FACULTAD DE CIENCIAS ECONÓMICAS Y EMPRESARIALES

BLOCKCHAIN, “LA NUEVA REVOLUCIÓN INDUSTRIAL”

Autor: Miguel Alvarez de Linera Alperi
Director: Laura Fernández Méndez

Madrid

Abril 2018

Miguel
Alvarez de Linera
Alperi

BLOCKCHAIN, LA "NUEVA REVOLUCIÓN INDUSTRIAL

Blockchain, la "nueva revolución industrial"

Miguel Álvarez de Linera Alperi
Universidad Pontificia de Comillas (ICADE)

RESUMEN. Blockchain, o cadena de bloques, es un término que se ha popularizado a escala mundial durante el último año 2017. Debido al interés de la gente por profundizar en el tema y al mío propio por aprender y hacer entender a la gente el poder disruptivo de la tecnología, he decidido estudiar el blockchain en profundidad en el trabajo, yendo desde los conceptos más simples de la tecnología hasta los ámbitos más concretos y específicos. El blockchain ya no es un tema reservado a técnicos y profesionales de la tecnología, sino que cada día más es un término que todos deberíamos conocer y entender.

Mediante este TFG pretendo dar una explicación sencilla y consistente de la tecnología, pero también hacer ver que la implementación de la tecnología ya no es una quimera, si no cada vez más, una realidad muy próxima. A lo largo del TFG, aparte de las cuestiones teóricas, expondré diversos ejemplos, aplicaciones y futuras posibilidades y oportunidades que puede brindar esta tecnología.

Siguiendo la misma línea que lo dispuesto anteriormente, a lo largo del TFG trataré de hacer un estudio progresivo de la tecnología, yendo desde los aspectos más básicos, como son el desarrollo teórico de la tecnología hasta los más complejos como son la posible evolución futura del blockchain, la aplicabilidad de la tecnología en el sistema financiero, los problemas de escalabilidad de las redes de blockchain y las alternativas a esta tecnología que ya están empezando a ser desarrolladas.

Este trabajo permitirá obtener al lector una visión global sobre la tecnología y las aplicaciones futuras que se pueden esperar de esta.

🔑 Blockchain, nuevas tecnologías, innovación, movimiento social, disrupción, criptografía, descentralización, smart contract, ICO.

Blockchain, la "nueva revolución industrial"

Miguel Álvarez de Linera Alperi
Universidad Pontificia de Comillas (ICADE)

ABSTRACT. Blockchain is a term that has become popular worldwide during the last year 2017. Due to the interest of people to delve into the subject and my own to learn and make people understand the disruptive power of technology, I decided to study the blockchain in depth, going from the simplest concepts about the technology to the most specific areas. Blockchain is no longer reserved for technicians and technology professionals, but is has become a term that we should all know and understand.

Through this TFG I intend to give a simple and consistent explanation of the technology, but also to show that the implementation of the technology is no longer a chimera, but increasingly, a very close reality. Throughout the TFG, apart from the theoretical issues, I will expose several examples, applications and future possibilities and opportunities that this technology can offer.

Following the same line as previously stated, throughout the TFG I will try to make a progressive approach to the technology, going from the most basic aspects, such as the theoretical development of technology to the most complex, such as the possible future evolution of the technology. blockchain, the applicability of technology in the financial system, the scalability problems of blockchain networks and the alternatives to this technology that are already beginning to be developed.

This work will provide the reader with a global vision of the technology and future applications that can be expected from it.

🔑 Blockchain, new technologies, innovation, social movement, disruption, cryptography, decentralization, smart contract, ICO.

Índice

Tabla de ilustraciones y tablas

1- Introducción. El origen y nacimiento del Blockchain.

Si bien es verdad que el blockchain como tecnología se puede decir que nació en el año 2008 de la mano del whitepaper de Bitcoin ideado por Satoshi Nakamoto (Mazzei, 2017), también hay que destacar que para llegar hasta este punto tuvo una muy importante relevancia el grupo de activistas Cypherpunk (Barlett, 2016). Este era un grupo de desarrolladores libres que, a partir de los años 80, empiezan a promover la encriptación de documentos y tecnologías que favorezcan la privacidad con el objetivo de que los estados perdieran poder y que esto provocara un cambio en la vida pública y en la política (Loop, 2016).

Este movimiento continúa durante los siguientes 30 años, creciendo cada vez más y más la comunidad. Existían ciertos grupos de desarrolladores, cada grupo especializado en un sector o especialidad diferente.

Muchos autores por lo tanto consideran el 2008 como año de nacimiento de la tecnología blockchain, ya que este fue el año en el que el desarrollador o grupo de desarrolladores conocido como Satoshi Nakamoto publicaron el whitepaper de Bitcoin. Si bien profundizaremos posteriormente en el tema podemos adelantar que la tecnología que hace funcionar el Bitcoin y le da coherencia y utilidad es lo que se conoce como blockchain. Podríamos definir brevemente blockchain como el motor de Bitcoin.
Es a partir de este momento del lanzamiento del whitepaper y durante los siguientes años en los que se empieza a vislumbrar lo que de verdad puede suponer el uso de la tecnología blockchain para el mundo (Hodge, 2017). El código de Bitcoin es un código abierto, lo que permitió que la tecnología se expandiera con mucha mayor rapidez y también que nacieran una gran cantidad de proyectos basados en tecnología blockchain. El desarrollo a partir de este momento es imparable y queda reflejado en la evolución del precio del Bitcoin que se puede apreciar en el siguiente gráfico (Ciaian, Rajcaniova, Kancs, 2016).

En las Figuras 1 y 2 vemos la evolución del precio del Bitcoin paralelamente con la capitalización bursátil. Se puede apreciar que la evolución del precio es exponencial sobre todo a partir del año 2017, año en que se populariza a nivel mundial el término,

llegando a sobrepasar incluso los 18.000 dólares por Bitcoin y más de 300 billones de dólares de "capitalización bursátil."

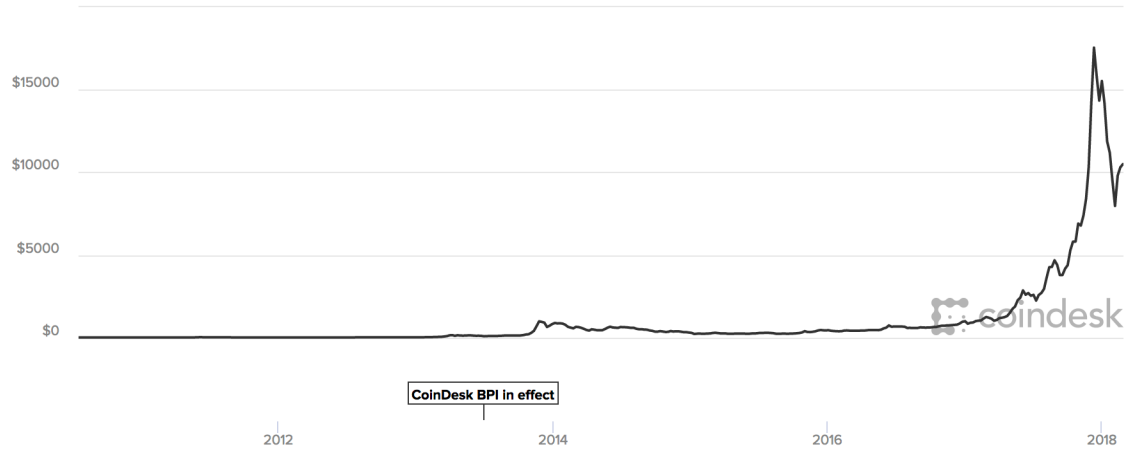

Figura 1. Evolución del precio del Bitcoin, 2008-2018. Recuperado de Cuen, L., Hochstein, M., Godbole, O. and Zhao, W. (2018). *Bitcoin Price Index - Real-time Bitcoin Price Charts*. CoinDesk. Available at: https://www.coindesk.com/price/

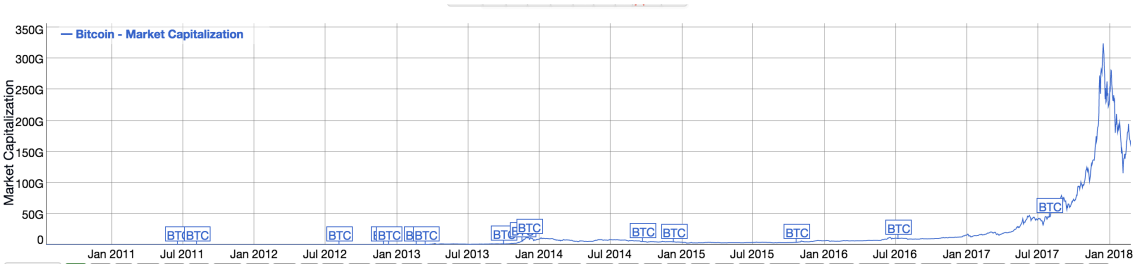

Figura 2. Evolución de la capitalización bursátil del Bitcoin 2008-2018. Recuperado de Bitinfocharts (2018). *Bitcoin Market Capitalization chart*. Bitinfocharts.com. Available at: https://bitinfocharts.com/comparison/bitcoin-marketcap.html

Satoshi Nakamoto se refería a blockchain de manera separada como block y chain, y no es hasta 2016 cuando se populariza el concepto conjunto de blockchain gracias a un artículo de The Economist en el que se habla ya de la blockchain 2.0, o como la implementación de los smart contracts en las blockchains iba a revolucionar los sistemas de pagos, otro de los aspectos que cubriremos en profundidad en este TFG.

Desde entonces, ya no solo se considera la importancia que puede tener el Bitcoin como instrumento de inversión y de valor al margen de la regulación central, sino que

también se empieza a estudiar y tratar la tecnología detrás de este curioso instrumento cómo herramienta de gestión y optimización.

Ejemplos de esta expansión a partir del año 2016 son la reunión del *World Economic Forum* en noviembre de 2016 para crear un laboratorio de investigación Blockchain (Coindesk, 2016), la creación del proyecto Nxt para investigar sistemas de votación a través de Blockchain de por la Comisión de Valores Rusa (NSD) (Nxtplatform, 2016) o la apertura de un centro de innovación e investigación en Blockchain en Singapur por la multinacional IBM (IBM).

Si bien es verdad que blockchain no es el primer sistema de DTL (Distributed Ledger Technology) o sistema de información distribuida, este es el técnicamente más desarrollado y seguro hasta la fecha, y por lo tanto, el que más posibilidades tiene de implementarse en la sociedad en el corto medio plazo.

La influencia de estas nuevas tecnologías ya no se ve solo en la increíble apreciación del Bitcoin en los últimos 10 años, (Coindesk, 2018) sino también en la cantidad de nuevos proyectos y aplicaciones que están saliendo al mercado basados en tecnologías blockchain. Más de 1000 cryptodivisas distintas (Cryptocompare, 2018) cada una con su protocolo particular, más de 800 billones de dólares invertidos en mercados de cryptoactivos e ICOs (Initial Coin Offerings) que llegan hasta el billón de dólares en preICO avalan que este tema ya no está solo reservado a los ingenieros informáticos, sino que se ha convertido en un tema por el que cada vez más individuos, profesionales, empresas multinacionales y países empiezan a preocuparse.

2- Estado de la cuestión

Al ser un tema tan novedoso, el análisis se hará paso por paso, cubriendo cada uno de los puntos que confieren al blockchain de sus características únicas, por ello en este apartado se tratarán: (a) Características esenciales del blockchain; (b) Tipos de Blockchain y por qué esto es importante, (c) La seguridad en las redes descentralizadas materializado en la resolución del problema del Bizantine Fault Tolerance y por último, (d) Sistemas de consenso y minación.

Por último, e innegable y directamente relacionado con el blockchain, incluyo un breve análisis de los smart contracts, qué son, que suponen para la revolución del blockchain y en qué estado de desarrollo se encuentran a día de hoy.

a) ¿Qué es el blockchain?

Blockchain se puede traducir directamente al castellano como **"cadena de bloques"** y es efectivamente eso una cadena en la que se enlazan bloques de información. Visto así no parece que se produzca ninguna innovación, pero esta cadena de información tiene unas características particulares. Hablando en palabras coloquiales, la definición más exacta que existe es que el blockchain es un "registro público" o *public ledger*, pero como decíamos antes, con una serie de características que hacen a esta tecnología única y disruptiva (Deloitte, 2017):

- **Es completamente transparente y público:** toda la cadena de bloques se descarga en cada uno de los nodos de la red. Por nodo tenemos que entender ordenador o CPU que se encarga de validar las transacciones en blockchain. Más adelante avanzaremos con los tipos de blockchain que existen y como se ejecuta la validación de cada bloque, ya que cada red puede tener métodos distintos.
- **Auditoría:** es importante remarcar que el hecho de que todas las transacciones queden registradas implica que los sistemas de auditoría van a convertirse en sistemas mucho más eficientes y seguros tanto para el inversor como para el regulador que tiene que controlar la actividad de las empresas.
- **Velocidad de las transacciones:** si bien es cierto que todavía queda mucho por mejorar en este aspecto, la tecnología blockchain acabará provocando que las transacciones se realicen en segundos. A día de hoy el Bitcoin es el protocolo que más lento ejecuta el proceso de generación de bloques ya que tarda entre 10-15 minutos, Ethereum por su parte consigue reducir este tiempo a 4 minutos y ya hay proyectos como Universia que están planteando recortar este tiempo hasta ser capaces de procesar 25.000 transacciones por segundo. (Universia, 2017). Empresas como Visa son capaces de procesar 50.000 transacciones por

segundo, pero los sistemas de back office que implementan no tienen tanto recorrido como pueden tener las tecnologías derivadas del blockchain.

