GRADO EN ADMINISTRACIÓN Y DIRECCIÓN DE EMPRESAS

CURSO ACADÉMICO 2017/2018

TRABAJO FIN DE GRADO

Tecnología de Registro Distribuido evolución, aplicación y retos

Distributed Ledger Technology development, application and challenges

AUTORA
Jael Burgada Ruiz

DIRECTOR
Daniel Pérez González

FECHA
Septiembre 2018

RESUMEN

La tecnología de registro distribuido (DLT) cobra cada vez mayor importancia en el mundo de los negocios, ya que permite realizar transacciones de valor a través de internet entre desconocidos sin la intermediación de una entidad central que las controle. Crea consenso en un grupo de personas entre las que no hay confianza mutua.

Se trata de una innovación disruptiva que pone en cuestión el paradigma económico actual. Es importante, por lo tanto, informarse bien sobre sus posibles aplicaciones y los retos a los que se enfrenta. Para esto, es necesario tener una perspectiva más global, alejada de plataformas concretas que, si bien es cierto que son las más populares en la actualidad, quizás no perduren en el tiempo.

En este trabajo se hace una revisión cualitativa y bibliográfica de fuentes diversas, tanto formales como informales, sobre la DLT, con el fin de organizar parte de la gran cantidad de información sobre la tecnología, que a menudo es caótica, dispersa o incluso errónea.

En primer lugar, se explora el origen y la evolución de las plataformas DLT – criptomonedas, registro de transacciones, contratos inteligentes y mercados. Tras esto, se describen las características de los dos tipos de plataformas más relevantes – blockchain y hashgraph. Se crea un modelo para la aplicación más completa de plataformas DLT – una jerarquía de consenso, herramientas y aplicaciones –, tras lo cual se recopilan ejemplos de aplicaciones reales.

A pesar de ser tan prometedora, se mantiene una visión crítica ante esta innovación, exponiendo una serie de retos a los que la tecnología se enfrenta – desde el funcionamiento de la nueva criptoeconomía, el funcionamiento de las mismas plataformas, pasando por la seguridad, la gobernanza y la estabilidad, hasta la conformidad con la legislación – y sobre los que se tendrá que trabajar de cara al futuro.

ABSTRACT

Distributed Ledger Technology (DLT) becomes increasingly important in the business world, as it allows for transactions of value through the internet between strangers without the intermediation of a central entity that controls them. It creates consensus in a group of people who do not have mutual trust.

It is a disruptive innovation that questions the current economic paradigm. Therefore, it is important to get well informed about its possible applications and the challenges it faces. For this, it is necessary to acquire a more global perspective, away from specific platforms which, even though they are currently the most popular, might not remain after some time.

This paper does a qualitative bibliographical review of diverse sources, both formal and informal, about DLT, to organize part of the vast amount of information that is out there about the technology, which is many times chaotic, scattered or even wrong.

Firstly, the origin and evolution of DLT platforms are explored – cryptocurrencies, transaction records, smart contracts and markets. After this, the characteristics of the two most relevant platforms are described – blockchain and hashgraph. A model for the most complete application of DLT platforms is created – a hierarchy of consensus, tools and applications –, after which examples of real applications are compiled.

Although very promising, a critic eye on this innovation is maintained, exposing a series of challenges that the technology faces – from the dynamics of the new cryptoeconomy, the inner workings of the platforms themselves, security, governance and stability, to legal compliance – and on which work will have to be done in the future.

1. INTRODUCCIÓN

Bitcoin, criptomonedas o blockchain, son palabras que aparecen con creciente frecuencia en medios de comunicación pero que pocos comprenden. ¿Qué es exactamente? ¿Cuál es la diferencia entre blockchain y Bitcoin? ¿Para qué sirve una criptomoneda? ¿Acaso es esto importante, o es una moda pasajera? Es difícil para una persona sin conocimientos previos encontrar una fuente de información sobre la que crear una opinión crítica, que organice y clasifique todos estos conceptos de forma comprensible y global. Para tener una base clara sobre la que entender de qué se habla en este trabajo, hemos integrado los conceptos comunes de diferentes definiciones (Tapscott, 2015; Christidis, Devetsikiotis, 2016; Preukschat et al., 2017; Baird, Harmon y Madsen, 2018) en una sencilla y más general, que englobe a todas las plataformas que se encuentran bajo el mismo paraguas.

La tecnología de registro distribuido o *Distributed Ledger Technology* (DLT) permite realizar transacciones de valor desde cualquier lugar del mundo a través de internet entre desconocidos sin la intermediación de una entidad central que las controle.

Esta tecnología se encuentra en la etapa de introducción de su ciclo de vida y aún es muy desconocida para el público general. Las palabras de expertos como Don Tapscott, cofundador del *Blockchain Research Institute*, en el Foro Económico Mundial en Davos (2018) destacan el potencial de esta tecnología para causar un gran impacto favorable en la sociedad. Cada vez es mayor el interés por parte de grandes organizaciones como gobiernos, bancos y otras grandes corporaciones, manifestado por importantes inversiones en el desarrollo de esta tecnología. La capitalización de mercado – "el valor total del suministro de monedas circulantes multiplicadas por el último precio bajo el cual se han negociado" (Herrera, 2018) – de acuerdo con las webs *TradingView* y *BitcoinMagazine*, de las criptomonedas más importantes a fecha 16 de septiembre de 2018 son: Bitcoin más de 112 billones de dólares americanos, Ethereum más de 22 billones y Ripple 11 billones.

Todos estos indicios dejan ver que se trata de una innovación trascendental que se irá implantando cada vez más y a mayor velocidad. En las palabras de Tapscott, *"Such is the potential of blockchain. No facet of human activity will be left untouched" – Tal es el potencial de blockchain. Ningún aspecto de la actividad humana quedará intacto*. Aunque menciona "blockchain", se refiere a cualquier tipo de plataforma DLT. La relevancia de comprender todos estos conceptos es evidente. Para sobrevivir en un mundo en constante movimiento habrá que ser capaces de aplicar estas nociones, pues quien no evolucione con la tecnología que se va implantando en la sociedad se quedará atrás (TEDx Talks, 2016).

El objetivo de este trabajo es el análisis de la tecnología de registro distribuido (DLT), con el fin de aunar y organizar parte de la inmensa cantidad de información que existe sobre esta, que en la mayoría de los casos es caótica, dispersa y muy específica de plataformas concretas. Es importante tener una perspectiva más global, alejada de estas plataformas que, si bien es cierto que son las más populares en la actualidad, quizás no perduren en el tiempo. Es necesario conocer el el origen y la evolución de la tecnología para llegar a entender su funcionamiento y sus posibles aplicaciones en los negocios. Además, aunque la tecnología tiene un inmenso potencial, ni es perfecta, ni es una fórmula mágica para resolver todos los problemas de la sociedad (Grimes, 2018), por lo tanto, es necesario tener una visión crítica de ella y conocer los retos que se presentan, sobre los cuales se tendrá que trabajar de cara al futuro.

2. ANÁLISIS DEL ESTADO DEL ARTE

Son muchas las dudas que se presentan a partir de la definición propuesta en la introducción:

> "La tecnología de registro distribuido o *Distributed Ledger Technology* (DLT) permite realizar transacciones de valor desde cualquier lugar del mundo a través de internet entre desconocidos sin la intermediación de una entidad central que las controle".

¿Cómo es esto posible? Gracias a una red de ordenadores que operan el mismo software, una plataforma DLT, que anota todas las transacciones y eventos ocurridos en él en el orden exacto en que ocurren. Todos estos ordenadores tienen una réplica exacta de este registro o *ledger*, que es constantemente actualizada. Tan pronto como se produzca un cambio en una de las copias de este software, todas las otras copias serán actualizadas para coincidir, siempre y cuando se compruebe mediante un mecanismo de consenso que este cambio es legítimo.

¿Por qué surge la DLT? ¿No era ya posible hacer transacciones a través de Internet? Efectivamente, era posible hacer transacciones a través de internet, pero siempre mediante un intermediario que verifique las transacciones, como puede ser un banco o un sistema de pagos online como PayPal. Al eliminar a este intermediario surgiría el problema del doble gasto o *double spending problem*, un defecto que permite que una misma moneda digital se gaste más de una vez. Al igual que cualquier archivo informático, una persona podría duplicar los archivos de monedas y quedarse con una copia. Esto provocaría la pérdida de valor de la moneda y la invalidez de las transacciones realizadas con ella. Es vital para el correcto funcionamiento del dinero el estar seguro de que quien dice mandar una cantidad determinada de dinero lo haga de verdad y no lo pueda volver a gastar más tarde.

¿Cómo se puede confiar en que no va a haber doble gasto si no existe un intermediario que se asegure? Esto se llama el problema de los generales bizantinos, un problema muy antiguo que había sido irresoluble hasta la aparición de estos sistemas distribuidos. El problema es el siguiente: Cómo asegurar con completa certeza que varios actores separados por una distancia están en completo acuerdo antes de iniciar una acción. Es decir, cómo puede cada individuo asegurarse de que hay un consenso total, en este caso a través de internet, donde los participantes son desconocidos que no confían entre ellos. En el caso de la DLT, no es que la figura de un tercero que lo verifique se elimine, sino que se descentraliza. Este tercero sería la red P2P que valida y certifica todas las transacciones y asegura la confianza mediante un mecanismo de consenso.

