en internet y en la que los individuos que lo deseen pueden realizar aportaciones económicas a través de una plataforma crowdfunding especializada.

Fluctuación: Las fluctuaciones de divisas son simplemente los cambios en curso entre el valor relativo de la moneda emitida por un país en comparación con una moneda diferente.

Hacker: Un *hacker* es alguien que descubre las debilidades de un ordenador o un sistema de comunicación e información, aunque el término puede aplicarse también a alguien con un conocimiento avanzado de computadoras y de redes informáticas. Los hackers pueden estar motivados por una multitud de razones, incluyendo fines de lucro, protesta o por el desafío.

Hash – cash: Tecnología cuya finalidad era reducir el correo no deseado y los ataques de denegación del servicio; es la contrapartida al spam.

ICO: "Initial coin offering"/ Oferta inicial de moneda. Busca la financiación de una iniciativa mediante la emisión de una criptomoneda.

IOT (Internet of Things): El internet de las cosas es la interconexión entre dispositivos y objetos a través de una red, donde todos ellos pueden ser visibles e interaccionar.

Marketplaces: o supermercados digitales. Es un sitio web que permite tanto a vendedores como a compradores relacionarse entre sí para efectuar una transacción comercial.

Mempool: Se trata de una colección de transacciones de Bitcoin que han sido verificadas por los nodos de Bitcoin pero que aún no se han añadido a la cadena de bloques de Bitcoin. Estas transacciones son posteriormente comparadas por los mineros de Bitcoin y añadidas a la cadena de bloques de Bitcoin. Los nodos Bitcoin se comunican entre sí hasta que la transacción es conocida por toda la red de la cadena de bloques. Una vez verificada la transacción, se incluye en el mempool.

Open source: o código abierto. Terminología empleada para denominar cierto tipo de software que se distribuye mediante una licencia que permite al usuario final utilizar un código fuente del programa para estudiarlo, modificarlo y realizar mejoras en el mismo, permitiéndoles hasta redistribuirlos. Este tipo de software provee de características y ventajas únicas, ya que los programadores, al tener acceso al código fuente de una determinada aplicación pueden leerlo y modificarlo, y por lo tanto pueden mejorarlo, añadiéndole opciones y corrigiendo todos los potenciales problemas que pudiera encontrar, con lo que el programa una vez compilado estará mucho mejor diseñado que cuando salió de la computadora de su programador original.

Protocolo de consenso: Este permite que todas las partes de la red puedan llegar a un acuerdo común sin conocer todas las variables que lleven al mismo.

Red centralizada: En esta red todos los nodos son periféricos, salvo el central. Estos nodos se comunican entre ellos a través del nodo central y sus canales. Si el nodo central sufre una caída, el resto de los nodos dejan de tener flujo. Esta red se rige por el principio de conocimiento.

Red descentralizada: En esta red no existe un único nodo central, hay un centro colectivo de diversos puertos de conexión. Cuando uno de los nodos reguladores cae, se produce una desconexión de uno o varios nodos del conjunto de la red. Sin embargo, si cae el nodo centralizador se produce de manera obligatoria la ruptura de la red. Este tipo de red se rige por el principio de adhesión o participación.

Red distribuida: Esta red se caracteriza por la ausencia de un centro individual o colectivo. Los nodos se unen de uno a otro de tal forma que ninguno de ellos tiene poder de filtro sobre la información que se transmite en la red, en consecuencia, desaparece la idea de centro y periferia, características básicas en las redes centralizada y descentralizada. Si cae un nodo, no se desconectaría ningún otro, por lo que se convierte en una red práctica, robusta y eficiente. Esta red se rige por el principio de la interacción.

R3 CEV: Es una empresa de tecnología de blockchain empresarial. Lidera un ecosistema de más de 300 empresas que trabajan juntas para crear aplicaciones distribuidas sobre Corda (plataforma de blockchain de vanguardia que elimina la fricción costosa en las transacciones comerciales al permitir que las empresas realicen transacciones directamente) para su uso en industrias tales como servicios financieros, seguros, salud, finanzas comerciales y activos digitales.

Script de transacciones: Lenguaje de programación que se utiliza en Bitcoin para el procesamiento de transacciones.

Start up: o empresa emergente. Es una empresa de nueva creación que comercializa productos y/o servicios a través del uso intensivo de las tecnologías de la información y comunicación (TIC's). Siguen un modelo escalable, el cual permite un crecimiento rápido y sostenido en el tiempo.

Trading: Es un tipo de operación bursátil de carácter especulativo. Sus operaciones se basan en comprar un activo para, posteriormente, venderlo a un precio superior o para venderlo y comprarlo nuevamente a un precio inferior. Normalmente, los activos que se compran son acciones que se cotizan en mercados muy líquidos.

Transacciones pool: Colección de transacciones de Bitcoin que han sido verificadas por los nodos, pero aún no han sido introducidos en la cadena de bloques del Bitcoin.

Wallet: Monedero digital.