- **Es inmutable:** el hecho de que en todos los nodos se encuentre todo el registro de la blockchain provoca que los bloques previos no se puedan modificar ya que este cambio se notificaría en todos los nodos y se podría revertir el fallo. La red de información es completamente segura.
- **Seguridad:** por lo que hemos dicho previamente y además por la característica de que todas las claves están criptografiadas, de tal manera que tenemos una clave pública y una clave privada. La clave pública es con la que nos puede reconocer la gente o el mercado, pero a menos que la compartamos la gente no tiene acceso a nuestra información. Esta privacidad lleva a que se acuse al blockchain de favorecer el lavado de dinero negro. Si bien esto es cierto en cierta parte, más adelante profundizaremos en el tema para ver como se está peleando contra este fenómeno sin por ello dejar de aprovechar las buenas cosas que puede aportar esta tecnología.
- **Irreversibilidad:** Todas las transacciones que ocurren en la blockchain no se pueden revertir. Esto está ligado con la parte de inmutabilidad.
- **Descentralización:** este es el factor más importante como concepto. En un mundo centralizado como el que vivimos, el concepto de la descentralización nos asusta y, sobre todo, asusta a los gobiernos. En una sociedad descentralizada los organismos centrales pierden protagonismo. Tanto a nivel corporativo como a nivel administrativo, los gigantes del mercado van a tener que adaptarse a esta nueva idea de sociedad. Ejemplos de esto son Alastria, Santander, UBS, JP Morgan… Tanto los estados como las empresas quieren ponerse al día con esta tecnología.

  El carácter de descentralización queda reflejado en el hecho de que gracias a esta tecnología dos individuos que no se conocen de nada y que obviamente no confían uno en el otro pueden ponerse de acuerdo y cerrar transacciones sin tener que depender de una entidad central en la que confiar. Aquí radica el verdadero valor

Es importante empezar a familiarizarnos con esta tecnología, ya que según una encuesta realizada por el World Economic Forum en 2015 el 57,6% de los encuestados llegaron a

la conclusión de que al menos el 10% de la información concerniente al PIB mundial iba a estar almacenada en sistemas de blockchain para el año 2025. En la encuesta se preguntó a 800 ejecutivos y expertos informáticos cuál pensaban que sería el impacto de la tecnología blockchain en 10 años.

Por poner un ejemplo en términos monetarios, de acuerdo con el investigador Markets and Markets, el valor de los productos y servicios relacionados ascenderá a 7,7 billones de dólares para 2022. Durante el año pasado el valor de estos servicios ascendió hasta los 242 millones de dólares.

Gigantes como VISA, IBM, Google, Goldman Sachs y muchos otros de muy diferentes sectores están empezando a invertir en esta tecnología, ya no solo por razones de ahorro en costes, sino también por razones de crecimiento empresarial y de mejora de la eficiencia de los sistemas actuales. Según un estudio realizado por PwC en el año 2017, sobre tres cuartos de todas las instituciones financieras del mundo habrán adoptado sistemas blockchain como parte de sus procedimientos internos y de producción para el año 2020. (Del Río, 2017)

Por todo esto, el blockchain se ha llegado a calificar como **el invento más disruptivo desde la creación de internet** debido a sus múltiples aplicaciones no únicamente en ámbito financiero, si no también en muchos otros campos desde la medicina hasta la agricultura o el deporte (Hiesboeck, 2017).

b) Tipos de blockchains

- **Públicas**: Una blockchain pública puede describirse como un registro público en el que toda persona tiene acceso a la red tanto para leer y descargarse el *public ledger* o registro de transacciones, como también para convertirse en un nodo y empezar a minar y validar la red. El Bitcoin es el mayor exponente dentro de este tipo de red pero también existen otras blockchain públicas muy importantes como Ethereum o Z-Cash. (Blockchain España, 2017). Las redes públicas también se conocen como *permisionless* o redes que no necesitan permiso para

accederse en castellano. En estas, el número de usuarios está pensado para que sean millones, es decir, cuanta más gente se una, mejor.

- **Privadas**: son aquellas que tanto el proceso de validación como el proceso de minado y vista y descargado del *ledger* están controlados por una entidad central. Esto rompe con el principio de la descentralización, pero es cierto que en ciertas plataformas, el hecho de que la red sea privada es imprescindible para el correcto uso de la plataforma o del servicio que pretenden ofrecer (Fisher-Phillips, 2018). El ejemplo más conocido de blockchain privada es el de Ripple, un proveedor de servicios ágiles de pago. Las blockchains privadas también se conocen como *permissioned* o permisionadas. Para poder acceder a este tipo de redes se requiere consentimiento expreso de aquellos que están en control de la blockchain. Otros ejemplos son R3 o Hyperledger (Blockchain España). Estas, como se puede ver por la descripción del tipo de red, están pensadas para que el número de usuarios de la plataforma sean muy pocos, nunca llegando a perderse el control sobre todos los usuarios validadores (Coinsutra).

- **Semiprivadas**: Son aquellas que son permisionadas, pero con unos criterios más flexibles que las privadas. Se les conoce como *public permissioned* y son aquellas que funcionan como un club, es decir, si cumples ciertos requisitos puedes entrar. (Fisher - Phillips, 2018) En ciertos casos, también las redes semiprivadas de blockchain lo que dan a sus usuarios es acceso a ver las transacciones que ocurren en la blockchain pero no a la validación y generación de bloques. En palabras de William Mougayar autor de The Business Blockchain: "las blockchain semi-privadas serán similares a las páginas web privadas en términos de cómo están gestionadas. Tan pronto como los usuarios se acrediten en relación a unos criterios pre-especificados, se les dará acceso. No debería de haber discriminación para el acceso (…) En contraste con blockchains públicas donde todo el mundo puede participar, y en blockchains privada s donde la participación está fuertemente sujeta, las blockchains semiprivadas están gestionadas por una sola compañía que permite el acceso a aquél usuario que cumpla con los requisitos demandados por la plataforma". (The Business Blockchain)

Algunos ejemplos de redes semiprivadas de blockchain son las que utilizan las empresas Evernym o Blockchain DB.

El objetivo de las blockchains semiprivadas es que haya un número grande de usuarios pero que la plataforma siga manteniendo cierto control a la hora de permitir el acceso a la plataforma.

La **figura 3** resume los distintos requisitos y características de cada una de las diferentes blockchains:

Tipo ->	Publica	Privada	Semi - privada
Acceso	No necesita permiso	Solo miembros, que podrían ser los cofundadores	Usuarios cualificados a través de aprobaciones online
Implementación habitual	Como una aplicación pública c	A través de una implementación de blockchain privada	One compañía lanza el producto y adquiere usuarios progresivamente
Objetivo de innovación	Nuevos modelos de negocio	Procesos con relaciones existentes	Sirve para apoyar modelos de negocio actuales o para lanzar nuevos servicios
Poder dentro de la Blockchain	Consenso público	Peso igualitario a todos los participantes	Controlada por un único propietario
Número de usuarios	Millones	Desde docenas hasta cientos	Cientos de miles

***Figura 3*.** Blockchains públicas, privadas y semiprivadas. Recuperado de Medium. (2018). *Understanding Semi-private Blockchain Applications – William Mougayar – Medium*. Recuperado de: https://medium.com/@wmougayar/understanding-semi-private-blockchain-applications-6bbe91fc3596

Pero, ¿Qué convierte al blockchain en un sistema válido frente a otros sistemas previos qué también partían de la idea de la descentralización? Para poder entender mejor el sistema tenemos que ir a la raíz del problema, la razón por la que hasta el día de hoy los sistemas descentralizados no habían funcionado y la razón de por qué el blockchain es la solución. El problema originario de las redes descentralizadas sé conoce en el lenguaje informático cómo BFT o Bizantine Fault Tolerance.

c) Bizantine Fault Tolerance (BFT) y el problema inherente de seguridad en las redes descentralizadas

Bizantine Fault Tolerance o BFT es el sistema que permite que sistemas distribuidos solucionen el problema de los Generales Bizantinos. ¿Pero qué es esto y que tiene que ver con sistemas informáticos?

El problema de los generales bizantinos es un problema ideado por los investigadores Leslie Lamport, Robert Shostak and Marshall Pease en el año 1982. Estos describían el problema de dos generales bizantinos que quieren atacar una muralla al mismo tiempo, pero en medio de sus comunicaciones hay un intermediario, que puede ser o no un traidor. Eso provoca que no exista confianza en la red ya que la transmisión de la información está centralizada en el intermediario que puede o no ser el traidor.

Este problema es solucionado por los sistemas de información distribuida. Cuando el consenso no es dado por una entidad central sino por una serie de nodos interconectados donde la información está presente en todos ellos, este problema se elimina, y ya no existe la posibilidad de que alguna de las partes mande información falsa ya que toda la información es pública para todos los usuarios de la red y todos tienen acceso a ella al mismo tiempo. Esto unido a los sistemas de validación y creación de bloques crea un sistema que elimina por completo este problema y preocupación.

Estas tecnologías son las que se utilizan para los sistemas blockchain, y junto a la teoría del doble gasto, solucionar el BFT era uno de los objetivos principales a la hora de desarrollar el protocolo Bitcoin original.

Para que los sistemas descentralizados pudieran ser eficientes, sé necesitaba que este problema fuera resuelto y no fue hasta la aparición del protocolo de Bitcoin y de la introducción de los sistemas de consenso y minación cuando encontramos una solución eficiente a este problema.

d) La solución al BFT. Sistemas de consenso y minación.

Minación en el sentido tradicional de la palabra significa extraer un cierto material o mineral de una excavación en la tierra, pues bien, en este caso el concepto es similar pero aplicado a las nuevas tecnologías, pasemos a la explicación. En los sistemas tradicionales monetarios las entidades centrales son aquellas que tenían el control para imprimir más o menos dinero en función de lo que estos considerasen y en función de las necesidades de la economía. Este sistema con el Bitcoin desaparece ya que las monedas no se crean, sino que se descubren (bit2me, 2017). El descubrimiento se hace a través de una competición entre ordenadores que permite dar seguridad a la red. Los ordenadores o nodos deciden competir entre ellos porque contribuyendo a la red obtienen ciertas recompensas. Por ejemplo, en los primeros años de Bitcoin la recompensa por minar un bloque era de 50 bitcoins por bloque generado (Draupnir, 2016) Esto lo que se conoce como la descentralización del consenso y permite que partes que no se conocen cooperen entre sí.

Básicamente, entonces para lo que sirven los sistemas de minado es para confirmar las transacciones y escribirlas en el registro o "libro mayor", es decir, el blockchain. Por muchas transacciones que yo realice esto no valdría de nada si no queda registrado en la blockchain. Este tipo de sistemas solo son válidos cuando existe un gran número de participantes que valida la red ya que sino el sistema se vuelve imparcial e incluso hasta corrupto ya que podría ocurrir el caso en el que ciertos participantes de la red puedan tomar el control de la blockchain. Cuanto más descentralizado es el sistema, más eficiente será el mismo.

Dentro de los sistemas de validación que encontramos en los diferentes protocolos, los más conocidos e importantes son:

- **Proof of Work (PoW):** ciertas redes como Bitcoin para permitir ser minero y por lo tanto validador de la red, te piden que mines a través de este sistema. PoW es simplemente un algoritmo que a medida que vas resolviendo, se va volviendo más complejo, lo que cada vez va requiriendo más y más poder computacional. Para poder minar con este sistema necesitas tener un ordenador potente y tarjetas gráficas que te permitan ir decodificando el algoritmo.

PoW fue el primer sistema que se inventó, pero al crearlo no se pensó en que era difícilmente escalable. A día de hoy el número de mineros aumenta por días y esto provoca que cada vez sea mayor, y continúe creciendo, el consumo de electricidad. Para solucionar estos problemas se está empezando a desarrollar lo que conocemos a día de hoy como PoS.

- **Proof of Stake (PoS):** como decíamos previamente el PoS nació con el objetivo de solucionar el problema energético causado por su predecesor, el PoW. Los sistemas de PoS solucionan este problema ya que aquí no tienes que utilizar energía para solucionar el algoritmo, sino que minas o "creas" bloques proporcionalmente en función al número de participaciones en la red que tengas. BuzzCoin es una red que opera de este modo, y a mayor número de monedas que posees, mayor es el número de bloques que contribuyes a genera, y por lo tanto mayor el "stake" que te llevas por ayudar a esa generación. El protocolo da más facilidad para resolver bloques a aquellos que más participación tengan en la moneda, suponiendo de esta manera que aquellos que más monedas posean serán los que más interés pongan en proteger y asegurar la supervivencia de esta (Momoh, 2018)

- **Otros**: hay en otras ocasiones en las que nos encontramos redes preminadas en las que el propio equipo es el que se ocupa de validar los bloques, sin dar ningún tipo de *reward* o premio por ello. Un ejemplo de esto sería Ripple, con su divisa XRP. (Ripple)

e) Smart contracts

Una vez tratado el tema de que es el blockchain, para continuar con el trabajo es importante distinguir el concepto de un smart contract. El blockchain es un sistema disruptivo en sí mismo, pero es unido a los smart contracts cuando de verdad está revolución se extiende a todos los sectores.

Según la descripción del abogado e investigador de Uría Menéndez Miguel Stokes, un smart contract podría definirse como "códigos informáticos utilizados para monitorizar y ejecutar términos contractuales sin interferencia humana." A día de hoy este concepto

está de moda debido a la aplicabilidad que estos tienen una vez que lo implementas en una red de blockchain.

3- Metodología

La metodología del trabajo se basará en un análisis descriptivo cualitativo de la tecnología blockchain. Para ello se han utilizado fuentes secundarias provenientes fundamentalmente de trabajos académicos, de informes de bancos, informes de consultoría, estudios realizados por empresas de investigación y páginas web especializadas en la tecnología como son Reddit, Blockchain Council o Blockgeeks. El análisis descriptivo se complementa con una gran cantidad de ejemplos de cómo se está implementando la tecnología y también teorías y posibilidades que pueden tener lugar en el futuro gracias a la implementación del blockchain.