¿Y cómo se ponen todos ellos de acuerdo? Un sistema de votos sería la primera opción para llegar al consenso, pero surgen problemas en todos los puntos del proceso. ¿Cómo asegurar que todos los participantes han recibido el mensaje que contiene la acción sobre la que se vota? Este podría haber sido manipulado antes de llegar a los participantes, así como podrían haberlo sido los mensajes devueltos con los votos, que podrían no expresan la verdadera intención de quien ha votado. Habría que compartir un nuevo mensaje con los votos recibidos del resto de participantes, pero también estos podrían estar manipulados. Para ser efectivo, este sistema necesitaría el intercambio de una gran cantidad de mensajes para compartir y comparar la información sobre los votos para alcanzar consenso sobre una simple acción, lo cual es completamente ineficiente. Más adelante, en el desarrollo de la investigación, se hará una descripción de algunos de los diferentes mecanismos de consenso empleados para resolver este problema por las diferentes plataformas DLT.

3. METODOLOGÍA

Para este análisis se ha hecho una revisión cualitativa y bibliográfica de diversas fuentes sobre la tecnología de registro distribuido (DLT) desde sus orígenes hasta el momento actual, materiales que van desde el año 2015 hasta el presente, septiembre de 2018. Esta información se encuentra en diferentes medios, tanto escritos como audiovisuales. Las fuentes han sido tanto académicas, como webs, blogs, podcasts o canales de YouTube especializados en el tema de la DLT.

Una vez revisados todos los materiales, lo que ha permitido la comprensión de los conceptos, se ha realizado una selección, prescindiendo de aquellos contenidos de menor relevancia para el análisis objeto de este trabajo y además se han descartado aquellos que llevan a una confusión de los términos técnicos. Parte de la información que se encuentra en medios informales es de baja calidad y rigurosidad, en ocasiones se utilizan los términos de manera indistinta y en muchos casos errónea. Aun así, los medios informales son muy relevantes, ya que son una de las fuentes de información más actualizadas debido a que muchas plataformas cambian por decisiones de la comunidad.

Para realizar un análisis global, se ha tenido en cuenta la información en su conjunto, ya que las fuentes son independientes y cada autor habla sobre conceptos particulares o defiende un tipo de plataforma concreta de forma subjetiva. Algunos materiales hacen un estudio global de DLT y otros se centran más en aspectos concretos. Toda esta información es complementaria y su integración posibilita una comprensión mejor y más general de esta nueva tecnología.

4. DESARROLLO DE LA INVESTIGACIÓN

Se dice que estamos viviendo el comienzo de la cuarta revolución industrial. El nacimiento del internet del valor, como se llama a la DLT, se asimila al del internet de la información, reconocido como una de las piezas clave de la tercera revolución industrial. Hasta día de hoy, Internet ha dado lugar a profundos cambios económicos y socioculturales, transformando la conducta de las personas. Ha permitido la mejora de las comunicaciones, la expansión del conocimiento y ha propiciado enormes mejoras en la eficiencia del trabajo. En la actualidad, la vida sin internet es casi inconcebible a todos los niveles, a pesar de que en sus primeras décadas de existencia era una herramienta explorada y utilizada únicamente por expertos e individuos con una fascinación especial por la tecnología. A primera vista, no era evidente que fuera a convertirse en una herramienta que cambiaría la vida cotidiana de las personas. Se basaba en una tecnología poco accesible y difícil de utilizar, ya que requería de un profundo conocimiento técnico. Con su evolución se fue volviendo más accesible, se desarrollaron protocolos estandarizados y surgieron nuevas aplicaciones con interfaces más sencillas.

Debido al desarrollo de otra generación de nuevas tecnologías cuya implementación tendrá un impacto de gran escala tanto a nivel económico como sociocultural, se dice que comienza la cuarta revolución industrial (Tapscott, 2016). Como expone Klaus Schwab, economista y empresario fundador del Foro Económico Mundial, en el libro *The fourth industrial revolution* (2017), la integración de la tecnología de registro distribuido (DLT) junto con otros avances como el internet de las cosas (IoT), la inteligencia artificial (AI), el Big Data o la impresión 3D dará pie a complejas interacciones entre diversos ámbitos de conocimiento e infinidad de nuevas aplicaciones, tanto digitales como físicas. En un mundo digitalizado, la tendencia general es la búsqueda de la eficiencia a través de un uso más consciente y cuidadoso de los recursos y la propiedad, posible gracias a la colaboración y la integración del conocimiento y las tecnologías. Al igual que en los comienzos de Internet, actualmente sólo un pequeño porcentaje de la población mundial trabaja directamente sobre estas tecnologías, pero cada vez es mayor el interés general. Constantemente surgen nuevos proyectos, se resuelven problemas técnicos o se crean nuevas aplicaciones.

4.1. EVOLUCIÓN Y MADURACIÓN DE LA DLT

Cada etapa de la evolución de las plataformas DLT parte de la anterior, creando diferentes niveles, los cuales siguen madurando y construyendo una tecnología cada vez más compleja. Se tiene bastante conocimiento de los avances que se llevan a cabo en las plataformas públicas, pero desconocemos todos los productos que las grandes entidades privadas están desarrollando para sacar el máximo provecho a esta nueva tecnología.

Como el creador de hashgraph, Leemon Baird, explica en vídeos de Hedera Hashgraph (2018) – hay cuatro niveles de uso de la DLT (Figura 1), que fueron surgiendo en un orden lógico.

1. Criptomonedas – Dinero digital sin un organismo oficial que lo cree. Surgen las DLT como medida para combatir el doble gasto.

El origen de la tecnología blockchain se debe al nacimiento de Bitcoin en 2009. Hasta ese momento, no era posible hacer transacciones monetarias sin intermediarios por internet debido al problema del doble gasto, expuesto en la introducción. Un individuo o grupo de personas, bajo el pseudónimo de Satoshi Nakamoto, idearon un sistema mediante el cual poder realizar transacciones monetarias a través de internet de manera segura, sin intermediarios y sin necesidad de conocer y confiar en la otra persona. La confianza en la tecnología hace innecesaria la confianza en individuales o una institución central que controle las transacciones.

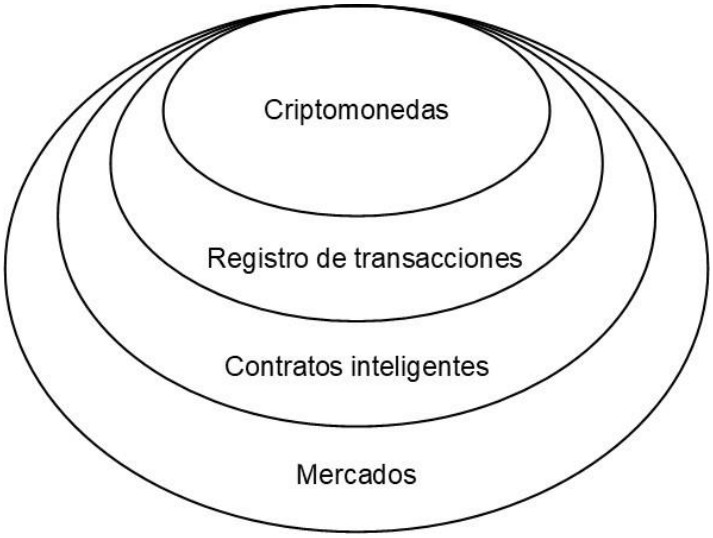

Figura 1 – Evolución de la tecnología de registro distribuido Fuente: elaboración propia, adaptación de How Hashgraph Works - Leemon Baird @ Thomson Reuters (2/21/2018) (Leemon Baird, 2018)

2. Registro de transacciones – Además de dinero, se puede hacer el seguimiento de cualquier activo de valor, como propiedad o identidad.

Tras un tiempo se deduce que, además de intercambiar monedas, es posible almacenar e intercambiar cualquier tipo de activo de valor digitalizado. Por ejemplo, se pueden almacenar identidades, certificados, la propiedad de un inmueble o acciones y bonos. Con todos estos activos, es posible hacer transacciones que queden plasmadas en este registro distribuido.

3. Contratos inteligentes – Intercambios más complejos y automatizados de diferentes activos de valor.

Con todos estos activos digitalizados, se genera la posibilidad de intercambiar valor de manera automática a través de contratos inteligentes. Esto ocurre por primera vez en la plataforma blockchain Ehtereum, en el año 2015. Estos contratos son programas informáticos que permiten la automatización de ciertas transacciones dadas unas condiciones determinadas en él (Bharadwaj, 2016), como pueden ser compraventas, acuerdos, votos o aplicaciones distribuidas, también conocidas como DAPPs. Los contratos pueden llegar a tener toda la complejidad que un programador sea capaz de incluir en su código.

4. Mercados – Intercambios entre grupos de vendedores y compradores de activos.

En este entorno es muy atractivo crear mercados en los que intercambiar valor entre múltiples participantes, equivalentes a lo que puede ser un mercado de valores, que case las ofertas de un grupo de gente que desea vender y otro grupo que desea comprar. Para llegar a esta gran escala, es crucial la neutralidad, ya que es importante que cada transacción sea documentada en el momento exacto en que es realizada para mantener un orden cronológico y que los resultados sean imparciales y justos.

4.2. PLATAFORMAS DLT

Con frecuencia se utiliza erróneamente el término blockchain, un tipo de DLT, para referirse la tecnología en general (BBVA, 2018). Las plataformas basadas en blockchain funcionan de una forma determinada, pero tan válida como cualquier otra que cumpla con las características de la definición - que permita realizar transacciones de valor a través de internet entre desconocidos sin la intermediación de una entidad central que las controle.

Hay diferentes tipos de plataformas, desde públicas y de código abierto, en las que quien lo desee puede participar, hasta privadas y de requerida autorización previa. Las normas y el funcionamiento de cada una de ellas en particular quedarán recogidas en su código. A continuación, se explica el funcionamiento de blockchain y hashgraph, los tipos de plataformas más conocidas y relevantes a día de hoy, de acuerdo con su aparición en la serie documental de Mike Maloney *Hidden Secrets of Money* en su octavo episodio *From Bitcoin to Hashgraph* (2018). Con estas explicaciones será posible apreciar las similitudes en sus objetivos y las diferencias en funcionamiento, las cuales crean diferentes retos, pero superan algunas limitaciones. Todo esto será explorado en próximos apartados.