BIBLIOGRAFÍA

Capítulo 1

- https://www.binance.vision/es/blockchain/history-of-blockchain
- https://www.ingenioindustrial40.com/2018/04/13/la-primera-revolucion-industrial-la-industria-4-0/
- https://www.elblogdeendesa.com/innovacion-tecnologica/primera-revolucion-industrial/
- https://www.elblogdeendesa.com/innovacion-tecnologica/industria-2-0/
- https://www.elblogdeendesa.com/innovacion-tecnologica/industria-3-0/

Capítulo 2

- https://www.queesbitcoin.info/
- https://bitcoin.org/es/
- https://www.ig.com/es/invertir-en-criptomonedas/que-son-las-criptomonedas
- https://www.bbva.com/es/smart-contracts-los-contratos-basados-blockchain-no-necesitan-abogados/
- https://miethereum.com/smart-contracts/#toc2
- https://www.binance.vision/es/blockchain/history-of-blockchain
- https://www.ingenioindustrial40.com/2018/04/13/la-primera-revolucion-industrial-la-industria-4-0/
- https://www.elblogdeendesa.com/innovacion-tecnologica/primera-revolucion-industrial/
- https://www.elblogdeendesa.com/innovacion-tecnologica/industria-2-0/
- https://www.elblogdeendesa.com/innovacion-tecnologica/industria-3-0/
- https://academy.bit2me.com/que-es-arbol-de-merkle/
- https://academy.bit2me.com/que-es-hashcash/
- https://academy.bit2me.com/que-son-los-smart-contracts/
- ROJO, MARIA ISABEL. (2018). BLOCKCHAIN FUNDAMENTOS DE LA CADENA DE BLOQUES. MADRID, ESPAÑA: RA-MA EDITORIAL.

Capítulo 3

- ALLENDE LÓPEZ, MARCOS; COLINA UNDA, VANESSA (2018) BLOCKCHAIN: COMO DESARROLLAR CONFIANZA EN ENTORNOS COMPLEJOS PARA GENERAR VALOR DE IMPACTO SOCIAL, https://publications.iadb.org/es/publicacion/17379/blockchain-como-desarrollar-confianza-en-entornos-complejos-para-generar-valor-de
- https://www.bbvaresearch.com/wp-content/uploads/2015/08/Situacion_Economia_digital_jul-ago15-Cap4.pdf
- https://miethereum.com/wp-content/uploads/2017/11/Tecnologia_blockchain-bbva.pdf
- https://miethereum.com/wp-content/uploads/2017/11/Blockchain-mirando-mas-alla-de-Bitcoin.pdf
- https://miethereum.com/wp-content/uploads/2017/11/Blockchain-Economia-de-Confianza-Deloitte.pdf
- https://www.bcn.cl/obtienearchivo?id=repositorio/10221/25308/3/Bolckchain_conceptos_impacto_en_industrias_y_marcos_regulatorios%20Final%20SUP.pdf

Capítulo 4

- https://www.innovaspain.com/blockchain-tecnologia-banco-santander-2019/
- https://bitcoin.es/actualidad/blockchain-para-los-bancos-usos-beneficios-e-inconvenientes/
- https://www.bbva.com/es/bbva-aboga-por-la-regulacion-de-la-tecnologia-dlt-incluido-el-blockchain/
- https://www.bbva.com/es/r3-apuesta-bancos-tecnologia-blockchain/
- https://www.eleconomista.es/empresas-finanzas/noticias/8962817/02/18/La-banca-se-suma-al-blockchain.html
- https://www.minsait.com/sites/default/files/newsroom_documents/informe_blockchain_logistica_uno_e_0.pdf
- http://www.blockchainservices.es/asociaciones-y-consorcios/tradelens-la-blockchain-de-maersk-e-ibm-y-sus-dilemas/
- http://www.cadenadesuministro.es/noticias/tradelens-la-solucion-de-blockchain-de-maersk-para-mejorar-la-transparencia-en-la-cadena-de-suministro/
- https://www-03.ibm.com/press/mx/es/pressrelease/54224.wss
- https://www.ecopost.info/potencial-la-tecnologia-blockchain-la-accion-climatica/
- https://www.criptonoticias.com/aplicaciones/convencion-cambio-climatico-reconoce-potencial-blockchain-objetivos/#axzz4qJc4srJ6
- https://www.criptonoticias.com/aplicaciones/futuro-blockchain-salud-grandes-empresas/
- https://www.cogesasl.com/2017/11/15/blockchain-sanidad/
- https://retina.elpais.com/retina/2018/07/30/tendencias/1532937675_015274.html
- PREUKSCHAT, ALEXANDER (2017) BLOCKCHAIN: LA REVOLUCIÓN INDUSTRIAL DE INTERNET-EBOOK. EDITORIAL GESTION 2000.

Capítulo 5

- https://coinrevolution.com/es/¿Cuáles-son-los-problemas-y-limitaciones-de-blockchains%3F
- https://www2.deloitte.com/content/dam/Deloitte/co/Documents/technology/Cadena%20bloques%20vectores%20progreso.pdf
- https://www.criptonoticias.com/gobierno/regulacion/vicepresidente-dtcc-considera-estandarizacion-global-blockchain/
- https://www.infobae.com/cripto247/mercados/2018/11/02/los-cinco-desafios-para-lograr-la-adopcion-de-blockchain/
- https://www.businessinsider.es/criptomonedas-2019-bitcoin-ethereum-ripple-litecoin-347423?page=1
- https://digiconomist.net/bitcoin-energy-consumption
- https://www.businessinsider.es/bitcoin-ya-consume-mas-energia-que-muchos-paises-252146
- https://www.businessinsider.es/minado-criptomonedas-consumo-energia-325471
- www.buybitcoinworldwide.com
- RODRÍGUEZ GARCÍA, ELÍAS. EL BITCOIN CONTRA OTROS MÉTODOS DE PAGO ¿ES UNA ALTERNATIVA REAL? (2018) EL ESPAÑOL OMICRONO https://omicrono.elespanol.com/2018/02/bitcoin-cifras-comparacion/
- ROJO, MARIA ISABEL. (2018). BLOCKCHAIN FUNDAMENTOS DE LA CADENA DE BLOQUES. MADRID, ESPAÑA: RA-MA EDITORIAL.