El hecho de que el tema sea tan novedoso implica que todavía queda mucho por desarrollar y que por lo tanto muchas cosas no se puedan afirmar con una rotundidad absoluta. Eso también es una oportunidad para aprender para el lector ya que muchas de las teorías sobre la futura implementación y desarrollo del blockchain están también recogidas en este trabajo.

Como se acaba de comentar se trata de un trabajo de naturaleza descriptiva que trata de sintetizar lo que conocemos hasta ahora sobre un novedoso concepto del que aún no existen muchos trabajos académicos y del que aún queda mucho por investigar.

A continuación, pasaremos a analizar los siguientes aspectos de la tecnología desde una perspectiva teórica: (a) Origen y aplicaciones de los smart contracts, (b) La relación entre Blockchain, inteligencia artificial, IOT y redes sociales, (c) La revolución del sistema bancario y financiero internacional, (d) El problema de la escalabilidad de las redes Blockchain, (e) Nuevos sistemas alternativos al Blockchain: Hashgraph y Tangle.

4- Origen y aplicaciones de los Smart contracts

Antes de empezar con el concepto de Smart contract es importante recordar que un contrato se definir en palabras de la Real Academia Española cómo un "Pacto o convenio, oral o escrito, entre partes que se obligan sobre materia o cosa determinada, y a cuyo cumplimiento pueden ser compelidas." (RAE). Como bien dice la definición, para que un contrato tenga validez tiene que estar en formato digital o escrito y en muchas ocasiones además se necesita la participación de un notario, es decir, un proceso costoso y complejo. Además, una vez que existe controversia respecto a alguno de los términos del contrato la solución no es inmediata, sino que normalmente hay que pasar por largos y arduos procesos en los juzgados en los que todos los términos del contrato pueden estar sujetos a cierto tipo o grado de interpretación (Uría – Menéndez, 2017).

Los primeros contratos inteligentes nacen en el año 1997 de la mano del jurista y criptógrafo Nick Szabo. El concepto de Smart contract fue concebido en el mismo año en un trabajo conocido como "Formalizing and Securing Relationships on Public Networks". El concepto se hizo conocido debido a la disrupción que podría provocar en el futuro, sin embargo, no es hasta 2009 con el nacimiento del Bitcoin, y sobre todo del Blockchain, cuando verdaderamente se empieza a ver la aplicabilidad de este novedoso concepto (Gord, 2016).

Gracias a la implementación de los Smart contracts estos problemas desaparecen ya que la ejecución de los términos de un contrato se realiza de manera automática y como bien reza la definición de Stokes no es necesaria intervención humana. Por otra parte, como todos los términos están escritos en un código o *script* se eliminan los problemas de interpretación de las partes.

Al mezclar los contratos inteligentes con las plataformas de blockchain creamos un sistema único en el que, como toda la información sobre el Smart contract es pública y está registrada en la blockchain, la validez de los términos contractuales se puede asegurar tanto si las partes son personas físicas, como jurídicas, como máquinas autónomas (Mik, 2017).

Hasta el día de hoy no era posible el hecho de que dos instrumentos o máquinas autónomas contrataran entre sí, pero ahora vamos viendo que el concepto de los Smart contracts, junto con el blockchain y la tecnología conocida como IOT (*internet of*

things) está dilucidando un futuro en el que esto puede ser posible. Una de las empresas pioneras entre tipo de sistema de tres vértices es IOTA, de la que posteriormente hablaremos de su sistema particular de validación, pero que básicamente lo que pretende es llevar el IOT al siguiente nivel, creando una plataforma única que permita, por ejemplo, que un coche contrate de manera autónoma el pago de la zona azul cuando lo aparcas o que una nevera te haga la compra por ti. (IOTA)

IOT es uno de los ejemplos, pero son muchos los sectores en los que se va a poder aplicar este tipo de sistemas, desde los mercados financieros, sector inmobiliario, se seguros, de sanidad, de distribución… etc. Las aplicaciones son infinitas.

Llevando el concepto de la ejecución automática más allá, el paso siguiente será conectar 4 de los mayores avances tecnológicos actuales de la humanidad que son el blockchain o los sistemas de registro distribuido, la inteligencia artificial, el *internet of things* y las redes sociales. ¿Pero, cuál es la relación real entre todas estas? Ese será el próximo punto a tratar después del análisis de la metodología que se llevará a cabo en el trabajo.

5- La relación entre blockchain, inteligencia artificial, IOT y redes sociales.

Las próximas líneas del trabajo se basan en el estudio que llevo haciendo a lo largo del último año sobre nuevas tecnologías, y, sobre todo, en el cambio que puede suponer una efectiva implementación de estas. Hay muchos proyectos que sirven o están dirigidos en el corto-medio plazo a hacer dinero, pero hay muy pocos que en el largo plazo se planteen cambiar o mejorar la humanidad. Este es uno de los del segundo grupo, pero para que se cumpla se necesita:

1- cooperación de los estados
2- solidaridad de las corporaciones
3- comprensión, flexibilidad de adaptación y entusiasmo por parte del público en general

A día de hoy cuando utilizamos redes sociales como Facebook, Instagram o Whatsapp estamos entregando datos a los propietarios de las plataformas a cambio de un servicio.

Si bien es cierto que el servicio es gratuito también lo es la información que se entrega a cambio para ellos, y, a pesar de lo que el público en general puede pensar, nuestra información tiene mucho más valor que el coste de la plataforma, por eso para estas compañías es un negocio muy rentable. Solo en la Unión Europea las empresas de información proveen más de 10 millones de empleos y suponen un 4% del PIB total de la región que en valor monetario supone unos 60.000 millones de euros anualmente (Urrutia, 2018).

Ahora pónganse en el caso de que pudiéramos cambiar esta información por valor, que al particular le pagaran por simplemente utilizar las redes sociales, ahí está la verdadera revolución. Esto es solo un párrafo introductorio, pero quiero que piensen en esta idea. Pongamos cuatro puntos, el blockchain, las redes sociales, IOT y la inteligencia artificial.

¿Cuál es la idea?

El ser humano tiene valor en sí mismo por su capacidad racional, que es la frontera a la que aún no han llegado las máquinas y robots. Al final el paradigma de la inteligencia humana se basa en la recopilación de comportamientos aleatorios e irracionales que nos permitan llegar a que una máquina pueda razonar como un humano, pero de la misma manera ser completamente irracional justificándose en una supuesta razón. Los humanos podemos enfadarnos sin sentido, actuar por impulsos, reír sin motivo… y eso no son comportamientos racionales, sino que son comportamientos irracionales derivados de la propia racionalidad.

Pongámonos en el caso. Si una empresa X le propone a un sujeto tener acceso a sus redes sociales de forma anónima a cambio de una cantidad de dinero fija al mes, probablemente este diría que sé. El sujeto en cuestión mantendría su anonimato en todo momento, pero la empresa podría estudiar sus patrones de comportamiento y la manera en la que ejecuta sus relaciones personales. Si todos los perfiles están criptografiados, el particular no corre riesgo de ser identificado, y a cambio lo que el particular recibe es dinero por su información. El resultado es que el sujeto en cuestión por seguir haciendo lo que hace, ahora además pasa a cobrar una cantidad determinada de dinero al mes. Esta información quedaría registrada en una blockchain y posteriormente se transmitiría a los ordenadores.

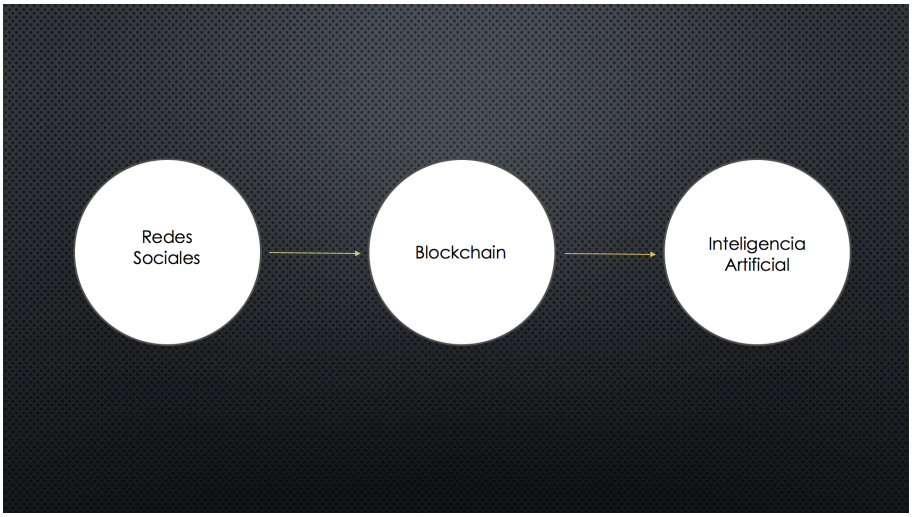

Figura 4. Explicación gráfica de cómo funcionaría el proceso de transferencia de información entre las distintas plataformas. Creación propia

Lo que conllevaría esto es, básicamente, que al rastrear la información y mensajes que una persona envía a sus contactos podemos estudiar. Recopilar, compartimentar y entender la irracionalidad del hombre. Podremos introducir en una computadora como un niño se enoja con su madre, los patrones de comportamiento de dos jóvenes hablando del día a día, como terminar una relación sentimental, como se comporta un sujeto ebrio… y todo esto asociarlo con distintas situaciones e ir creando compartimentos de información que permitan a una computadora generar sus propias conclusiones y, sobre todo, sus propios patrones de comportamiento. En el momento en que esto ocurra el valor del trabajo del ser humano desaparece, y solo serán útiles y necesarios aquellos trabajos especialmente técnicos, creativos, de asesoría o de pura dirección.

Asimismo, esto no conllevaría la extinción de la humanidad, sino que simplemente la gente contaría con un salario mínimo o el conocido como "salario universal" y podría dedicar su tiempo a producir o crear otro tipo de instrumentos e ideas que no desarrollen las máquinas. El ser humano podrá dedicar íntegramente su vida a sí mismo y su creatividad.

Si bien esto simplemente es una breve introducción a la idea, mi propósito es desarrollarlo a lo largo de los próximos años en profundidad.

A día de hoy no podemos predecir con exactitud cuál sería el coste de proveer de

energía durante todo el día a una máquina, pero lo que si podemos prever es que el coste es infinitamente menor al de tener un trabajador a sueldo. Esto abarataría enormemente los sistemas de producción y permitiría reinvertir los excesos del capital generado en garantizar un salario universal.

Todo este estudio conllevaría un análisis no solo tecnológico, sino también moral, social, filosófico y político ya que se cambia el concepto que se tiene de la humanidad, se modificarían las estructuras sociales y dependiendo de la profundidad con la que se aborde el tema se podría acabar por erradicar el eterno problema del hambre y la escasez en el mundo. A través de sistemas automatizados el hombre podría dejar de tener que trabajar y podría empezar a trabajar únicamente por placer y propia realización.

¿Cómo funcionaría el sistema?

El sistema habría que implementarlo a través de la creación de una empresa que opere una blockchain semiprivada (para más explicación sobre una blockchain semiprivada ir al punto 3). Las redes sociales mandarían datos, que quedarían registrados en la blockchain, los bloques se validarían y esta información se procesaría y se transmitiría a inteligencias artificiales, que a largo plazo lo que esperamos es que se empiecen a comportar con la misma racionalidad e irracionalidad de seres humanos. Esto mismo lo que nos permitirá en un futuro es que estas puedan sustituir al hombre en las tareas más automáticas.

La consecuencia directa de la implementación de este sistema es que gracias al trabajo producido se podrá generar una renta básica a todas las personas, de tal manera que solo aquellas que puedan y quieran trabajarán. Los puestos de trabajo se reducirán a creativos, jefes de estado y puestos de ingeniería y asesoría. El paradigma de la humanidad. La gente en una primera fase cobrará por ceder su información y en un segundo punto porque el sistema será tan eficiente que permitirá que las máquinas generen rendimientos suficientes para crear lo que se conoce como “salario universal” que permita que la gente trabaje única y exclusivamente por autorrealización personal.

Es importante a la hora de realizar el análisis destacar las empresas que a día de hoy están haciendo cosas parecidas en el mundo blockchain. Dentro de estas y como proyectos más prometedores tenemos:

SteemIt: con más de medio millón de usuarios es el proyecto más prometedor a día de hoy en el mundo del blockchain con redes sociales. (Sayapina, 2017) Según el whitepaper de la compañía esta se describe a sí misma como "An incentivized, blockchain-based, public content platform" o, en otras palabras, una plataforma incentivada, basada en blockchain y de contenido público (Steem).

La particularidad de Steem con respecto a otros proyectos es que los autores en la plataforma reciben tokens por valorar, generar y votar contenido. Es algo así como un Médium, pero más eficiente ya que el hecho de que la gente cobre por elaborar contenido de calidad hace que la plataforma se vuelva más eficiente y sobre todo, más interesante y atractiva al público.

Matchpool: con un sistema de *matching* descentralizado, la plataforma pretende que su algoritmo genere grupos de gente con los mismos intereses. En este caso, y como todos los proyectos basados en la descentralización, pretende dar a los usuarios una herramienta para monetizar el uso de la plataforma. En esta plataforma, la finalidad es otra y lo que se pretende es dar puntos de conexión a las personas, de tal manera que se vaya generando una confianza en el mercado que sirva como verdadero instrumento de valor en el futuro.

Golos: proyecto similar a Steem, pero con fundadores rusos.

SocialX: Este proyecto por ejemplo te da la posibilidad de poder ceder los derechos de uso de tus fotos o utilizarla como una red al uso. Como otros proyectos, también este nos permite disponer de una wallet y crear y validar contenido de tal manera que monetizamos nuestra actividad.

E-chat: pensado como una plataforma de mensajería descentralizada. El cometido de esta plataforma ya no es solo que se permitan mandar mensajes como ocurre con otras aplicaciones como Whatsapp o Telegram, sino también que la plataforma te permita almacenar monedas en tu wallet o efectuar pagos en cryptodivisas.