4.2.1. Blockchain

Blockchain es un tipo de software que funciona como un libro de registros digital, organizado como una cadena de bloques de transacciones, distribuido en una red entre pares (P2P) y cuyo propósito es mantener un registro permanente e inmutable de datos transaccionales. Bitcoin fue tanto la primera plataforma como aplicación del concepto blockchain, y Ethereum fue la primera en permitir la creación de contratos inteligentes.

Cada copia del software se denomina nodo, y estos pueden ser nodos completos o ligeros. Un nodo completo recoge toda la historia de la cadena de bloques mientras que un nodo ligero sólo es una lista parcial, aunque está conectada a uno completo para asegurar su fiabilidad.

La cadena está protegida por criptografía y organizada cronológicamente en bloques de transacciones datados y relacionados entre sí matemáticamente. La creación de bloques es periódica, como si fueran los latidos del sistema. Como ejemplo, en la cadena de bloques pública Bitcoin esto ocurre cada diez minutos. Si bien es cierto que los bloques están ordenados, las transacciones incluidas y su orden dentro de cada bloque dependen del minero que resuelva el bloque (pasxizeis et al., 2017). Para entender esto, se analizará el proceso de creación de bloques.

Este proceso comienza con las transacciones, que se llevan a cabo cuando dos participantes intercambian un activo digital o digitalizado. Dependiendo de los parámetros de la red, las transacciones pueden ser verificadas instantáneamente o transcritas en un registro seguro y colocadas en una cola de transacciones pendientes a verificar en un momento posterior (Piscini et al., 2016). Los nodos determinarán si las transacciones son válidas basándose en unas normas acordadas por la red que quedan reflejadas en el código de la blockchain, en el software. Teóricamente, todas estas transacciones serán añadidas a un bloque.

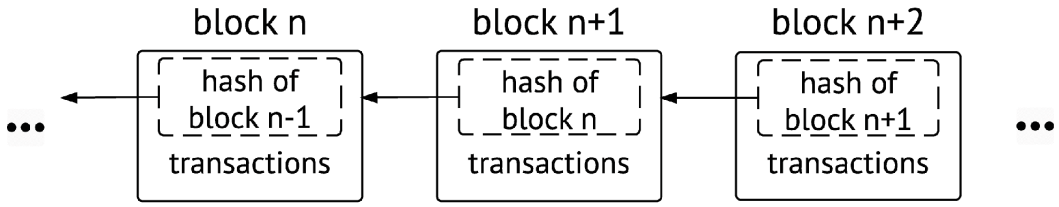

Figura 2 – Estructura blockchain. Fuente: Blockchains and Smart Contracts for the Internet of Things (Christidis, Devetsikiotis, 2016)

La cadena, entendida por el orden de los bloques, está protegida criptográficamente. Cada bloque está identificado por su cabecera, un resumen criptográfico o hash creado a partir de un algoritmo acordado por la red en el código del software. Cada bloque contiene su cabecera, una referencia al *hash* del bloque anterior y un grupo de transacciones. La secuencia de *hashes* interconectados crea la cadena de bloques. La referencia al bloque anterior hace de la cadena un elemento seguro, ya que todos

hashes contienen una referencia a su bloque precedente hasta “el principio del tiempo”, es decir, el primer bloque generado en esa cadena (Figura 2).

Antes de ser añadidos a la cadena, los bloques tienen que ser validados. En la mayor parte de blockchains de código abierto, el mecanismo de consenso utilizado es la prueba de trabajo o *Proof of Work* (PoW), la solución a un puzle matemático derivado de la cabecera del bloque. Además de PoW existen otros mecanismos de consenso más prometedores como la prueba de interés o *Proof of Stake* (PoS) y otras variaciones, adoptadas por otras plataformas como Ethereum (Cachin, Vukolić, 2017; Kostarev, 2017). El objetivo de esta prueba de trabajo es ralentizar la velocidad a la que los bloques son creados para evitar excesivas bifurcaciones, que se comentarán más adelante en este apartado. Los mineros intentan encontrar la solución del bloque, lo cual es un proceso repetitivo que requiere la inversión de una gran cantidad de capacidad de cálculo. Encontrar la solución para emitir un bloque es muy complejo, pero, por la naturaleza del tipo de criptografía utilizado, que el resto de participantes verifiquen que este es correcto es sencillo. Cuando un bloque es validado, se emite a la red y el minero que haya encontrado la solución del bloque es premiado. Cada nodo añade el nuevo bloque a la cadena y se aplican las transacciones para actualizar los balances de todos los participantes.

Cuando un participante emite un nuevo bloque y este es validado por el resto de participantes de la red, el primero es recompensado con una cantidad de un token o una criptomoneda, recibe una cuota de cada transacción, o una combinación de ambos sistemas. La cantidad y forma de la recompensa vienen determinadas por el código de la plataforma, acordado por la comunidad de usuarios. La razón por la que los mineros son premiados es motivar a los participantes de la red a validar nuevos bloques en la cadena, ya que el proceso requiere mucho poder computacional, el cual conlleva un gran gasto eléctrico con su correspondiente coste económico.

Además de lo anterior, la emisión de nuevos bloques mantiene la seguridad de la cadena. Existe la posibilidad de que se creen bifurcaciones, pero estas serán eliminadas. Debido a su código, el propio software escogerá la cadena más larga como válida. Se puede producir una bifurcación en la cadena de dos modos – en consenso o sin consenso (Herrera, 2018). Una bifurcación en consenso ocurre cuando varios nodos resuelven un bloque al mismo tiempo y se crean dos cadenas divididas. Esta situación es temporal, pues la cadena que encuentre el siguiente bloque se convertirá en la principal y la otra será descartada.

Una manipulación de los datos causaría una bifurcación sin consenso en la cadena. Cuanto más antigua sea una transacción, más segura se convierte, ya que hasta el más pequeño cambio causaría que el *hash* del bloque que contiene esa transacción fuera diferente, lo que cambiaría todos los *hashes* sucesivos. Cuando el resto de nodos detectan estos cambios, rechazan el bloque, por lo tanto, el manipulador tendría que conseguir replicar todos estos bloques y encontrar el nuevo mientras compite con el resto de participantes de la red que intentan emitir el bloque más reciente. Este proceso requeriría tal capacidad computacional que cambiar una transacción pasada se convierte en una tarea virtualmente imposible.

4.2.2. Hashgraph

Hashgraph es una estructura de datos y algoritmo de consenso que permite la creación de plataformas para el consenso distribuido, es decir, permite que una comunidad de usuarios llegue a un acuerdo sobre el orden en que se generan transacciones sin una autoridad central en la que confíen todos ellos. Hashgraph es la manera por la que los ordenadores que participan en la red van a comunicarse con el fin de ponerse de acuerdo en el orden y la datación de las transacciones que se realicen. Según los datos

del Libro Blanco de Hedera Hashgraph, en comparación con anteriores tecnologías, este software es rápido, seguro y justo (Baird, Harmon y Madsen, 2018).

En el año 2016 Leemon Baird publicó un documento sobre el nuevo mecanismo de consenso que había ideado y patentado: *Swirlds hashgraph consensus algorithm*. Él junto con Mance Harmon fundaron Swirlds Inc. en 2015 para ofrecer una plataforma sobre la que crear "la capa de confianza de internet". Como dicen en su web, "Swirlds es una plataforma que permite crear y operar mundos compartidos - aplicaciones completamente distribuidas que aprovechan el poder de la nube sin servidores". Su negocio principal ha sido la venta de licencias para el uso de hashgraph a entidades privadas, lo cual siguen haciendo. Más recientemente lanzaron su plataforma pública, Hedera Hashgraph. Esta plataforma todavía es muy nueva comparada con otras basadas en blockchain, aún no ha habido tiempo suficiente de comprobar su rendimiento en casos reales comparado a las cifras de sus pruebas teóricas, aunque del gran éxito de sus plataformas privadas se deduce que es un importante competidor en el entorno DLT.

Una de las mayores y más polémicas diferencias entre hashgraph y otros algoritmos de consenso es que está patentado en lugar de ser *open source*, aunque su código está disponible para revisión. En su Libro Blanco (Baird, Harmon & Madsen, 2018), Hedera es descrito como "un cuerpo de gobierno y plataforma hashgraph pública diseñada para servir las necesidades del mercado general". Sus creadores creen que para que una plataforma DLT sea adoptada de manera generalizada, es necesario que tenga un modelo de gobernanza establecido, que defina las normas y políticas que dictan la evolución del software, la expedición de criptomonedas y el modelo utilizado para incentivar la participación en la red. Para conseguir estabilidad en la plataforma Hedera Hashgraph, implantan unos mecanismos técnicos y legales con el propósito de proteger a los usuarios y empresas que operen en ella. Hedera tiene un modelo de gobernanza privado junto con consenso público o abierto. Esto quiere decir que el orden de las transacciones de será dictado por los usuarios de la plataforma, pero que las decisiones referentes a la estructura de Hedera serán tomadas por un comité de gobierno de la plataforma, constituido por un grupo de hasta 39 importantes empresas internacionales, expertas en diferentes industrias, que aportarán los conocimientos necesarios para el correcto funcionamiento de una DLT pública. Ninguna de estas empresas tendrá el control absoluto ni un poder mayor que otros miembros del comité.