Todas estas empresas su objetivo principal es **descentralizar el poder de posesión de la información**. En el momento en que esto se pueda hacer efectivo la información estará en las blockchains de estas empresas, pero será accesible a todo el mundo. Lo que

se critica a día de hoy no es únicamente el poder que tienen empresas como Facebook, Google o Palantir, sino que esa información es propiedad de estas y no del público general como debería de ser.

Si antes la mayor fuente de valor eran los medios productivos y el capital, ahora podemos ir viendo más y más como esto está cambiando y que lo que verdaderamente tiene valor es la información, y sobre todo los análisis y métricas que se extraen a partir del análisis de información de manera masiva.

Cambiando ahora de ámbito y yendo al futuro cercano creo que es importante analizar el impacto del blockchain en el sector financiero, ya que este será sin duda uno de los que sufran una mayor transformación.

6- La revolución del sistema bancario y financiero internacional.

Analizaremos el siguiente apartado a partir de los siguientes puntos: (a) El poder disruptivo del blockchain en el sector financiero, (b) La relación entre el blockchain y los bancos centrales y en último lugar (c) Las ICOss como nueva forma de financiación de las empresas.

a) El poder disruptivo del blockchain

La pregunta que nos hacemos aquí es; ¿Cómo va a revolucionar blockchain un sistema tan tradicional y arraigado como el bancario y financiero?

En primer lugar y antes de entrar más en profundidad en el análisis del impacto de la tecnología blockchain en el sector, es importante nombrar los potenciales beneficios y riesgos que puede tener su aplicación. Hay que tener en cuenta que ya no es solo los beneficios que la tecnología pueda conllevar sino también como trasladamos toda la información de los sistemas antiguos a los nuevos y como evitamos los potenciales riesgos que pueden acontecer durante la transición.

Dicho esto, los sistemas de información distribuida o DLT (*distributed ledger technology)* nos permiten optimizar sobre todo 5 funciones de los servicios y mercados financieros (Arnold, 2018) entre los que destacan mejorar la eficiencia de los mercados

financieros a través de la mejora de los sistemas de compensación y liquidación, la simplificación de procesos, la creación de un registro público que permitirá mejorar la accesibilidad a la información, que conllevará el incremento de la transparencia y la inmutabilidad de los registros, la mejora de la seguridad de los sistemas de información al estar la información distribuida en diferentes nodos y la reducción de riesgos operacionales y financieros.

Por otra parte, los riesgos a los que se somete el mercado aplicando esta tecnología tan incipiente se resumen en la potencial incertidumbre sobre cómo implementar la tecnología en tareas operacionales y financieras, la falta de adaptación u operatividad con sistemas de información actuales, el problema de la transición desde sistemas tradicionales a sistemas modernos informáticos, las cuestiones legales y de compliance (control de legalidad) concernientes al uso de sistemas de información distribuida, la ausencia de sistemas robustos de gobernanza debido a la reciente implantación de esta tecnología y todos aquellos problemas relacionados con la integridad de los datos, inmutabilidad y privacidad, y, por último y ya como reto o riesgo puramente tecnológico, la escalabilidad de los sistemas informáticos. Este factor es importante, ya que será el que a futuro nos permita comparar la eficiencia de ambas tecnologías; las tradicionales de registro centralizado y las modernas de registro distribuído.

Entrando ya en la mejora de eficiencia de los mercados financieros me gustaría empezar con una cita que dijo el profesor Andreas Park de la Universidad de Toronto en unas conversaciones con el clearing house SWIFT: “La cosa que más me llamo la atención cuando empecé a leer sobre blockchain fue sobre todo el alto nivel de transparencia. Porque cuando tienes un alto nivel de transparencia, eso provoca un cambio en la naturaleza de las transacciones económicas.”

El término eficiencia es muy amplio y en ocasiones vago si no se utiliza con la determinación adecuada. En este caso la eficiencia ha de ser medida en función de la velocidad y del coste que tiene el ciclo entero de transferencias de un activo concreto y de la precisión con que esta operación cubre las necesidades de las partes y del mercado al que está sirviendo. Al final el objetivo de los mercados financieros es conectar la oferta con la demanda y cuanto más fluido y barato sea este proceso, más eficiente será el mismo.

Precisamente y solo por mencionar, SWIFT es uno de los grandes gigantes de la industria que se va a ver amenazado por la implementación de esta tecnología. Como ya discutió hace tiempo el CEO de la compañía SWIFT, Gottfried Leibbrandt, en una entrevista con el periódico digital The Finanser, todavía queda mucho por avanzar en tecnología blockchain para ser comparable con una empresa como SWIFT (Skinner, 2017). El avance es lento pero seguro y si compañías como SWIFT o CLS (Continuous Linked Settlement) no se adaptan y se adelantan, probablemente acabe perdiendo su sitio en el mercado como ya pasó como otros gigantes como IBM que tuvo que reconvertirse en la época del *dotcom bubble* a principios de la década 2000 después de que empresas como Microsoft o Apple le ganaran la posición en la producción de ordenadores. IBM anunció la venta de su negocio de fabricación de ordenadores a Lenovo el 7 de diciembre de 2004 (Pctimeline).

Uno de los aspectos más margen de disrupción ofrece a las nuevas empresas tecnológicas dentro del sector financiero es la parte de compensación y liquidación debido a su elevado coste, su lentitud y la falta de renovación de sus sistemas.

Dentro de los aspectos que cambiará la aplicación del blockchain, el primer punto a mejorar es el de agilización de los sistemas de compensación y liquidación, lo que en inglés se conoce como *clearing and settlement*. Aquí es donde de verdad el factor de descentralización del blockchain toma protagonismo ya que a día de hoy toda la estructura concerniente a este tipo de operaciones está dominada por intermediarios y entidades centrales como los Central Securities Depositories (CSDs) y otros sistemas como el ECB's Correspondent Central Banking Model (CCBM) del Banco Central Europeo (BCE, 2017).

Este problema es mucho más grave de lo que pueda parecer a simple vista. Informes como el de Santander, Oliver Wyman y Anthemis Group, que estudiaba las ineficiencias de los mercados financieros, esperan que para 2022, gracias al uso de tecnologías blockchain, las instituciones financieras se ahorren entre 15 – 20 billones de euros al año. El ahorro provendría fundamentalmente de 3 puntos:

- Pagos internacionales
- *Trading* de activos
- Cumplimiento de la legalidad (*compliance)*

Por su parte, Accenture ha estimado en un informe titulado, "*Banking with Blockchain"* que el ahorro que puede suponer a los bancos el uso de la tecnología en los procesos de compensación y liquidación puede ascender hasta los 10 billones de dólares al año. (Accenture, 2017).

Viendo los datos y entrando posteriormente a analizar más en profundidad el estudio de Accenture, podemos observar también que debido a los enormes ahorros que se prevén, las grandes multinacionales del sector financiero están empezando a realizar enormes inversiones en la tecnología para no quedarse atrás en la carrera del blockchain. Si en septiembre de 2015 pudimos ver como Aite Group pronosticaba que en 2016 la inversión en blockchain por parte de grandes multinacionales ascendería hasta los 125 millones de dólares, 1 año después, pudimos ver a través de un estudio realizado por Greenwich Associates que la inversión efectiva durante el año 2016 doblo las expectativas, alcanzando una inversión total de más de 280 millones de dólares.

Empezando el análisis, a las primeras entidades que va a afectar el uso del blockchain es a las *clearing houses* como The New York Stock Exchange, el NASDAQ, BME clearing o la London stock Exchange.

¿Cómo funciona una *clearing house* o cámara de compensación?

Básicamente poniéndose en la posición contraria a cada uno de los lados de una transacción, dando así liquidez al mercado. Por ello este tipo de entidades no son útiles únicamente en un mercado de valores al uso, sino que también se plantean imprescindibles en los mercados de futuros, donde necesitas que una entidad estable mantenga el activo y asegure que se cierra la operación con la contraparte.

El problema de este tipo de entidades es que muchas de las operaciones todavía se están cerrando de forma manual y que para realizar estas operaciones en muchas ocasiones se cuentan con sistemas de cifrado y mensajes complejos que pueden llevar a confusión y retrasos en las confirmaciones. Además, como parte del sistema se realiza de forma manual, en muchas ocasiones se dan fallos, fallos que en sistemas automatizados no ocurrirían. Todas estas tareas se pueden automatizar gracias a uso del blockchain. Mediante la utilización de un registro común y el uso de smart contracts que permitan cerrar automáticamente las operaciones, los bancos pueden ahorrarse millones de euros al año, y sobre todo y más importante, eliminar ineficiencias y fallos inherentes al

sistema.

Por ello, no es que las *clearing houses* sobren, sino que sus modelos y sistemas necesitan ser modernizados para ser competitivos. Desde la crisis de 2008, las entidades reguladoras han hecho que los beneficios de los bancos disminuyan, con instrumentos como MIFID del regulador europeo, y ello ha causado la desaparición de muchos pequeños y medianos bancos a nivel mundial (Ridley, 2008). A nivel Europa, MIFID ya ha entrado en circulación, y por lo que pude aprender durante este último verano de prácticas en un banco de inversión, tal es la estructura de *compliance* que los bancos deben adoptar, que solo aquellos que tengan la envergadura suficiente podrán soportar el coste que ello supone.

A día de hoy son muchos los *clearing houses* que están llevando a cabo esta transformación implementando blockchain. Uno de los ejemplos más relevantes es el de la Australian Securities Exchange, que junto con la ayuda de la compañía Digital Asset Holdings está siendo uno de los pioneros hacia la transformación blockchain.

En Estados Unidos, la compañía DTCC (Depository, Trust and Clearing Compensation) ya está, junto con el apoyo de la empresa tecnológica R3, empezando a desarrollar también su propio sistema de blockchain para liquidar y compensar CDSs (Credit Default Swaps) o Swaps de Incumplimiento Crediticio. Si bien su idea es implementar este mismo sistema también para el *trading* de derivados, todavía queda tiempo hasta que se compruebe si funciona correctamente en el mercado de CDSs (Arnold, 2017).

Además de la compensación y liquidación otro de los aspectos más afectados y de los que más se ha oído hablar en el último año dentro de la implementación del blockchain en los mercados financieros es en pagos internacionales o transfronterizos. A nivel internacional SWIFT se posiciona cómo la empresa más directamente afectada por esta revolución debido a sus arcaicos sistemas y su elevado coste para las empresas

Para explicar mejor este apartado paso a analizar la revolución que sufrirá un sistema de ámbito mundial y arcaico como es el de SWIFT en el ámbito de pagos transfronterizos.

Las siglas de SWIFT significan Society for Worldwide Interbank Financial Telecommunications, es una empresa establecida en el año 1973, está presente en 210 países y presta sus servicios a más de 10.000 instituciones financieras distintas. SWIFT

es una empresa que se encarga fundamentalmente de asegurar que las compañías financieras transfieren información de forma completamente segura a través de un sistema estandarizado de códigos (Seth, 2017).

Junto con todos los problemas que mencionábamos antes, Ripple nos apunta otros tres que sin duda apoyan una reforma completa del sistema de transacciones internacionales y que dan pie a que empresas como Ripple empiecen a cuestionar la autoridad de SWIFT. Si bien es verdad que el proyecto nace en el año 2004, no es hasta la asociación del proyecto con grandes grupos financieros como el Santander, UBS o AMEX cuando este empieza a coger de verdad inercia y relevancia. Dentro de los datos que convierten el mercado en ineficiente a día de hoy hay que destacar el hecho de que los pagos internacionales son lentos, que las transacciones tardan entre 3 y 5 días en completarse, los costes son excesivamente altos (ascendiendo hasta 1,6 trillones de dólares al año) y, por último, que el sistema de ejecución manual que existe a día de hoy provoca que se generen numerosos fallos (Ripple).

Por todo esto las empresas y las personas demandan un sistema más eficiente, que parece que Ripple conseguirá en el corto o medio plazo.

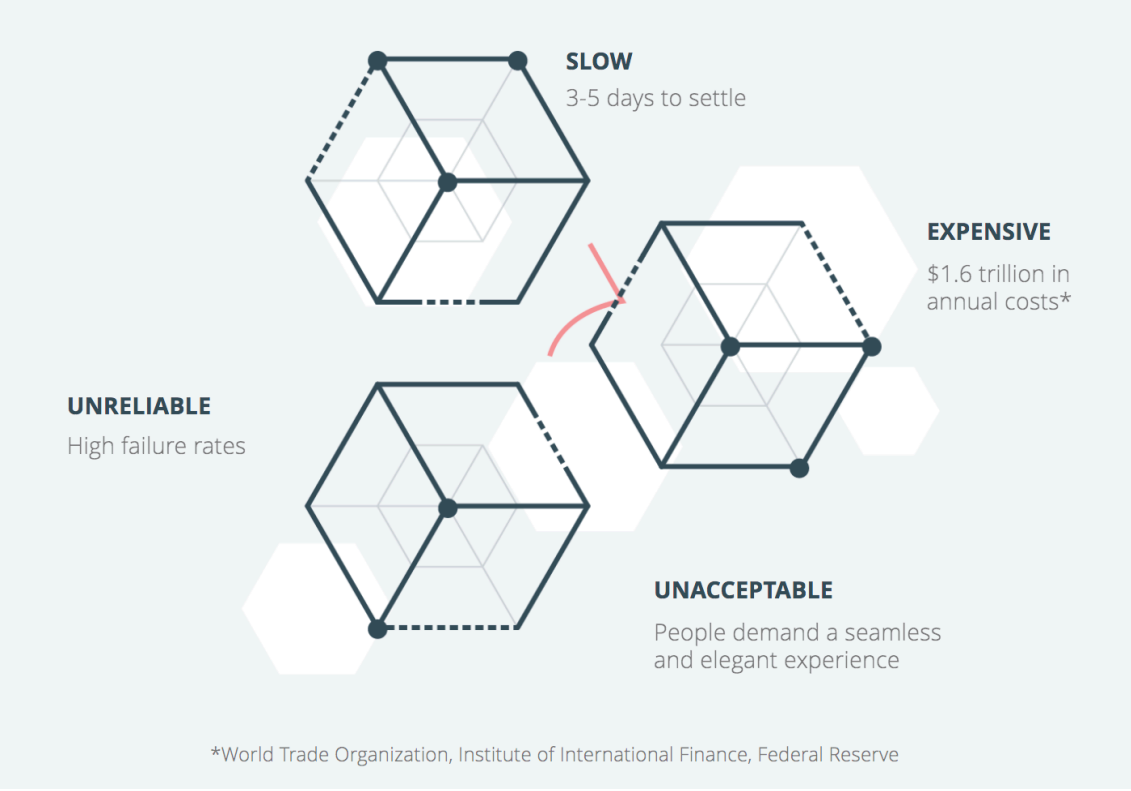

Figura 5. Imagen con la que Ripple explica las ineficiencias de los pagos

internacionales. Recuperado de Ripple. (2018). *Banks - Global Payment Uses Cases | Ripple*. Recuperado de: https://ripple.com/use-cases/banks/

Estos datos están extraídos de la World Trade Organization, del Institute of International Finance y de la Federal Reserve de los Estados Unidos.