Hashgraph es un mecanismo de consenso basado en votos virtuales, la combinación de un sistema de votos y protocolo *gossip*. Como explica en múltiples ocasiones su creador, Leemon Baird, esta combinación es clave (Hedera Hashgraph, 2017, 2018). Los sistemas de voto aseguran un consenso definitivo, pero son muy lentos. Como se explicó en el análisis del estado del arte, para que un sistema de votos sea efectivo, se necesitaría una gran cantidad de mensajes para compartir y comparar la información sobre los votos enviados y recibidos para alcanzar consenso en una simple acción, lo cual es completamente ineficiente. El protocolo *gossip* consiste en el envío aleatorio y exponencial de datos entre los participantes de una red. Como su nombre indica, los datos se difunden como cotilleos, es decir, de un nodo pasa a otro, estos dos se lo pasan a otros dos, esos cuatro a cuatro más y así crece exponencialmente. Este método es muy veloz para difundir información en una red, pero no aporta consenso ya que, debido a su aleatoriedad, cuando se difunden múltiples mensajes, estos no llegan en orden al resto de nodos.

Cuando ocurre una transacción en hashgraph, esta información es aleatoriamente distribuida mediante *gossip about gossip*, lo que se podría traducir como cotilleo sobre cotilleo. Este mecanismo consiste en no sólo difundir los datos de la transacción, sino cuándo y de quién se ha recibido este mensaje. Gracias a esta pequeña cantidad de información adicional, los participantes son capaces de crear un diagrama de la historia

de cómo un mensaje ha sido transmitido. Al analizar este diagrama, es posible conocer el momento en que un mensaje ha alcanzado a la mayoría de nodos y decidir de manera consensuada una data para todas las transacciones, es decir, una marca de fecha y hora. Este proceso sustituye la votación para llegar a un consenso. Es posible calcular lo que los otros nodos votarían, ya que todos conocen la misma realidad, por lo tanto, en lugar de un sistema de votos, se trata de un sistema de voto virtual o implícito. Este mecanismo es mucho más eficiente y justo que la prueba de trabajo (PoW) utilizada en muchas plataformas blockchain y, a diferencia de esta, llega a alcanzar un consenso total y justo sobre el orden de las transacciones, en lugar de una probabilidad creciente pero nunca total de que la transacción se ha producido.

En el Libro Blanco de Hedera Hashgraph se hace una comparación entre la estructura de las plataformas blockchain y hashgraph. Una de las diferencias entre ambas plataformas es la imparcialidad. En blockchain existe la figura de los mineros, que, como se explicó en el apartado anterior, pueden decidir qué transacciones añadir a sus bloques basándose en el beneficio económico que les aportarán. Cuando dos mineros resuelven un bloque simultáneamente, uno de ellos será descartado y las transacciones que no estén contenidas en el bloque “oficial” volverán a una cola de transacciones por añadir a la cadena. En hashgraph no existen los mineros, todos los participantes contribuyen a las decisiones que ordenan las transacciones, y todas ellas son añadidas al diagrama de *hashes* (Figura 3). Las transacciones son ordenadas de manera imparcial, ya que el orden es decidido en base a la data acordada por la comunidad. Toda la comunidad participa en el proceso de datación; ningún nodo puede generar esta información aisladamente. La data se calcula mediante el diagrama de hashes como la mediana de las horas a las que la mayoría de los nodos han recibido esa transacción. Esta imparcialidad es crucial para algunas aplicaciones a nivel de mercados.

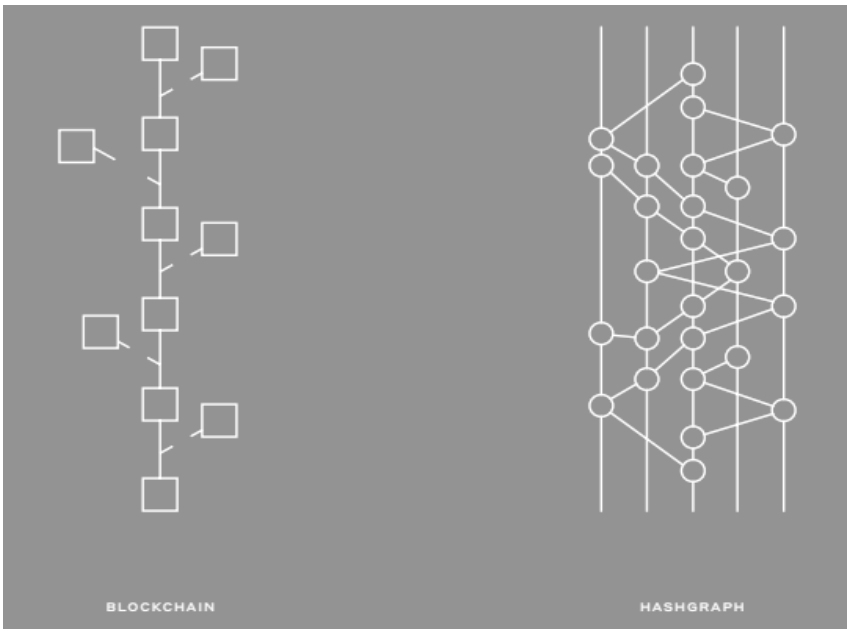

Figura 3 – Estructura blockchain vs. Hashgraph. Fuente: Hedera: A Governing Council and Public Hashgraph Network (Baird, Harmon y Madsen, 2018)

Gracias a abandonar la prueba de trabajo (PoW), hashgraph es muy rápido comparado con otras plataformas blockchain. En lugar de un puñado de transacciones, es capaz de procesar cientos de miles de transacciones por segundo. Consigue una latencia de segundos, que es el periodo de tiempo desde que la transacción se ejecuta hasta que hay una seguridad completa de que esta ha ocurrido, con una prueba criptográfica de que toda la red la ha recibido y está de acuerdo con ella. Como declaran en la web, “las aplicaciones construidas en la plataforma Swirlds son justas, veloces, y alcanzan

consenso rápidamente, dándole al usuario 100% seguridad del orden acordado". Estas características permiten crear nuevas aplicaciones que no eran posibles con la anterior tecnología.

4.3. NIVELES DE APLICACIÓN

Las posibilidades que la DLT trae consigo son inconmensurables, algunas tan difíciles de imaginar con nuestra limitada experiencia actual como lo eran las aplicaciones de internet en sus primeras décadas de existencia. Cada día se generan nuevas ideas de uso de esta tecnología para la resolución de problemas o la creación de nuevos servicios que no eran posibles hasta el momento.

A partir de las ideas, los conceptos de proyectos y las aplicaciones ya en práctica que uno puede encontrar online, hemos identificado una jerarquía que podría desencadenar un enorme potencial de la DLT (Figura 4).

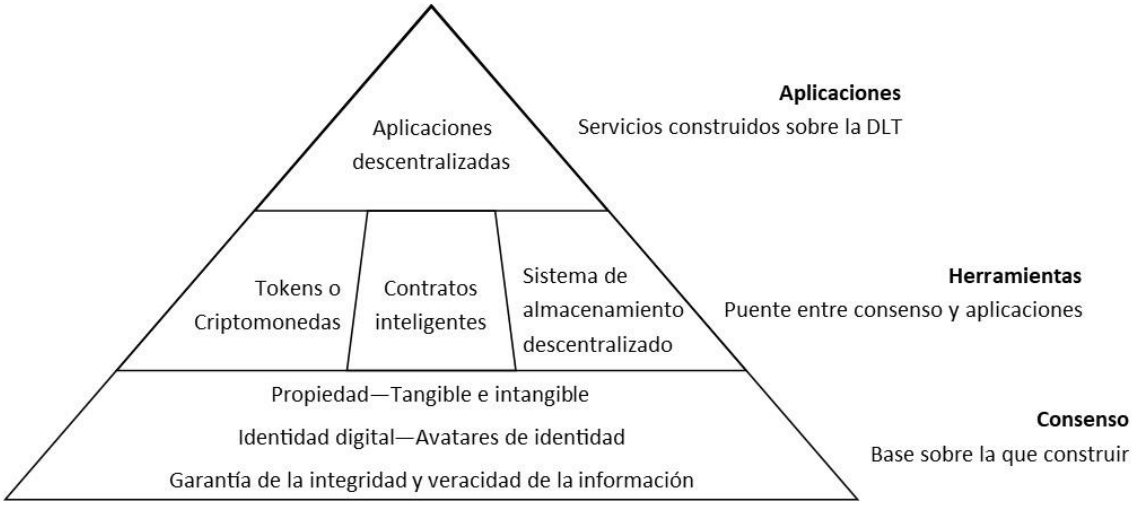

Figura 4 – Jerarquía para la aplicación de la tecnología de registro distribuido (DLT). Fuente: Elaboración propia

Si bien es cierto que no todas las aplicaciones requerirán saber todo sobre el usuario, este esquema es una forma práctica de organizar en un orden lógico el máximo de necesidades que una plataforma podría exigir. El ideal en las plataformas públicas sería que el usuario tenga el control total sobre su identidad y su privacidad.

4.3.1. Consenso – La base sobre la que construir

En primer lugar, es crucial que existan mecanismos por los cuales se garantice la integridad y veracidad de la información recogida en las plataformas DLT. Cuando una información se introduce en la plataforma, esta es inmutable y no hay modo de modificarla, únicamente de transaccionar con ella. Por esto es necesaria la intervención de un tercero de confianza a la hora de tokenizar o integrar información en la plataforma de forma seria y fiable, como un notario o un organismo de gobierno, que certifique que lo que se está introduciendo en la plataforma de verdad existe y que es exigible a la hora de hacer transacciones (Libro Blockchain, 2017f; Kravchenko, 2018). En palabras del notario Javier González Granado en una entrevista por Óscar Domínguez (2016), "Blockchain no va a acabar con el notariado, es un instrumento al que no ay que tenerle miedo sino ponerlo a nuestro servicio".