SWIFT a día de hoy es una empresa que funciona a través de unos sistemas de estandarización de cifrado para enviar mensajes como las órdenes MT101 o ISO 20022.

A día de hoy, y previendo que Ripple les sustituya como plataforma de pagos internacionales, SWIFT ha creado un instituto conocido como el *GPII (Global Payments Innovation Initiative)* que básicamente su función es la de intentar agilizar los pagos internacionales a través del fomento de la cooperación entre los bancos.

Sistemas como el ***que*** existen a día de hoy provocan que en transacciones internacionales haya hasta 6 participantes entre el pagador y el pagado. Estos son el pagador, el banco del pagador, el correspondiente del banco del pagador (los correspondientes son aquellos que proveen de liquidez a la plataforma), correspondiente del banco del beneficiario, banco del beneficiario y beneficiario

De manera esquematizada esto sería:

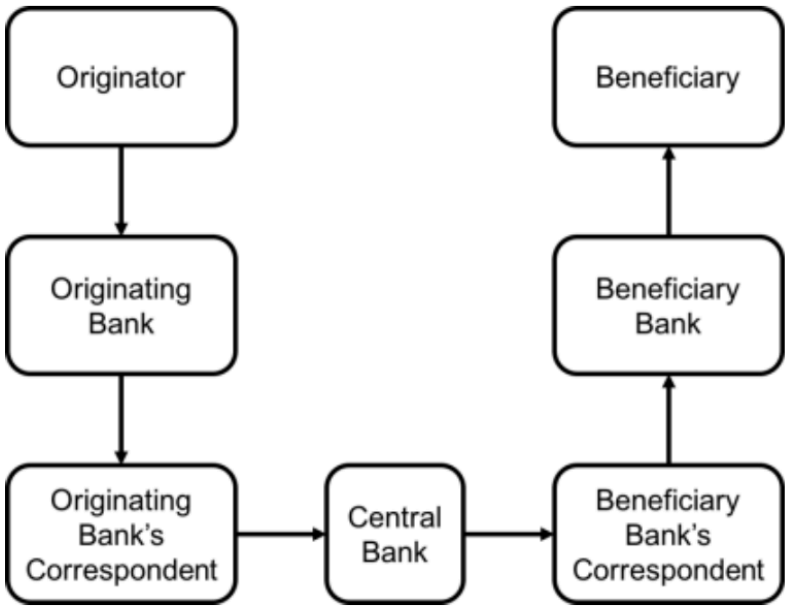

Figura 6. Ripple vs GPII. Recuperado de Treasurytoday.com. (2018). *Ripple vs SWIFT: payment (r)evolution | Treasury Today*. Recuperado de: http://treasurytoday.com/2017/07/ripple-vs-swift-payment-r-evolution-ttpv

Sistemas como Ripple ofrecen un servicio mucho más simplificado que consta de 4 pasos. Si bien el proceso es complejo, la operación se realiza en segundos. El proceso consta de los siguientes pasos: (a) El banco de origen requiere a qué precio está la divisa, Ripple contesta con los precios del mercado, se procede al procesamiento de las comisiones y los requerimientos legales. El precio de las divisas es el que está ahora mismo en el mercado, sin intervención de ningún tipo. (b) El banco de origen da el visto bueno, se cierra el precio del par y Ripple retiene ciertos fondos que serán transmitidos al banco receptor. Los fondos retenidos se quedan en una especie de sub registro en el que figuran las dos entidades, receptora y emisora, (c) El banco de origen transfiere los fondos, (d) El banco beneficiario confirma haber recibido el dinero.

	RIPPLE	GPII
Velocidad	Segundos	Horas o días
Comisiones	Las más bajas posibles	Públicas
FX	El mejor precio posible	Determinadas por el consejo de tipos del banco
Datos	Entrega total	Pensado para la versión 2
Seguimiento	No se necesita	Si
Tecnología	Ripple y ILP	SWIFT + nuevos mensajes
Número de bancos	45	80
Dificultad	Similar	Similar

Figura 7. Diferencias entre Ripple y GPII. Recuperado de Treasurytoday.com. (2018). *Ripple vs SWIFT: payment (r)evolution | Treasury Today*. Recuperado de: http://treasurytoday.com/2017/07/ripple-vs-swift-payment-r-evolution-ttpv

En relación a esto Ripple ofrece tres tipos de servicio distintos para optimizar los sistemas actuales: (Ripple)

- **xCurrent**: esta es la verdadera revolución y la herramienta que las empresas están usando en la realidad. A través de Xcurrent, los bancos pueden realizar transacciones internacionales al instante. Los bancos se mandan unos códigos de confirmación, que si son aceptados por ambas entidades, permite el pago instantáneo sin pasar por todos los intermediarios previamente descritos.

Para asegurar que las operaciones se realizan de manera segura y siguiendo todas las normas legales concernientes a pagos internacionales, Ripple ha creado una entidad que se llama RippleNet Advisory Board. Esta entidad se encarga además de controlar de elaborar junto con las entidades colaboradoras el Ripple Rulebook, que pretende guiar un marco que permita guiar la actuación de las empresas que forman parte de la comunidad Ripple en caso de conflicto. El Rulebook contiene concretamente:

- los derechos y obligaciones de los participantes en la comunidad Ripple
- Las reglas a la hora de operar y hacer negocio
- Compliance: modos de gestión y sanción en caso de incumplimiento

Uno de los apoyos más sonados es el del Santander con Ripple. Santander anunció a principios de Febrero de 2018 que en los próximos meses tiene previsto el lanzamiento de una aplicación que permita realizar transacciones a través de Ripple, y más concretamente a través del sistema xCurrent.

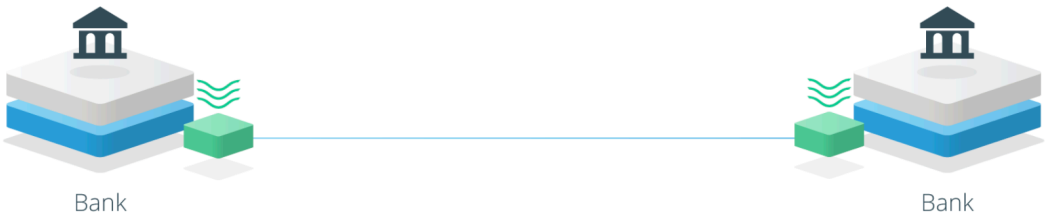

Figura 8. Funcionamiento XCurrent. Recuperado de Ripple. (2018). *XRP | Ripple*. Recuperado de: https://ripple.com/xrp/

- **xVia**: este es un servicio pensado fundamentalmente para todo aquel que quiera realizar envíos a través de varias redes pero con una única interfaz. Se podría entender como una solución fácil para los usuarios para realizar pagos o envíos de dinero. Es algo así como un Paypal que opera a través de blockchain. El esquema que incluyo aquí abajo es el mismo que utiliza Ripple en su página web para explicar el funcionamiento del sistema:

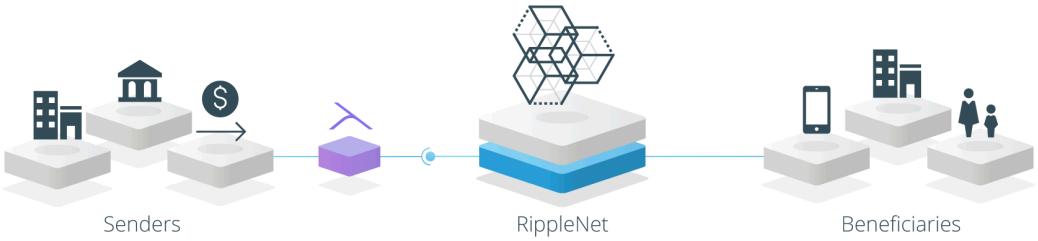

Figura 9. Funcionamiento XVia. Recuperado de Ripple. (2018). *XRP | Ripple*. Recuperado de: https://ripple.com/xrp/

- **xRapid**: Sirve como sistema de liquidez en mercados emergentes. Este es de menos importancia para el desarrollo del TFG así que simplemente mencionaremos que es el único servicio de Ripple que efectivamente utiliza la divisa propia de la compañía XRP.

Esto nos permite ver que las entidades más grandes ya se están organizando para crear no solo un sistema que sea eficiente a nivel funcional, sino también un sistema regulatorio al margen de la centralización del estado. Si algo está permitiendo el desarrollo del blockchain es precisamente la autonomía frente a los estados. Si esto prosigue así, probablemente en el futuro los estados simplemente se delimiten a regular las "líneas rojas" que ninguna compañía debe sobrepasar, dejando mucha más libertad y autonomía a las empresas para regular sus propias situaciones.

Por otra parte, en términos de transferencias internacionales, a día de hoy las instituciones financieras no intercambian entre ellas recursos fácticos (o, en otras palabras, divisas), sino que lo que se intercambian son cifras y datos. Esto es muy problemático ya que si bien es verdad que ningún banco está interesado en mentir en este tipo de operaciones o gastar doblemente un dinero del que fácticamente no dispone, lo cierto es que estos podrían hacerlo. No es la primera vez que los bancos juegan en el límite de la legalidad o lo sobrepasan. Por medio de sistemas blockchain el sistema no es solo más seguro y eficiente para las instituciones financieras, sino que también es mejor para los inversores, ya que pueden tener la seguridad de que estos fondos son efectivamente transferidos.

Otros aspectos de los mercados financieros que cambiarán de manera radical gracias a la implementación del blockchain

Para empezar el análisis partimos de este estudio realizado por Accenture, en colaboración con la empresa McLagan, creador de *benchmarks* para empresas del sector financiero. Ambas empresas crearon un estudio de cómo las tecnologías de registro distribuido, y en particular el blockchain, iban a afectar a los costes de la industria y mercados financieros. Lo más importante a destacar aquí es la leyenda que podemos observar en la parte baja del gráfico.

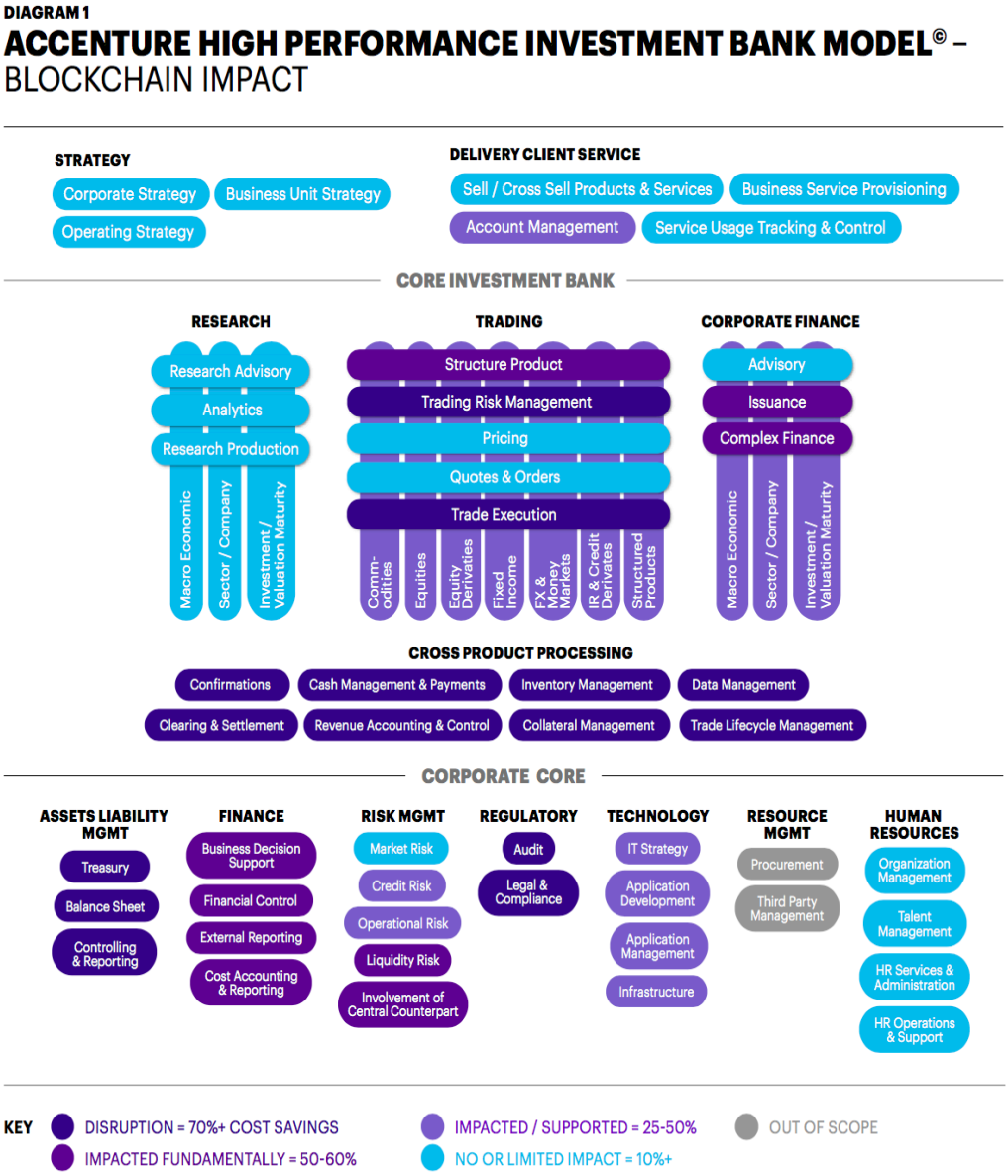

Figura 10. Mejora de la eficiencia en los bancos de inversión. Recuperado de Accenture.com. (2018). Recuperado de: https://www.accenture.com/t20170120T074124Z__w__/us-en/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Consulting/Accenture-Banking-on-Blockchain.pdf#zoom=50.

El estudio analiza desde todos aquellos ámbitos y departamentos que encontramos en un banco de inversión. En función del nivel de impacto, tenemos uno u otro color.

Como podemos ver y también relacionado con lo que hemos estado tratando hasta ahora en el trabajo, las áreas que más se van a ver afectadas (etiquetadas con la etiqueta de "disruptivas") son fundamentalmente:

- **Trading:** y dentro de trading gestión de riesgos y ejecución de operaciones.
- **Procesamiento de activos cruzados:** Aquí es donde se refiere a toda la problemática tratada previamente de cierre de operaciones, confirmaciones y liquidaciones, gestión de datos… etc.
- **Regulatorio:** en todo aquello referido a los procesos de auditoria de la empresa, los costes se reducen drásticamente.
- **Gestión de activos y pasivos:** tesoro de la empresa, creación de los balances de situación…

Por el lado contrario, las áreas de la empresa donde menos se va a notar la influencia del blockchain serán fundamentalmente los departamentos de recursos humanos, investigación o *research*, servicios de asesoría y estrategia y servicios de atención al cliente

A pesar de que hay ciertos departamentos en los que el blockchain tiene menor aplicación podemos ver que en todos los departamentos tiene al menos una mínima influencia. Por ejemplo, en recursos humanos, puede ser que no se recorten gastos por medio del blockchain de manera directa, pero si de manera indirecta. A través de una identidad digital generada en blockchain se puede asegurar que el *background check* (o verificación de los datos proveídos) que normalmente todas las empresas aseguran a una tercera empresa, queda verificado a través del blockchain. De esta manera todas las personas tienen una identidad digital en el que sus logros o hechos quedan previamente

validados. Esto da seguridad al sistema, y sobre todo permite ahorrar costes a la empresa que va a contratar. El proceso de contratación se hace de esta manera mucho más ágilmente. Empresas en el sector de las identidades digitales nos podemos Este es solo un ejemplo, pero en el resto de departamentos de una manera u otra este tipo de sistemas puede ayudar a crear procesos más eficientes, tanto de forma directa como indirecta.

Dentro de las start-ups que ya están trabajando en optimizar este tipo de procesos nos podemos encontrar empresas como Digital Asset Holdings, R3CEV, SETL, T0, Clearmatics y más.

Además del sector privado es importante tomar en consideración el impacto que el uso de estas tecnologías puede tener en el sector público, ya que, sin apoyo regulatorio, la adaptación de los sistemas a nivel privado carece de sentido.

b) Blockchain y los Bancos Centrales

i. Las criptomonedas en blockchain como divisa fiat. La utilidad de los bancos centrales en redes descentralizadas

Como hemos comentado previamente, la mayor disrupción que crean los sistemas basados en blockchain es la aportación a la sociedad del concepto de descentralización. A día de hoy vivimos en sociedades en las que todo lo que hacemos tiene que estar controlado y gestionado o validado por una entidad central, ya que, sin esta, ni el mercado ni el resto de conciudadanos tomarían como válidas nuestra información o nuestro dinero. Para que los euros tengan valor, tiene que ser emitido por el Banco Central Europeo, para que tengamos una identidad, lo tiene que acreditar el estado, para tener una propiedad, un registrador… etc. El problema recae en que las personas por naturaleza desconfiamos unas de otras, provocando esto que deleguemos el poder a instituciones centrales que actúen como baremo de validez, pero, ¿Qué pasa si nuestra confianza es en balde? ¿Son las empresas privadas de fiar? ¿Confiamos más en una empresa que en toda una comunidad de nodos?

Por poner un ejemplo, cuando tenemos una cuenta en PayPal y por ejemplo disponemos de 1000$ en esta, nosotros confiamos en que tenemos una disponibilidad inmediata de estos fondos porque PayPal lo acredita, pero, lo cierto es que este dinero es un mero número y que PayPal dispone de esos fondos para gastarlos y que te siga apareciendo el numerito de 1000$ dólares. La respuesta a esto es que obviamente nosotros nos fiamos del sistema porque ha pasado unos ciertos controles regulatorios, el equipo es de fiar… etc., pero lo cierto es que el control está en su mano. Esto es lo que se conoce como el problema del doble gasto que soluciona en su momento y por primera vez Bitcoin hoy que está relacionado con la descentralización en la que después profundizaremos. Gracias a sistemas blockchain, el dinero que se gasta no se puede volver a gastar debido a que todas las transacciones quedan registradas en la red. Es decir, si te hackean la cuenta y te roban te han robado, pero ves claramente que ese dinero ya no está y que eso queda registrado en la blockchain. En redes centralizadas el único que acredita esas operaciones es la propia empresa o equipo. Esto sin embargo no ocurre en redes descentralizadas donde los validadores de la red y las transacciones son desconocidos. Estos trabajan a cambio de incentivos por lo que el sistema permite que unas personas confíen en otras para realizar transacciones y que, por otra parte, desaparezca la necesidad de un ente centralizado. La red es inmutable y por tanto inmanipulable salvo ciertos casos difíciles de probar como *51% attack* en el que no vamos a entrar ya que no tiene mucha aplicabilidad en el mundo real.

En el momento que tú con un activo digital puedes comprar una casa, irte de vacaciones, heredar o comprar el pan por las mañanas ya que todos estos comerciantes te lo admiten como método de pago, ¿qué utilidad tiene el euro y sobre todo el BCE?

Obviamente esta pregunta solo la hago de manera tan drástica para poner en relieve la posición del BCE en este tema, pero el BCE a parte de la centralización de la emisión de la moneda hace muchas otras cosas como el control de la política monetaria y, más específicamente, el control de la inflación o la promoción de los sistemas de pago (BCE).

Es importante plantearnos que todos estos proyectos no tienen ninguna utilidad hasta que no son aplicados en ámbito institucional. Es por ello que podemos catalogar dos tipos de países:

1- Aquellos que se lanzan a innovar dentro de su propio territorio para ser pioneros en la materia (caso de Estonia o Venezuela)
2- Aquellos que esperan a que ya haya funcionado bien en otro país para implementarla.

Ahora en el siguiente punto pasaremos a estudiar las que efectivamente se han lanzado a ser pioneras en el cambio, empezando por el conocido caso de Venezuela y su cryptomoneda, Petro.

Uno de los más fuertes argumentos que tienen los tradicionalistas contra las inversiones en blockchain es que aseguran que cuando inviertes en una moneda no estás invirtiendo en algo tangible, con lo que se puede decir que no tiene colateral. Cuando inviertes en una empresa, en principio en caso de quiebra se supone que tienes derecho sobre los rendimientos generados por la liquidación de los activos de esta. Si bien esto no es siempre así, como se ha visto en el caso del Banco Popular (Hernández, 2017), a muchos inversores es lo que más les transmite tranquilidad. Si Bitcoin de repente pasa a valer 0, ¿Qué responde sobre el activo? Efectivamente, nada.

Esa es la preocupación que quiso atacar el gobierno de Venezuela creando la moneda Petro.

Petro es el primer ejemplo efectivo de una cryptomoneda emitida por un país relevante a nivel internacional y su característica fundamental es que el gobierno venezolano asegura que el valor del Petro está respaldado por las reservas de petróleo del país, que a día de hoy ascienden hasta los 5300 millones de barriles de petróleo, siendo la emisión total de hasta 100 millones de tokens. El ticker del Petro es PTR.

Literalmente en palabras del gobierno de Venezuela en su Whitepaper: “El Petro, será un criptoactivo soberano respaldado por activos petroleros y emitido por el Estado venezolano como punta de lanza para el desarrollo de una economía digital independiente, transparente y abierta a la participación directa de los ciudadanos. También servirá como plataforma para el crecimiento de un sistema financiero más justo y que contribuya al desarrollo, la autonomía y el intercambio entre economías emergentes.

Activos petroleros venezolanos servirán para impulsar la adopción de criptoactivos y de

tecnologías basadas en las cadenas de bloques en el país.

El Petro será un instrumento para dar estabilidad económica e independencia financiera de Venezuela, aunado a una visión ambiciosa y global para la creación de un sistema financiero internacional más libre, equilibrado y justo."

Si bien es cierto que el manifiesto atiende no solo a razones económicas sino también políticas debido al bloqueo de Estados Unidos, la intención del gobierno de Venezuela con la creación de esta moneda se hace más que patente.

El objetivo de la cryptodivisa Petro es fundamentalmente sortear los bloqueos internacionales a los que está sometido el país. De esta manera, en el momento en el que el Petro sea aceptado como método de pago internacional, Venezuela habrá salido si no efectivamente, si a efectos prácticos del bloqueo económico. Países como Estados Unidos ya se han lanzado a prohibir el trading de Petro en el país.

Según fuentes oficiales del gobierno de Venezuela, en el primer día de lanzamiento de la moneda Petro llegó a recaudar hasta 735 millones de dólares.

Por lo tanto, lo que pretende el gobierno de Venezuela es básicamente que el Petro sea la primera moneda respaldada por activos reales que sea atractiva para el inversor. Si bien es cierto que sus reservas de petróleo son las mayores del mundo, la situación sociopolítica y el hecho de que la blockchain sea privada puede provocar que el sistema no genere demasiada confianza al inversor.

Dentro de los otros países que están desarrollando cryptomonedas nacionales podemos encontrar países tan influyentes a nivel internacional como Rusia, Dubái, Japón o Suecia.

ii. El poder del blockchain frente a los bancos centrales

Mi respuesta a esto es que no y lo explicaré en profundidad en las siguientes líneas. Si bien es verdad que la labor de los bancos centrales cambiará, es la sociedad misma la que no le conviene carecer de un ente regulador. Yo siempre he sido partidario de la existencia de una única divisa a nivel global. Pero ya que debido a millones de intereses

dispares esto no sucederá jamás, creo que cada banco central y entidad reguladora tiene que seguir existiendo para poder velar por los intereses de los ciudadanos de sus respectivas regiones.

El blockchain al final es una herramienta que fundamentalmente facilita el registro correcto y sin alteraciones de los datos que van entrando en el sistema con lo cual esto solo sería útil en un mundo en el que nos planteemos que todos los estados van a cooperar entre ellos o que la humanidad va a crear una cryptodivisa que sirva como medio mundial de pago sin ningún tipo de ánimo de lucro.

El hecho de que un país o entidad central monetaria emita una cryptomoneda no quiere sino decir que están intentando digitalizarse, pero no crear un sistema que les sustituya. Al final, tomando el ejemplo de Venezuela, el hecho de que emitan 100 millones de monedas y nada más les acabará perjudicando porque la moneda fluctuará igual que cualquier otra moneda.

Las monedas fiat a día de hoy se basan en la confianza de las personas. Es decir, un euro a día de hoy como cualquier otra moneda fiat no tiene ningún tipo de respaldo de ningún activo concreto. Hasta el 15 de agosto de 1971, cuando Richard Nixon abolió el patrón oro, había un patrón internacional que era el patrón oro que permitía que los dólares fueran intercambiados por ciertas cantidades de oro. De esta manera y con la supresión del patrón oro cambiamos el dinero fiduciario (que significa respaldado por activos) por dinero fiat que es una palabra proveniente del latín y que significa “así se haga”. El dinero tiene el valor que tiene por Convenio, es decir, porque los estados asumen que son ellos los que tienen el poder de emitir moneda y los que tienen autoridad para decidir que su moneda es la única con curso legal. (Esteve, 2016)

A efectos prácticos, el Bitcoin tiene el mismo respaldo que un euro siendo este respaldo la confianza del mercado. El Bitcoin, como comentábamos previamente, ha llegado a alcanzar, en menos de 10 años de vida, una capitalización bursátil de más de 300 billones de dólares, más que todas las empresas del IBEX por separado y, que, por ejemplo, el triple de un gigante como INDITEX. Esto, unido a que la divisa ya es aceptada por un gran número de personas y comercios nos hace pensar que quizás en un futuro, si la gente se cansa de la actuación de los bancos centrales, estos pasen a un segundo plano y las divisas digitales a un primero.

La única manera de la internacionalización de los métodos de pago a través de blockchain es a través de una divisa neutral que no atienda a los intereses de nadie que se erija como método de pago válido aceptado cuasi-mundialmente. Eso es lo que a día de hoy podría ser el dólar americano que ya si estás en Japón, India o Europa hay muchos sitios en los que te aceptan dólares como método de pago.