Cuando hay confianza en que la información es veraz, el siguiente paso son las identidades digitales. Carlos Kuchkovsky Jiménez, CTO de New Digital Business en BBVA y miembro del consejo del proyecto Hyperledger, en una entrevista para Libro Blockchain (2017d), comenta algo muy importante para el avance social en la DLT – es indispensable tener una identidad digital oficial, expedida por el gobierno. Es cierto que

en la actualidad las personas tienen diferentes identidades digitales, pero no están integradas y no hay un organismo oficial que verifique que esta información es cierta. Kuchkovsky dice que "la identidad digital es el capacitador principal para una transformación digital de la sociedad". También menciona la importancia de tener la posibilidad de generar avatares de identidad. En el mundo actual, tanto físico como digital, tu identidad de cara al gobierno y a empresas como bancos, aseguradoras o servicios públicos, no es la misma que tu identidad de cara a tus círculos sociales. "La identidad está vinculada a la reputación" y la reputación de una persona en un grupo no debería influir a todas las demás áreas de su vida, como ocurre en el episodio *Nosedive* (Wright, 2016) – en España "Caída en picado" – de la aclamada serie *Black Mirror*.

Cuando la información recogida en las plataformas DLT es veraz y está vinculada a las personas de manera oficial, es posible registrar a su nombre todo tipo de propiedad que estas puedan tener, tanto tangible como intangible. Desde los propios certificados de identidad, permisos y titulaciones oficiales, hasta la propiedad de terrenos o inmuebles y la propiedad intelectual o industrial. Estos tres niveles de la pirámide crean una base muy sólida para construir aplicaciones que aprovechen de manera justa los recursos de las personas, teniendo cada individuo el control de su identidad, información y propiedad, siendo capaz de percibir las ganancias económicas que con su uso puedan producir.

4.3.2. Herramientas – El puente entre el consenso y las aplicaciones

Entre la base de una información veraz y las aplicaciones, que son las que aportan valor a los usuarios, son necesarias unas herramientas que faciliten las interacciones entre participantes de la red. En el Libro Blanco de Hedera Hashgraph (Baird, Harmon & Madsen, 2018) se describen los elementos que conforman este segundo nivel, lo cual es extrapolable a otras plataformas. Estos elementos son las criptomonedas o tokens, los contratos inteligentes y un sistema de almacenamiento de datos descentralizado. Estos tres elementos, además de ser herramientas, que como se expondrá en el siguiente apartado, podrían ser utilizados como aplicaciones.

El sistema de almacenamiento permitirá a los usuarios alcanzar un consenso sobre lo que está o no está almacenado en la plataforma. Las criptomonedas o tokens permitirán realizar transacciones en las aplicaciones de la plataforma. Por último, los contratos inteligentes harán posible la automatización de transacciones y la creación de aplicaciones descentralizadas en la plataforma.

4.3.3. Aplicaciones – Servicios construidos sobre la DLT

El tercer nivel son las aplicaciones que aportan valor a los usuarios de la plataforma DLT. Los únicos límites de este nivel son la imaginación de los creadores y programadores. Existen ya muchos servicios ofrecidos gracias a la DLT y en el futuro, con la maduración de las plataformas, surgirán infinidad de aplicaciones que aprovecharán las enormes posibilidades que la tecnología ofrece. En este trabajo se expondrán algunas de ellas para mostrar cómo la DLT será disruptiva y cambiará el funcionamiento y el modelo económico de muchas industrias.

Las criptomonedas son un tema muy amplio, complejo y en constante evolución al que se podría dedicar más de un trabajo completo. Bitcoin fue la primera aplicación blockchain y fue el detonante de toda la evolución de la tecnología DLT. En la actualidad Bitcoin es un activo con múltiples usos. Es difícil verlo como método de pago habitual, ya que no está muy extendido y es muy volátil. En la actualidad se trata más de un activo sobre el que especular que de una moneda útil para la compra de bienes y servicios (Fundación Bankinter, 2018). Algunas plataformas, como Ripple, usan Bitcoin como puente entre diferentes monedas fiat. Explica Susan Athey en un vídeo de *Stanford Graduate School of Business* (2015) que, aunque su valor no es muy estable en

periodos de tiempo más largos, estos intercambios se llevan a cabo en cuestión de minutos y la fluctuación de su valor no es considerable, por lo que es útil como moneda de cambio.

Como elemento de inversión, las criptomonedas se han convertido en un activo financiero más en el que repartir la riqueza. Javier Molina, Economista y Máster en Mercados Financieros justifica esto en una entrevista para Libro Blockchain (2017a) definiendo las características de un activo financiero, que son la liquidez, la rentabilidad y el riesgo. La oferta y la demanda de estos activos indica la certeza de que se vayan a poder vender en el momento en que se desee. La novedad de esta forma de representación de valor dificulta la percepción de las criptomonedas como un método de distribución de los ahorros, especialmente las criptomonedas menos conocidas. A día de hoy, Bitcoin es la más intercambiada y Ethereum cobra importancia. Estas inversiones conllevan un riesgo alto, aunque a cambio ofrecen más rentabilidad, por lo tanto, no serán adecuadas para todos los perfiles inversores y normalmente tampoco representarán grandes proporciones de los patrimonios de las personas. Sus ventajas principales son la diversificación y la independencia de las criptomonedas con el resto de tipos de activos financieros en los que podrían consistir las carteras de inversión. En cuanto al modo de valorar y gestionar su riesgo, Molina explica que se aplicaría el análisis técnico de manera similar a cómo se gestionarían acciones u otro tipo de activos financieros.

La siguiente herramienta que podría tener aplicaciones por sí misma son los sistemas de almacenamiento descentralizado. Por ejemplo, permitirían a organismos oficiales la expedición y revocación de documentos y certificados oficiales ligados a las personas. De acuerdo con las aclaraciones del Libro Blanco de Hedera Hashgraph (Baird, Harmon y Madsen, 2018), en esta plataforma en concreto la información estará almacenada de tal forma que no se pierda en caso de que algún nodo falle y sólo podrá ser emitida y eliminada por quienes tengan permiso. Un ejemplo es la expedición de un permiso de conducción a un usuario por la Dirección General de Tráfico. Ambos actores firmarían digitalmente una transacción para añadir un *hash* al documento, el cual es inmutable, aunque cualquiera de los dos podría actualizarlo o eliminarlo en el futuro, y se incorporaría a la plataforma DLT. Este *hash* es la forma que un tercero tendría de comprobar que ese documento sigue siendo válido. Cuando el usuario quisiera probar que tiene este permiso, le entregaría al tercero una copia del archivo y este podrá comprobar que su *hash* sigue estando en la plataforma y por lo tanto que el documento es válido en ese momento.

La identidad digital permitirá el desencadenamiento de grandes cambios en los modelos de negocio actuales. Por ejemplo, en una entrevista para Libro Blockchain (2017e), el experto en innovación y emprendimiento Ignacio Madrid Benito presenta el concepto de energía móvil. Hasta ahora el consumo energético de una persona se vincula al contador de su casa, pero la integración de su identidad digital con aplicaciones DLT permitirá la contabilización de su consumo de energía en cualquier lugar en su contrato energético. Es decir, que el consumo energético de una persona sea personal y se desvincule de un lugar físico concreto.

Gracias a los contratos inteligentes, la economía colaborativa vivirá una gran transformación. Las plataformas que entendemos como colaborativas en la actualidad, como pueden ser Airbnb, Uber o Blablacar, son plataformas agregadoras de servicios que se benefician económicamente gracias a los individuos que están dispuestos a compartir sus recursos (Talks at Google, 2016; TED, 2016). Los usuarios necesitan estas plataformas para dar visibilidad a sus ofertas. A través de un sistema sin intermediarios que absorban parte de las ganancias económicas, la economía colaborativa podría beneficiar estrictamente a quienes intercambien sus recursos.

A nivel de mercados y volviendo al ejemplo de la electricidad, también será posible la aparición de mercados de electricidad sin intermediarios. Las personas que produzcan energías renovables desde sus hogares, por ejemplo, con paneles solares, podrán vender automáticamente, a través de un contrato inteligente, la energía que produzcan en exceso y no vayan a utilizar y comprar más cuando no estén generando suficiente para cubrir sus necesidades. Leemon Baird (Hedera Hashgraph, 2018), da un ejemplo sobre este nivel de mercados que escapa del ámbito financiero. Imagina un videojuego global en el que sea importante saber qué acción ha ocurrido primero, si un disparo o un regate, ya que de este orden depende el resultado. Si el regate ocurrió primero, el disparo no matará al contrincante.

La integración de la DLT con otras tecnologías innovadoras dará lugar a multitud de nuevos modelos de negocio. Por ejemplo, relacionado al Internet de las cosas o *Internet of things* (IoT), una empresa que fabrique vehículos autoconducidos podría tener una flota que ofreciera servicios de transporte a las personas que lo soliciten. El coche, gracias a sus sensores y al estar completamente digitalizado, podrá hacerse cargo de su propio mantenimiento cuando sea necesario. Tendrá la capacidad de ir a un taller, comunicar sus necesidades y, con el dinero obtenido a través de sus servicios, pagar por las reparaciones.

En otra entrevista para Libro Blockchain (2017c), Daniel Díez y Gonzalo Gómez hablan sobre las aplicaciones de las nuevas tecnologías en el sector de los seguros. Dan un sencillo ejemplo que ilustra la mejora en la eficiencia a través de la simplificación de los procesos. En el ejemplo, un contrato inteligente que represente un seguro de viajes podrá detectar automáticamente, a través de *big data*, que un vuelo se ha retrasado y compensar al cliente directamente, sin necesidad de que este haga una reclamación. La mejora en la experiencia de los clientes sería notable.