A día de hoy el proyecto que más se acerca a esa realidad es el Bitcoin, pero con los graves problemas de escalabilidad que sufre aún queda mucho por evolucionar antes de que podamos llegar a un concepto tan avanzado de la divisa. Obviamente, y como en todo casual, las divisas pueden ser prohibidas por las instituciones regulatorias, pero únicamente en concepto de que los comercios no puedan aceptar el pago en una determinada cryptodivisa, ya que el control de las *wallets* debido a la criptografía se torna imposible. La gente, aunque una cierta divisa este prohibida para el comercio podrá operar con ella en mercados secundarios o en mercados P2P con lo cual a los estados no les interesa prohibirla sino fomentar su implementabilidad en un sistema nacional que permita las transacciones en este tipo de activos. Si al final la gente va a poder invertir igualmente, cuanta más liquidez y respaldo jurídico tenga el mercado, más avanzado será el sistema. Actualmente, parece que todos los estados fuertes están de acuerdo en que prohibir este tipo de activos no sería una solución sino una piedra más en un proceso de digitalización que deviene imparable.

Los países que a día de hoy están trabajando más fuertemente en desarrollar sistemas propios no son aquellos que tienen sistemas jurídicos fuertes y sistemas políticos estables sino aquellos que quieren salir de ciertos bloqueos económicos y que por lo tanto buscan alternativas a la financiación como son los ejemplos de Irán y Venezuela.

Estos proyectos pueden ser rentables para el país que los emite, pero al largo plazo no ayuda a consolidar un sistema monetario sólido.

En términos de la desaparición de los bancos centrales solo cuando las personas den más validez a proyectos nacidos de la iniciativa particular que a proyectos nacidos de la iniciativa estatal será cuando de verdad podamos hablar de una mutación o desaparición íntegra de este tipo de instituciones.

iii. Más allá de la desaparición ¿Cuáles son los aspectos principales que cambiarán los bancos centrales en el futuro cercano?

En función de lo que hemos estado viendo hasta ahora y lo que requieren los mercados financieros a día de hoy, las grandes instituciones financieras están invirtiendo en tecnologías de descentralización fundamentalmente por tres razones fundamentales que son el ahorro de costes y eficiencia, la competición con *startups* y los nuevos modelos de negocio como plataformas de pagos internacionales utilizando blockchain (Meola, 2017).

Si bien es verdad que las instituciones financieras privadas ya se han lanzado a la aventura tecnológica, en el plano institucional público estas entidades son todavía reticentes a arriesgarse y poder equivocarse. En palabras del BCE y del Banco Central de Japón, estas tecnologías aún no son maduras y por tanto no están preparadas para instrumentalizar los sistemas de pago internacionales (Koranyi y Evans, 2017).

La desconfianza desde las instituciones públicas está provocando que estas se dediquen a cooperar con las empresas, pero desde la distancia, llevando el proceso de manera mucho más lenta que el sector privado.

Las funciones que fundamentalmente empezarán a desarrollar los bancos centrales a partir de tecnologías blockchain se centrarán en temas de transparencia, pagos, gestión de riesgos, identidades digitales, auditoría, divisas digitales y resistencia a ataques y a caídas del sistema (Del Río, Hileman, 2017).

Los contrapuntos a los que se refieren los bancos centrales son por una parte la falta de privacidad, que el registro sea público permite que todo el mundo pueda acceder a la información que se registra en la blockchain y otra parte la escalabilidad. Como todos, hasta que este problema no se resuelva va a ser muy difícil que veamos a instituciones públicas apostando por la tecnología.

A continuación, expongo una tabla creada por el investigador César A. Del Río en su trabajo "***Use of distributed ledger technology by central banks: A review"*** en la que categoriza el estado de la implementación del blockchain por parte de las instituciones públicas desde 4 puntos. Los países seleccionados para la muestra son aquellos del G20 más los de la OECD (Organización para la cooperación y el desarrollo económicos)

excluyendo los países de la Unión Europea que no son parte de la OECD. El estudio se rige entonces en 4 puntos que son: (a) Funciones del blockchain para los bancos centrales, (b) Estado de adopción del blockchain, (c) Medios por los que se ha compartido el estado de adopción y (d) Postura de los bancos centrales: positiva, negativa, neutral.

Dentro del gráfico también se verán las siglas PCS y DCS siendo PCS, pagos, compensación y liquidación y DFC divisas *fiat* digitales.

Bancos centrales y Tecnologías de Registro Distribuido (DLT en inglés)

#	Países	Región	Banco Central	Funciones para usar DLT	Adopción de Sistemas de DLT	Comunicaciones	Postura
1	Argentina	Sudamérica	Banco Central de la República Argentina	PCS	Estudiándolo	Entrevista (Marty, 2016)	Positiva
2	Australia	Oceanía	Reserve Bank of Australia	PCS	Estudiándolo	Informe (Reserve Bank of Australia, 2017)	Positiva
3	Austria	Europa	Oesterreichische Nationalbank	No info	Abiertos a la tecnología	Interview (Das, 2017)	Neutral
4	Bélgica	Europa	National Bank of Belgium	No info	Estudiándolo	Report (National Bank of Belgium, 2017)	Positiva
5	Brasil	Sudamérica	Banco Central	PCS IM	Experimentando	Informe (Burgos, Filho, Suares, y	Positiva

			do Brasil			de Almeida, 2017)	
6	Canadá	Norte América	Bank of Canada	PCS	Experimentando	Announcement (Wilkins y Gaetz, 2017), announcement (TMX, 2017)	Positiva para compensación y liquidación y negativa para DFC
7	Chile	Sudamérica	Banco Central de Chile	PCS RM	Estudiándolo	Informe (Furche, Madeira, Marcel, y Medel, 2017)	Positiva
8	China	Asia	People's Bank of China	DFC	Experimentando	Pronunciamiento (Casey, 2017)	Positiva
9	República Checa	Europa	Czech National Bank	No info	Open to it	Entrevista (Czech National Bank, 2017)	Neutral
10	Dinamarca	Europa	Danmarks Nationalbank	DFC PCS	Estudiándolo	Pronunciamiento (Levring, 2016), report (Danmarks Nationalbank, 2017)	Positiva para PCS, y negativa para DFC
11	Estonia	Europa	Bank of Estonia	DFC	Estudiándolo	Pronunciamiento (Daniell, 2017)	Positiva
12	Finlandia	Europa	Bank of Finland	PCS	Estudiándolo	Pronunciamiento (Bank of Finland, 2016)	Positiva

13	France	Europa	Banque de France	PCS	Experimentando	Pronunciamiento (François Villeroy de Galhau, 2017)	Positiva
14	Alemania	Europa	Deutsche Bundesbank	PCS DFC	Experimentando	Informe (Deutsche Bundesbank, 2017)	Positiva para PCS, negativa para DFC
15	Grecia	Europa	Bank of Greece	No info	No info	No info	No info
16	Hungría	Europa	Hungarian National Bank	No info	No info	No info	No info
17	Islandia	Europa	Central Bank of Iceland	DFC	Abiertos a la tecnología	Entrevista (Central bank of Iceland, 2017)	Positiva
18	India	Asia	Reserve Bank of India	DFC	Estudiándolo	Informe (IDRBT, 2017)	Positiva
19	Indonesia	Asia	Bank of Indonesia	No info	No info	No info	No info
20	Irlanda	Europa	Central Bank and Financial Services Authority of Ireland	TR	Experimentando	Pronunciamiento (Lane, 2017)	Neutral

21	Israel	Asia	Bank of Israel	No info	No info	No info	No info
22	Italia	Europa	Banca d'Italia	No info	No info	No info	No info
23	Japón	Asia	Bank of Japan	PCS	Experimentando	Pronunciamiento (BCE y BOJ, 2017)	Negativa
24	Corea del Sur	Asia	Bank of Korea	No info	Experimentando	Pronunciamiento (2017)	Positiva
25	Letonia	Europa	Bank of Latvia	No info	No info	No info	No info
26	Luxemburgo	Europa	Banque Centrale du Luxembourg	No info	No info	No info	No info
27	México	Norte América	Banco de México	No info	No info	No info	No info
28	Holanda	Europa	De Nederlandsche Bank	PCS	Estudiándolo	Entrevista (del Castillo, 2016a)	Positiva
29	Nueva Zelanda	Oceaníaa	Reserve Bank of New Zealand	No info	Abiertos a la tecnología	Pronunciamiento (Fiennes, 2017)	Neutral
30	Noruega	Europa	Norges Bank	DFC	Estudiándolo	Pronunciamiento (Nicolaisen, 2017)	Positiva

31	Polonia	Europa	National Bank of Poland	No info	Abiertos a la tecnología	Pronunciamiento (Zhao, 2017)	Negativa
32	Portugal	Europa	Banco de Portugal	No info	No info	No info	No info
33	Rusia	Asia	Bank of Russia	PCS	Experimentando	Report (Khrennikov y Rudnitsky, 2017)	Positiva
34	Arabia Saudí	Asia	Saudi Arabian Monetary Authority	No info	No info	No info	No info
35	Eslovaquia	Europa	National Bank of Slovakia	No info	No info	No info	No info
36	Eslovenia	Europa	Bank of Slovenia	No info	Estudiándolo	Página web	Positiva
37	Sudáfrica	África	South African Reserve Bank	DFC	Abiertos a la tecnología	Pronunciamiento (Higgins, 2017), report (del Castillo, 2017)	Positiva
38	Corea del Sur	Asia	Bank of Korea	DFC	Experimentando	Pronunciamiento (EconoTimes, 2017)	Positiva
39	España	Europa	Banco de España	PCS	Open to it	Informe (González-Páramo, 2017)	Negativa

40	Suecia	Europa	Sveriges Riksbank	DFC	Estudiándolo	Informe (Sveriges Riksbank, 2017)	Positiva
41	Suiza	Europa	Swiss National Bank	PCS DFC	Abiertos a la tecnología	Pronunciamiento (del Castillo, 2016b)	Neutral
42	Turquía	Europa	Central Bank of the Republic of Turkey	No info	No info	No info	No info
43	Reino Unido	Europa	Bank of England	PCS DFC	Experimentando	Pronunciamiento (Carney, 2017a), speech (Carney, 2017b), report (Cleland, 2017)	Neutral
44	Estados Unidos	Norte América	Federal Reserve System	PCS DFC	Experimentando	Pronunciamiento (Powell, 2017), report (Federal Reserve System, 2017)	Neutral
45	Unión Europea	Europa	European Central Bank	PCS	Experimentando	Pronunciamiento (BCE y BOJ, 2017)	Negativa
46		Mundo	Bank for International Settlements	PCS	Experimentando	Informe (BIS, 2017), report (Bech y Garratt, 2017)	Neutral

Tabla 11. Estudio de la situación internacional a nivel estatal y supraestatal respecto al blockchain. Recuperado de César del R. Use of distributed ledger technology by central banks: A review. *Enfoque, Vol 8, Iss 5, Pp 1-13 (2017)* [serial online]. 2017;(5):1.

Recuperado de: Directory of Open Access Journals, Ipswich, MA.

Como vemos existem discrepancias entre los distintos países y regiones geográficas, pero el *grosso* de los 46 países analizados plantea una perspectiva favorable en torno al estudio de la tecnología y futura implementación de esta en la sociedad.

c) Las ICOs como nuevo sistema de financiación de empresas

i. Origen y concepto de las ICOs

Las siglas ICO (Inital Coin Offering) provienen del conocido término bursátil IPO (Initial Public Offering). Si una IPO se puede entender como una emisión primaria de acciones en un mercado secundario, una ICO se podría entender como una primera emisión de cryptomonedas o tokens (Verhage, Russo y Katz, 2017)

Las ICOs son por lo tanto las primeras emisiones de monedas o tokens en el mercado que ofrece una plataforma. Las ICOs están pensadas como métodos alternativos a los sistemas tradicionales de financiación. En este tipo de operaciones la empresa pone un plazo para completar una cierta cuota de inversión (*soft cap y hard cap)* y a medida que se invierte se van distribuyendo los tokens. En la gran mayoría de ocasiones hasta el día de hoy las ICOs se han desarrollado a través de protocolo Ethereum. Esto implica que los tokens que se emiten estarán registrando y operativos a través de la blockchain de Ethereum, a pesar de ser de la compañía que los emite. Además de Ethereum hay muchas otras blockchains en las que se pueden emitir tokens como pueden ser Waves, Universa, AEternity o Stellar.

Como origen de todo esto, la primera ICO tuvo lugar en el año 2013, de la mano de una compañía conocida como Mastercoin (Buterin, 2013). A partir de ahí el crecimiento a lo largo de los años ha sido exponencial.

Normalmente en los mercados regulados para captar financiación se necesita cumplir una gran cantidad de requisitos, sin embargo, por medio de las ICOs, la regulación estatal se queda fuera (por lo menos hasta hace poco) y lo único que importa son las

proyecciones del proyecto en concreto y la cantidad que estén dispuesta a invertir la comunidad.

ii. Instrumentos necesarios para realizar una ICO e impacto de estas en la economía mundial

Para llegar a una ICO las empresas disponen fundamentalmente de 4 factores para captar inversión:

- **Whitepaper o papel blanco**: entendido como el Business Plan de la empresa. En este se detallan el calendario de hitos de la empresa, el funcionamiento del protocolo, la plataforma sobre la que se ejecuta la emisión, el sistema de minación y consenso… etc. Cada Whitepaper contiene lo que la empresa quiere transmitir al mercado ya que como no hay ninguna regulación que especifique los requerimientos que por ley tienen que cumplirse cada empresa lo adapta a sus necesidades.
- **Beta o *Minimum Viable Product:*** si bien es verdad que hasta el día de hoy escasean los proyectos que se hayan presentado con una buena Beta, las empresas en el futuro, debido al creciente número de participantes en el mercado y a la intervención de las autoridades públicas tendrán que desarrollar cierta prueba de viabilidad para dar confianza a los inversores. Una empresa que realizó una Beta muy consistente antes de su ICO fue Augur, una plataforma de mercados predictivos que permitía entrar en su simulador para que los usuarios pudieran ver cómo iba a funcionar la plataforma una vez estuviera operativa. (AUGUR, 2017).
- **Equipo:** en este tipo de proyectos en los que prácticamente ninguno podrá estar operativo en el corto medio plazo debido a las dificultades, tanto técnicas como administrativas el equipo es fundamental, ya que normalmente asegura cierto nivel de diligencia. Ejemplos de proyectos que han tenido éxito gracias a un buen equipo son Ethereum, Cardano o Ripple.
- **Publicidad:** hasta el día de hoy hemos visto que si bien es verdad que los proyectos que eran extraordinariamente buenos han salido sin apenas gasto en publicidad, muchos otros han necesitado importantes inversiones en este ámbito

para poder hacerse ver en la comunidad.