Las microtransacciones serán una de las aplicaciones más útiles para los creadores de contenido. Los usuarios podrán beneficiarse económicamente del contenido que creen, por pequeño que sea, y podrán apoyar a otros creadores de forma directa cuando consuman su contenido. Uno de los primeros ejemplos reales de esto ocurrió con la iniciativa de la cantante Imogen Heap de compartir su sencillo "*Tiny Human*" en Ethereum, una plataforma DLT, mediante un contrato inteligente (Serres, 2017). Mediante este contrato inteligente cualquiera puede comprar licencias para descargar, escuchar en *streaming*, remezclar o sincronizar la canción. Los pagos son realizados a través de la plataforma acorde al uso que se haga de la canción, y los beneficios son repartidos entre ella y sus colaboradores por la parte que a cada uno le corresponde. Este tipo de iniciativas permiten que los artistas tengan una compensación más justa y un mayor control sobre sus creaciones, que hasta ahora quedaban insuficientemente protegidas en internet. Al igual que músicos, se podría aplicar a otros artistas, desde escritores, editores o diseñadores gráficos, hasta fotógrafos o productores de vídeo; todas las personas de las que depende que una obra quede completada.

Algunos otros ejemplos de aplicaciones podrían ser: seguimiento de la cadena de suministros y prueba de procedencia, seguimiento de las labores de ONGs, voto por internet, *crowdfunding*, microtransacciones en medios de comunicación, seguridad informática, descentralización del Internet de las cosas, aplicaciones militares, aplicaciones en Internet, *smart cities*, alquiler de propiedades, seguridad automatizada, etc. Estas son una pequeñísima muestra de todas las aplicaciones que posibilita la DLT (Rodríguez, 2016), y esta lista se hace más grande cada día.

4.4. RETOS

La DLT tiene un enorme potencial, pero, coincidiendo con el escepticismo de *The Economist* (2015) y *Harvard Business Review* (Iansiti, Lakhani, 2017), cada plataforma tiene una serie limitaciones técnicas que resolver y retos que afrontar para llegar a ser

considerada una opción seria y fiable como medio sobre el que desarrollar modelos de negocio o procesos oficiales. A continuación, se exponen de forma no exhaustiva algunos de los retos presentes, pero existen más y seguirán apareciendo según vaya pasando el tiempo (Tabla 1).

Tabla 1 – Retos de la tecnología de registro distribuido DLT. Fuente: elaboración propia

Criptoeconomía	• Nuevo modelo económico • Funcionamiento y uso de criptomonedas • Evolución de las criptomonedas en el futuro
Funcionamiento	• Velocidad • Escalabilidad • Impacto medioambiental • Interoperabilidad
Seguridad	• Privacidad • Robo o pérdida de activos • Vulnerabilidad a ataques informáticos
Gobernanza y estabilidad	• Bifurcaciones en blockchain • Pericia en ámbitos complementarios a la DLT - técnico, económico, regulatorio • Modelo de financiación de las transacciones • Sistema de incentivos en las plataformas
Conformidad con la legislación	• Anonimato • Control de la veracidad de los datos

4.4.1. Criptoeconomía

Como ya se ha mencionado anteriormente, las criptomonedas son un tema inmenso y complicado. Como planteamiento general, uno de los retos que afrontar es el funcionamiento, uso y evolución de las criptomonedas en el futuro, ya que tienen un modelo de funcionamiento que ha sido poco utilizado en los últimos tiempos - un modelo deflacionario (Hulleman, 2017). Deflacionario significa que, con la misma cantidad de una moneda, se podrá adquirir más valor en el futuro que en el momento actual.

Históricamente, el valor del dinero estuvo ligado al oro durante mucho tiempo, el cual es finito y, por lo tanto, deflacionario. Este modelo ha ido sufriendo muchas transformaciones hasta el momento actual, en el que la cantidad de dinero en circulación está dictada por los bancos centrales en un modelo inflacionario.

Las criptomonedas, al menos las más conocidas hasta el momento, responden al modelo deflacionario debido a sus propias normas de funcionamiento. Por ejemplo, habrá un número limitado de Bitcoin en el mundo, por lo tanto, su valor crecerá en el tiempo, al contrario que el valor del dinero en la actualidad, el cual decrece. Con una cierta cantidad de moneda, podrás adquirir hoy más de lo que se podrá mañana.

Cuando el modelo es inflacionario las personas están motivadas a consumir en el momento actual, pero cuando este es deflacionario, mantener ese dinero sin gastar permitirá adquirir más valor en el futuro, por lo tanto, el consumo se paraliza. Sería necesario analizar e idear modelos económicos alternativos, posiblemente menos dependientes en el consumo por el consumo.

4.4.2. Funcionamiento de las plataformas DLT

Los retos técnicos de las plataformas no son pocos, y se trabaja constantemente para conseguir mejoras en su velocidad y escalabilidad. Nuevos mecanismos como hashgraph parecen resolver muchos de estos problemas, por lo que habrá que seguir prestando atención a innovaciones de este tipo, siendo lo ideal que encuentren soluciones a los problemas de raíz y no consistan en arreglos encima de un sistema imperfecto.

Es muy importante tener en cuenta las implicaciones medioambientales de los diferentes mecanismos de consenso. El inmenso impacto negativo de la prueba de trabajo, una de las más populares en las plataformas blockchain, es injustificable. Como ejemplo ilustrativo, la web Digiconomist (2018) compara en el gráfico siguiente (Figura 5) el consumo energético de las plataformas Bitcoin y Ethereum con el sistema de pagos VISA. El gráfico muestra la energía total consumida por cada una de estas redes, medida como el número total de hogares en Estados Unidos que podrían ser abastecidas, en millones. Toda la energía gastada por la red Bitcoin podría abastecer 6 millones de hogares y Ethereum casi 2 millones. Al lado de esto, el consumo de VISA es insignificante; podría abastecer 17 mil. En la misma web se indica que por cada transacción en Bitcoin, 30 hogares podrían ser abastecidos durante un día completo, y en Ethereum 3 hogares.

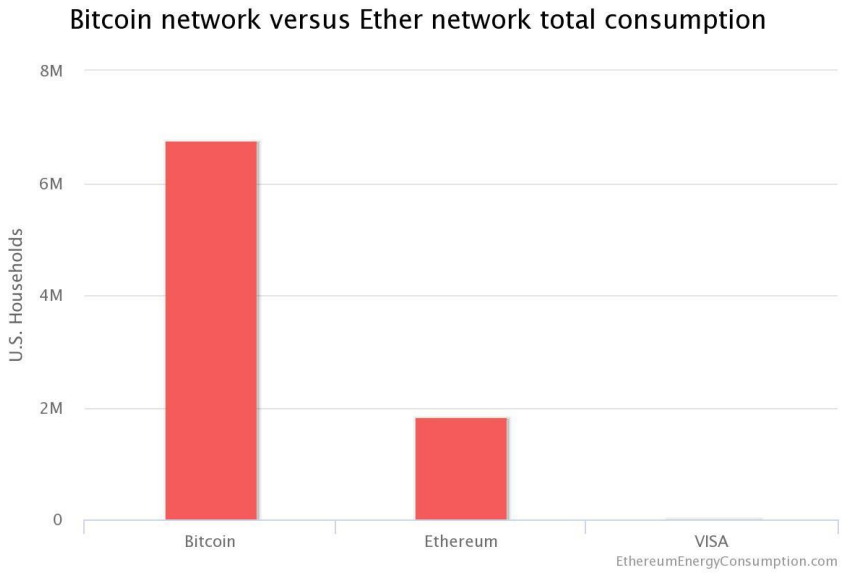

Figura 5 – Comparación del consumo energético total de Bitcoin, Ethereum y VISA. Fuente: Ethereum Energy Consumption Index (beta) (Digiconomist, 2018).

Por último, también es interesante plantear la interoperabilidad entre plataformas, ya que una de las mayores oportunidades que la DLT ofrece es la colaboración social. Con cada plataforma siendo desarrollada por diferentes grupos de personas que persiguen objetivos diversos y emplean mecanismos de funcionamiento variados, es probable que muchas plataformas sean incompatibles. Esto iría en contra de la idea de integración y es posible que dificulte los proyectos para los que las personas acuden a la DLT.

4.4.3. Seguridad

Los escándalos de seguridad que sufrieron algunas plataformas DLT son los que provocaron las malas connotaciones que perjudican la reputación de la prometedora tecnología. Se han robado criptomonedas y se han perdido otras muchas. Se han llevado a cabo actos criminales aprovechando el anonimato que estas plataformas aportan (Juels, Kosba y Shi, 2016). Lo que es importante tener en cuenta es que estas plataformas son una mera herramienta, que al igual que cualquier otra pueden ser

usadas para múltiples fines. De hecho, Kathryn Haun, del departamento de justicia de Estados Unidos, cuenta en un vídeo de TEDx Talks (2016) que la inmutabilidad de estas plataformas ha permitido resolver crímenes que en un primer momento fueron facilitados por ellas mismas.

A pesar de parecer ser anónimas, la privacidad no es tan alta en ciertas plataformas como se pensaba. En 2013 (Meiklejohn et al.), se hizo un estudio que indica que, a pesar de que las transacciones en Bitcoin sean anónimas, es posible analizar los flujos de transacciones mediante un método de agrupación y asociar las claves públicas a identidades reales, ya sean personas u organizaciones. La comparación de las criptomonedas al dinero metálico no es perfecta, ya que con metálico no se necesita ningún tercero para que la transacción sea válida – se intercambia un objeto tangible. En las transacciones con criptomonedas, estas necesitan un "tercero", la red global P2P que valida y certifica las transacciones. Por esto, el estudio concluye que las identidades de Bitcoin son pseudoanónimas. Que los usuarios consigan mayor anonimidad supondría mucho esfuerzo por su parte, lo que conlleva una pérdida de practicidad que únicamente será atractiva para los usuarios más motivados, como podrían ser los que tuvieran intenciones criminales.

Hacer hincapié en la educación sobre la seguridad informática es primordial. La seguridad en la DLT depende de cada usuario. Si no mantiene segura su clave privada, un usuario es susceptible de perder sus activos o ser robado. Pero esto no es un problema de DLT, sino un problema de seguridad en general. Aunque uno tenga la mejor cerradura en la puerta de su casa, si deja la llave debajo del felpudo cualquiera puede entrar a robar. Por esto es importante que se insista en la importancia de mantener la vida electrónica tan segura como se hace con la física.

También queda abierta la posibilidad de que las plataformas que hasta el momento han sido seguras, se tornen vulnerables a ataques informáticos más sofisticados, ya que históricamente el software malicioso ha ido avanzando para aprovecharse de las innovaciones tecnológicas. En este aspecto no hay un momento en el que se vaya a poder prometer una seguridad del 100%.

4.4.4. Gobernanza y estabilidad

Como exponen Don y Alex Tapscott (2018) y los creadores de hashgraph (Baird, Harmon y Madsen, 2018), el entorno DLT necesita una gobernanza más organizada y responsable. Muchos problemas podrían ser evitados si existiera un organismo que, gracias a sus conocimientos y experiencia, aconsejara o guiara el camino que la DLT sigue. Mucha de la inestabilidad que algunas plataformas blockchain han sufrido en el pasado se debe a bifurcaciones en sus cadenas de bloques cuando la comunidad no ha sido capaz de llegar a un acuerdo común sobre la dirección de la plataforma.

Ya hay una necesidad, que únicamente irá en aumento, de mano de obra debidamente cualificada para llevar a cabo proyectos que requieran amplios conocimientos técnicos, como programar para estas plataformas DLT. Además de programar, serán necesarios abogados, notarios y profesionales de otros ámbitos que necesitarán entender el lenguaje técnico para asegurarse de que los contratos inteligentes o las aplicaciones están programadas correctamente para hacer lo que se supone que deben (Yabo, 2018). Por esto, cada vez cobrarán más importancia los programas académicos que incluyan estos contenidos.

También hay que tener en cuenta el método de incentivos para la participación y el consenso, y el modelo de financiación de las transacciones en las plataformas DLT. Como dice Carlos Vivas en una entrevista para Libro Blockchain (2017b), el que no haya intervención humana en los procesos no quiere decir que estos sean gratuitos. Seguirá

habiendo costes de energía, procesamiento, cómputo, infraestructura, etc. Todo esto tiene un coste económico que de alguna forma tendrá que ser pagado.

4.4.5. Conformidad con la legislación

El anonimato en las plataformas públicas es una de las características más atractivas en la DLT, pero puede dar pie a actividades delictivas como las que dieron mala fama a Bitcoin en sus primeros años de existencia – en el documental de Netflix *Banking on Bitcoin* (Cannucciari, 2016) se explica cómo Bitcoin fue usado para el tráfico de drogas en el conocido caso de *Silk Road*. Por ejemplo, una solución que ofrece Hedera Hashgraph en su Libro Blanco es el aporte voluntario por parte del usuario de sus datos de identidad oficial, que seguirían siendo privados, aunque permitirían un mayor control por parte de las autoridades cuando sea necesario para prevenir actividad criminal.

Por último, el control de la veracidad de los datos introducidos en las plataformas es esencial, ya que, como se menciona previamente, estos son inmutables. Sin confianza en que la información recogida en la plataforma DLT es auténtica, no es posible hacer transacciones con ella.

5. CONCLUSIONES

Tras esta recopilación de información es posible comprender mejor la tecnología de registro distribuido (DLT), que permite realizar transacciones de valor a través de internet entre desconocidos sin la intermediación de una entidad central que las controle. Crea consenso en un grupo de personas entre las que no hay confianza mutua.

- La tecnología DLT ha tenido cuatro etapas en su evolución, que fueron surgiendo basándose en las anteriores - criptomonedas, registro de transacciones, contratos inteligentes y mercados. Todas ellas siguen madurando con el paso del tiempo.
- Existen muchas plataformas DLT de diversos tipos, tanto públicas como privadas. Las dos plataformas más relevantes a día de hoy se diferencian en su arquitectura, funcionamiento y mecanismos de consenso – desde la prueba de trabajo (PoW) en blockchain hasta hashgraph, la novedad más prometedora en el momento actual.
- Para la aplicación generalizada de esta tecnología es necesaria una base sólida que permita garantizar la integridad y veracidad de los datos sobre identidad y propiedad recogidos en las plataformas, la cual, a través de unas herramientas - criptomonedas o tokens, contratos inteligentes y un sistema de almacenamiento de archivos descentralizado - permitirá crear infinidad de aplicaciones que aporten valor a los usuarios.
- Aún hay muchos retos que la DLT tiene que afrontar para llegar a un uso y aceptación generalizada. Estos retos abarcan desde el funcionamiento de la nueva criptoeconomía, el funcionamiento de las mismas plataformas, pasando por la seguridad, la gobernanza y la estabilidad, hasta la conformidad con la legislación.

El uso de la DLT pone en cuestión el paradigma económico más extendido y utilizado hasta el momento actual, lo que afecta también al ámbito sociocultural, por lo que será necesario construir nuevos modelos que permitan comprender los mecanismos de la nueva criptoeconomía y analizar los cambios culturales que surgirán a través de las nuevas aplicaciones que esta tecnología posibilita.

5.1. LIMITACIONES DEL TRABAJO Y POSIBLES LÍNEAS DE INVESTIGACIÓN FUTURA

Aunque se han consultado muy diversas fuentes de información sobre la tecnología analizada, la cantidad disponible es mucho mayor, por ello existe una limitación en la información utilizada para la redacción del trabajo. Además, debido a la cambiante naturaleza de la tecnología y su corta existencia, este trabajo queda limitado en el tiempo. Por ejemplificar estos cambios constantes, la plataforma Hedera Hashgraph fue puesta en marcha hace menos de un mes, la última semana de agosto de 2018. La tecnología continuará evolucionando, pasará por diferentes etapas y se hará evidente qué plataformas sobrevivirán y cuáles se quedarán atrás. Además, su adopción por un público más general permitirá la generación de nuevas ideas de las que surgirán otras innovaciones y modelos de negocio, los cuales serán interesantes de investigar en el futuro.

Hay muchos aspectos relacionados con la DLT que quedan fuera del ámbito de este trabajo, pero que son de gran interés para futuras líneas de investigación. Como ejemplos se proponen:

- La criptoeconomía, entendida como la economía generada gracias al uso de las criptomonedas. La creación de un nuevo modelo a través del cual entender su funcionamiento.
- El seguimiento continuado de las plataformas DLT, su evolución y su uso real en el futuro.
- El uso de la DLT en combinación con otras tecnologías actuales como el internet de las cosas, el big data o la inteligencia artificial.
- El análisis de las ventajas competitivas que consigue un negocio que implemente el uso de la DLT en sus operaciones.

6. BIBLIOGRAFÍA

BAIRD, L. 2016. *The Swirlds Hashgraph Consensus Algorithm: fair, fast, byzantine fault tolerance.* White Paper, Swirlds Inc. [Consulta: Agosto, 2018]. Disponible en: <https://www.swirlds.com/downloads/SWIRLDS-TR-2016-01.pdf>.

BAIRD, L., Harmon, M. y Madsen, P. 2018. *Hedera: A Governing Council and Public Hashgraph Network.* White Paper, Hedera Hashgraph. [Consulta: 23 Agosto, 2018]. Disponible en: <http://hedera-hashgraph.s3.amazonaws.com/hh-whitepaper-v1.0-180313-2.pdf>.

BBVA. 2018. *¿Cuál es la diferencia entre una DLT y 'blockchain'?* BBVA. [Consulta: 23 Agosto, 2018]. Disponible en: <https://www.bbva.com/es/diferencia-dlt-blockchain/>.

BHARADWAJ, K. 2016. *Blockchain 2.0: Smart Contracts.* Paper, linkDapps. [Consulta: 2 Julio, 2018]. Disponible en: <http://www.linkdapps.com/Blockchain2.0-SmartContracts.pdf>.

CACHIN, C. y Vukolić, M. .2017, Blockchain Consensus Protocols in the Wild. Disponible en: <http://arxiv.org/abs/1707.01873>.

CANNUCCIARI, C. 2016. *Banking on Bitcoin.* [Documental en Netflix]. [Consulta: 12 Julio, 2018].

CHRISTIDIS, K. & Devetsikiotis, M. .2016, Blockchains and Smart Contracts for the Internet of Things. *IEEE Access,* **vol. 4**pp. 2292-2303. ISSN 2169-3536. Disponible en: <https://ieeexplore.ieee.org/document/7467408>.

Digiconomist 2018. *Ethereum Energy Consumption Index (beta).* Digiconomist. [Consulta: 14 Septiembre, 2018]. Disponible en: <https://digiconomist.net/ethereum-energy-consumption>.

DOMINGUEZ, O. 2016. *"Blockchain no va a acabar con el notariado, es un instrumento que tenemos que poner a nuestro servicio".* En: Territorio Bitcoin, Información independiente de Bitcoin Blockchain y Fintech en España. [Consulta: 29 Junio, 2018]. Disponible en: <https://www.territoriobitcoin.com/blockchain-no-va-a-acabar-con-el-notariado-es-un-instrumento-que-tenemos-que-poner-a-nuestro-servicio/>.

Fundación Bankinter. 2018. *¿Qué es el bitcoin? Conoce cómo se creó la popular criptomoneda.* Fundación Bankinter. [Consulta: August 23,]. Disponible en: <https://www.fundacionbankinter.org/blog/noticia/future-trends-forum/-que-es-el-bitcoin-conoce-como-se-creo-la-popular-criptomoneda>.

GoldSilver (w/ Mike Maloney). 2017. *From Bitcoin To Hashgraph (Documentary) Hidden Secrets Of Money Episode 8.* [Vídeo en YouTube]. Mike Maloney. [Consulta: Agosto, 2018]. Disponible en: <https://www.youtube.com/watch?v=SF362xxcfdk>.

GRIMES, R.A. 2018. *Why blockchain isn't always the answer.* CSO Online. [Consulta: 4 Julio, 2018]. Disponible en: <https://www.csoonline.com/article/3269236/blockchain/why-blockchain-isn-t-always-the-answer.html>.

Hedera Hashgraph. 2018. *How Hashgraph Works - Leemon Baird @ Thomson Reuters (2/21/2018).* [Vídeo en YouTube]. Leemon Baird. [Consulta: Agosto, 2018]. Disponible en: <https://www.youtube.com/watch?v=IVlmwsleu6c&t=886s>.

Hedera Hashgraph. 2017. *Leemon Baird x Harvard Talk - Hashgraph: New Directions for Blockchains & Distributed Ledgers.* [Vídeo en YouTube]. Leemon Baird. [Consulta: Agosto, 2018]. Disponible en: <https://www.youtube.com/watch?v=IjQkag6VOo0>.

HERRERA, C. 2018. *¿Qué es la capitalización de mercado y por qué no define el valor de una criptomoneda?* Coincrispy. [Consulta: 16 Septiembre, 2018]. Disponible en: <https://www.coincrispy.com/2018/05/15/capitalizacion-mercado-criptomonedas/>.

HULLEMAN, M. 2017. *Bitcoin is a Deflationary Currency: What does it Mean?* Invest In Blockchain. [Consulta: Septiembre, 2018]. Disponible en: <http://www.investinblockchain.com/bitcoin-is-a-deflationary-currency/>.

IANSITI, M. & Lakhani, K.R. 2017. *The Truth About Blockchain.* Harvard Business Review. [Consulta: 4 Julio, 2018]. Disponible en: <https://hbr.org/2017/01/the-truth-about-blockchain>.

JUELS, A., Kosba, A. & Shi, E.2016, The Ring of Gyges: Investigating the Future of Criminal Smart Contracts. *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security,* pp. 283–295. Disponible en: <http://doi.acm.org/10.1145/2976749.2978362>.

KOSTAREV, G. 2017. *Review of blockchain consensus mechanisms.* Waves Platform. [Consulta: 12 Julio, 2018]. Disponible en: <https://blog.wavesplatform.com/review-of-blockchain-consensus-mechanisms-f575afae38f2>.

KRAVCHENKO, P. 2018. *¿Necesitan los contratos inteligentes ser jurídicamente vinculantes?* Blockchain Media. [Consulta: 20 Junio, 2018]. Disponible en: <https://www.blockchainmedia.es/single-post/2018/05/17/%C2%BFNecesitan-los-contratos-inteligentes-ser-jur%C3%ADdicamente-vinculantes>.

Libro Blockchain. 2017a. *¿Cómo invertir en la Blockchain y criptomonedas? - Javier Molina.* [Vídeo en YouTube]. Javier Molina. [Consulta: Septiembre, 2018]. Disponible en: <https://www.youtube.com/watch?v=MTuUPfkf_hA>.

Libro Blockchain. 2017b. *¿Cómo utilizar Smart Contracts en Blockchain? Carlos Vivas.* [Vídeo en YouTube]. Carlos Vivas. [Consulta: Agosto, 2018]. Disponible en: <https://www.youtube.com/watch?v=sSR-pbzc414>.

Libro Blockchain. 2017c. *Las aseguradoras se reinventan con Blockchain - Daniel Díez y Gonzalo Gómez.* [Vídeo en YouTube]. Daniel Díez and Gonzalo Gómez. [Consulta: Septiembre, 2018]. Disponible en: <https://www.youtube.com/watch?v=xjTcCIgBIwQ>.

Libro Blockchain. 2017d. *Carlos Kuchkovsky explica el impacto de Blockchain en la banca.* [Vídeo en YouTube]. Carlos Kuchkovsky. [Consulta: Septiembre, 2018]. Disponible en: <https://www.youtube.com/watch?v=vLBG-lhnRJo>.

Libro Blockchain. 2017e. *El nuevo modelo energético con Blockchain - Ignacio Madrid Benito.* [Vídeo en YouTube]. Ignacio Madrid Benito. [Consulta: Septiembre, 2018]. Disponible en: <https://www.youtube.com/watch?v=bE2XwJmTrxc>.

Libro Blockchain. 2017f. *Smart Contract en Blockchain ¿y es eso legal? - José Ramón Morales Cáceres.* [Vídeo en YouTube]. José Ramón Morales Cáceres. [Consulta: Septiembre, 2018]. Disponible en: <https://www.youtube.com/watch?v=SA0F14EtNdE>.

MEIKLEJOHN, S., Pomarole, M., Jordan, G., et al .2013. A fistful of bitcoins: characterizing payments among men with no names. *Proceedings of the 2013 conference on internet measurement conference,* pp. 127-140. ISSN 9781-450319539. Disponible en: <https://cseweb.ucsd.edu/~smeiklejohn/files/imc13.pdf>.

pasxizeis, chalash, NigelClutterbuck, uptrenda, gabridome, G00dAndPl3nty & wasitrainyyesterday. 2017. *r/Bitcoin - How is the ordering of transactions decided in each block?* En: Reddit. [Consulta: Septiembre, 2018]. Disponible en: <https://www.reddit.com/r/Bitcoin/comments/6rk5ti/how_is_the_ordering_of_transactions_decided_in/>.

PISCINI, E., Guastella, J., Rozman, A. & Nassim, T. 2016. *Blockchain: Democratized trust.* Deloitte Insights. [Consulta: 8 Septiembre, 2018]. Disponible en: <https://www2.deloitte.com/insights/us/en/focus/tech-trends/2016/blockchain-applications-and-trust-in-a-global-economy.html>.

PREUKSCHAT, A., Kuchkovsky, C., Gómez Lardies, G., Díez García, D. & Morelo, Í. 2017. *Blockchain: la revolución industrial de internet.* Barcelona: Gestión 2000.

RODRÍGUEZ, M. 2016. *15 aplicaciones de la tecnología blockchain más allá de bitcoin.* Fintech. [Consulta: 29 Junio, 2018]. Disponible en: <https://www.fin-tech.es/2016/10/aplicaciones-de-la-tecnologia-blockchain.html>.

SCHWAB, K. 2017. *The fourth industrial revolution.* United States of America: Crown Business.

SERRES, T. 2017. *3 use cases of how blockchain technology is already unlocking value.* Animal Ventures. [Consulta: 29 Junio, 2018]. Disponible en: <https://animalventures.com/blog/3-use-cases-of-how-blockchain-technology-is-already-unlocking-value/>.

Stanford Graduate School of Business. 2015. *Susan Athey: The Economics of Bitcoin & Virtual Currency.* [Vídeo en YouTube]. Susan Athey. [Consulta: Septiembre, 2018]. Disponible en: <https://www.youtube.com/watch?v=JhdM4_iRHyE>.

Talks at Google. 2016. *Alex Tapscott: "Blockchain Revolution" | Talks at Google.* [Vídeo en YouTube]. Alex Tapscott. [Consulta: 4 Julio, 2018]. Disponible en: <https://www.youtube.com/watch?v=3PdO7zVqOwc&feature=youtu.be>.

TAPSCOTT, D. 2018. *Why blockchain is dominating discussions in Davos.* The Globe And Mail. [Consulta: 4 Julio, 2018]. Disponible en: <https://www.theglobeandmail.com/report-on-business/rob-commentary/why-blockchain-is-dominating-discussions-in-davos/article37753396/>.

TAPSCOTT, D. 2016. *Davos 2016: Are we ready for the Fourth Industrial Revolution?* The Star. [Consulta: 12 Julio, 2018]. Disponible en: <https://www.thestar.com/news/world/2016/01/18/davos-2016-are-we-ready-for-the-fourth-industrial-revolution.html>.

TAPSCOTT, D. 2015. *SXSW Preview: What's the Next Generation Internet? Surprise: It's all about the Blockchain!* LinkedIn. [Consulta: 4 Julio, 2018]. Disponible en: <https://www.linkedin.com/pulse/whats-next-generation-internet-surprise-its-all-don-tapscott/>.

TAPSCOTT, D. & Tapscott, A. 2017. *Realizing the Potential of Blockchain.* White Paper, World Economic Forum. [Consulta: 9 Julio, 2018]. Disponible en: <http://www3.weforum.org/docs/WEF_Realizing_Potential_Blockchain.pdf>.

TED. 2016. *How the blockchain is changing money and business* | *Don Tapscott.* [Vídeo en YouTube]. Don Tapscott. [Consulta: Junio, 2018]. Disponible en: <https://www.youtube.com/watch?v=Pl8OlkkwRpc>.

TEDx Talks. 2016a. *Blockchain is Eating Wall Street* | *Alex Tapscott* | *TEDxSanFrancisco.* [Vídeo en YouTube]. Alex Tapscott. [Consulta: Julio, 2018]. Disponible en: <https://www.youtube.com/watch?v=WnEYakUxsHU>.

TEDx Talks. 2016b. *How the US government is using blockchain to fight fraud* | *Kathryn Haun* | *TEDxSanFrancisco.* [Vídeo en YouTube]. Kathryn Haun. [Consulta: Julio, 2018]. Disponible en: <https://www.youtube.com/watch?v=507wn9VcSAE>.

The Economist. 2015. *The great chain of being sure about things.* ECONOMIST. [Consulta: 5 Julio, 2018]. Disponible en: <https://www.economist.com/briefing/2015/10/31/the-great-chain-of-being-sure-about-things>.

WRIGHT, J. 2016. *Nosedive.* [Episodio de la serie original Black Mirror en Netflix].

YABO, A. 2018. *Smart Contract Audits: The Ultimate Security Guide.* En: CoinFabrik Blog. [Consulta: 14 Septiembre, 2018]. Disponible en: <https://blog.coinfabrik.com/smart-contract-audits-ultimate-security-guide/>.