Hasta el día de hoy, desde el año 2014 ya han tenido lugar más de 1500 ICOs y se han captado más de 9 billones de dólares (Icodata, 2018). La gran explosión de este concepto fue en el año 2017 cuando más de 6 billones de dólares fueron invertidos a lo largo del año en este tipo de emisiones. El ritmo no parece bajar y ya en 2018 llevamos más de 2 billones de dólares invertidos. Hay que añadir también que a este buen rendimiento en el primer trimestre del año han contribuido 2 de las operaciones más grandes de la historia de este tipo de emisiones, la PreICO de Telegram, en la que se captaron más de 800 millones de dólares (Coindesk, 2018) y la de la moneda controlada por el gobierno venezolano Petro que captó, según la versión de su presidente, Nicolás Maduro, en Twitter más de 735 millones de dólares en su *presale*.

iii. Problemas regulatorios concernientes a las ICOs

A día de hoy los problemas más importantes concernientes a estos sistemas alternativos de financiación son aquellos relativos a la calificación jurídica de los instrumentos que se emiten. Si bien es verdad que muchos estados y organizaciones internacionales ya se han pronunciado al respecto, el informe más importante e influyente a día de hoy ha sido el que emitió la SEC (La comisión de valores estadounidense) en Julio de 2017 (SEC, 2017). En este informe no solo se advierte a los inversores de los riesgos potenciales de este tipo de instrumentos, sino que también se hace una clara distinción entre los distintos tipos de tokens que se pueden emitir y cuál será su regulación en función del tipo que sea. Los tokens procedentes de las ICOs hasta el día de hoy han sido clasificados en dos grandes grupos (Mourselas, C)

1. **Utility tokens:** los utility tokens son aquellos en los que en principio su emisión no está directamente pensada a ser considerada como un instrumento o contrato de inversión. Este tipo de tokens da acceso a servicios u otras características dentro de una plataforma concreta. El problema de estos instrumentos es que posteriormente se pueden intercambiar en mercados secundarios y en mercados P2P como cualquier otro tipo de instrumento especulativo provocando que nuevamente puedan ser susceptibles de regulación.

Ejemplos claros de utility tokens son por ejemplo los de Ethereum o AEternity. Los tokens de estas dos plataformas están pensados para que los desarrolladores o empresas creen aplicaciones descentralizadas (o Dapps en inglés) a partir de ellos. Estos tokens tienen una utilidad directa que básicamente pretende dar un servicio concreto.

2. **Security tokens:** son aquellos que bajo las premisas de la SEC americana son considerados como "contratos de inversión" y que por lo tanto tienen o pueden tener fines puramente especulativos. En castellano no hay una definición clara de *security* en una sola palabra, pero según la Revista Española de Capital Riesgo, podemos considerar una "security" como "*Instrumento financiero emitido por una empresa, gobierno u otra organización que ofrece evidencia de deuda o Equity. Por ejemplo, acciones, obligaciones y bonos u opciones y futuros."* El problema aquí lo encontramos en que en casi la totalidad de las ICOs los tokens no reparten propiedad o *equity* de la empresa ni se pueden considerar como títulos de deuda. Esto convierte a este tipo de instrumentos en un modo de financiación completamente nuevo y disruptivo porque lo único que el participante obtiene a partir de esta inversión es el token.

   Como todos los tokens tienen implementados en su código contratos inteligentes estos pueden tener distintas características y derechos incorporados en ellos, como pueden ser derechos de voto, derecho a dividendos o rendimientos que genere la empresa… etc. Los smart contracts son completamente customizables a gusto de la empresa en cuestión lo que los convierte en instrumentos muy flexibles. El inversor adquirirá tokens siempre que vea que el protocolo en cuestión le convence y le es de utilidad.

   Para ser considerado como un contrato de inversión bajo la ley americana es necesario que pase el Howey Test, un test creado en el año 1964 y que determina que es y que no es considerado como una *security*. Por lo tanto, para que un activo sea considerado como *security* es necesario que el activo cumpla una serie de características entre las que se destacan que conlleve una inversión de dinero o de otros activos como activos de inversión, que el inversor espere que la inversión genere beneficios, que la inversión sea en una empresa común,

> que todo el beneficio provenga de un promotor o tercero, es decir que el inversor espere que todo el beneficio provenga de la actividad de un tercero y que el inversor tenga poder sobre la generación de beneficio del activo. Si el inversor tiene poder, probablemente no sea considerado como security, en el caso contrario sí. (Findlaw)

Esta corriente de pensamiento ha sido seguida cuasi unánimemente por todas las potencias a nivel mundial y es por ello que ya muchas instituciones están creando organismos o grupos que pretenden crear un marco regulatorio para poder controlar este tipo de inversiones con el objetivo de que el pequeño inversor no quede desprotegido.

A nivel España contamos con Alastria que es un consorcio formado por algunas de las instituciones con más poder de nuestro país que pretende no solo dar a conocer la tecnología a nivel general sino también ayudar al estado a crear un marco regulatorio que pueda ser de utilidad en el futuro. (Alastria, 2018). Siguiendo en nuestro país, a nivel público el informe más relevante es el publicado en Febrero de 2017 en el que la CNMV expone los riesgos que tienen este tipo de instrumentos financieros y repite un poco la fórmula de los dos tipos de tokens propuesta por la SEC.

A pesar del innegable poder disruptivo de la tecnología, todavía son ineficientes estos sistemas y queda mucho por optimizar. Uno de los problemas más graves que sufre está tecnología es la escalabilidad que limita su operatividad e implementación a gran escala.

7- El problema de la escalabilidad de las redes blockchain

Son muchos aquellos que de primeras han criticado Bitcoin diciendo que el sistema no es escalable, que, a mayor número de operaciones, mayor es la lentitud del sistema, lo que provoca que el sistema ya no sea una opción para implementar a niveles internacionales.

Digamos que el *benchmark* a batir en este caso sería VISA. Si somos capaces de llegar al nivel de transacciones que puede procesar VISA podemos suponer que el sistema es operable a nivel internacional y que se adapta a la demanda mundial que estos sistemas

de pagos pueden tener.

Otro problema a tener en cuenta es que ahora hay muchas personas que a día de hoy no tienen cuenta bancaria. Este número de gente asciende hasta los 2 billones de personas a nivel mundial (Hodgson, 2017). La gran revolución del blockchain permite que, a pesar de que esta gente no tenga cuenta bancaria, acceda a invertir en sistemas plataformas de inversión que utilizan estas u otras tecnologías, y que, por ejemplo, tengan una cartera digital o "wallet". Por poner un ejemplo, si un señor de la India que no tiene acceso a una cuenta bancaria, pero si a internet, mina la cryptomoneda X, al final tendrá acceso a un instrumento dinerario que se puede transaccionar en la red y que tiene un cierto valor económico. ¿Cuál es la consecuencia de todo esto? Que hay que tener presente que ya no es solo tener en cuenta la escalabilidad en función de las operaciones que se realizan hoy en día, sino que también tenemos que considerar que si en el mundo hay en torno a 7 mil millones de personas esto supone prácticamente que un 20% más de gente va a empezar a tener acceso a realizar transacciones y que por lo tanto el sistema debe ser lo suficientemente escalable como para absorber toda esta demanda potencial. Si no, nuevamente, el sistema será ineficiente y quedará obsoleto.

A día de hoy, VISA es capaz de realizar en torno a 50mil transacciones al segundo, siendo esta la máxima capacidad que tienen. Prácticamente en ninguna ocasión se llega a utilizar toda la utilidad ya que no se considera necesario, ni siquiera en época de compras. (VISA)

En principio, las redes que utilizan sistemas blockchain no llegan ni a aproximarse a estos números. Poniendo de ejemplo la capacidad de procesamiento de las dos criptodivisas con mayor capitalización Bitcoin procesa entre 3 y 6 transacciones por segundo y Ethereum: aproximadamente 15 transacciones por segundo.

Como podemos ver estos sistemas ni se acercan a la media diaria necesaria para poder garantizar que las transacciones internacionales son eficientes. Pero existen soluciones dentro del blockchain, o al menos eso es lo que plantean los desarrolladores de proyectos como Universa, AEternity o Credits.

Estas empresas alegan que uno de los principales problemas que presenta Bitcoin es la enorme cantidad de información que los nodos tienen que almacenar para poder operar en la red. Cuando una persona configura un nodo de Bitcoin o ETH tiene que

descargarse toda la blockchain, de tal manera que cuanta más información se almacena, más potente tiene que ser el ordenador para poder mantener el mismo nivel de exigencia. Esto normalmente no lo cumplen todos los nodos por lo que las transacciones se van cada vez ralentizando más y más.

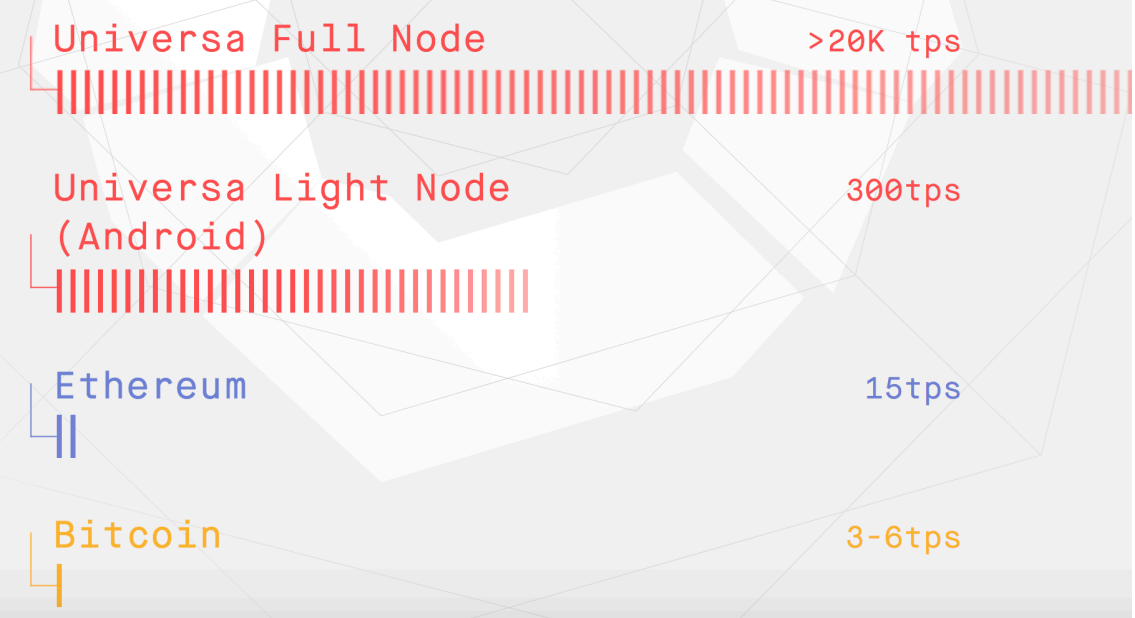

Figura 12. Comparativa de las transacciones por segundo entre los distintos protocolos blockchain. Recuperado de Universa Blockchain. (2018). *Universa Blockchain Protocol*. Recuperado de: https://universa.io/

Imagen procedente de la página web de Universa que pretende explicar las transacciones por segundo que ellos pueden realizar con su sistema en oposición a ETH y Bitcoin.

Otro de los proyectos que cambiará por completo el concepto que tenemos de Bitcoin es el llamado Lighting Network que básicamente lo que propone es no aumentar el tamaño de los bloques como argumentaban los desarrolladores de Bitcoin Cash para aumentar la velocidad, (SFOX, 2018) sino que lo que pretenden es hacer un cierto número de transacciones off-chain a través de Smart contracts. De esta manera el sistema se vuelve mucho más rápido y la blockchain estaría muchísimo menos saturada, permitiendo así un mayor número de transacciones por segundo.

Para resolver estos problemas de escalabilidad nacen proyectos, que, si bien están

inspirados inicialmente en sistemas de funcionamiento similares al blockchain, se postulan cómo una tecnología absolutamente nueva y disruptiva.

8- Nuevos sistemas alternativos al blockchain

Durante los últimos meses y fundamentalmente debido a problemas de escalabilidad de las redes de blockchain, han surgido dos ideas o conceptos que cada vez están cogiendo más fuerza y que, sobre todo, en palabras de empresarios y desarrolladores, puede llegar a dejar obsoleta la tecnología blockchain incluso antes de que esta se haya llegado a aplicar en la realidad.

Antes de empezar con el artículo, mi opinión personal es que aún queda mucho por desarrollar antes de entrar a valorar si estas tecnologías pueden suplantar al Blockchain y, sobre todo, si es verdad que blockchain no puede llegar a los mismos niveles de escalabilidad que sistemas como Hashgraph o Tangle. Proyectos como Lightning Network están ya trabajando para resolver este enorme problema. También encontramos dentro de este grupo de proyectos compañías como AEternity, Universia o Credits.

Con lo cual, si se diera el caso, una vez resuelto el problema de la escalabilidad, **¿Sigue siendo válido el argumento de la obsolescencia del blockchain?**

Empecemos entre tanto con el análisis de estas dos apasionantes tecnologías: Hashgraph y Tangle.

Hashgraph: Hashgraph es un sistema inventado por Leemon Baird, licenciado en *Computer Science* en la universidad de Carneggie Mellon University, emprendedor, consultor y también cofundador y CTO de la compañía *Swirlds*, empresa que implementa el uso de esta tecnología (Swirlds, 2016).

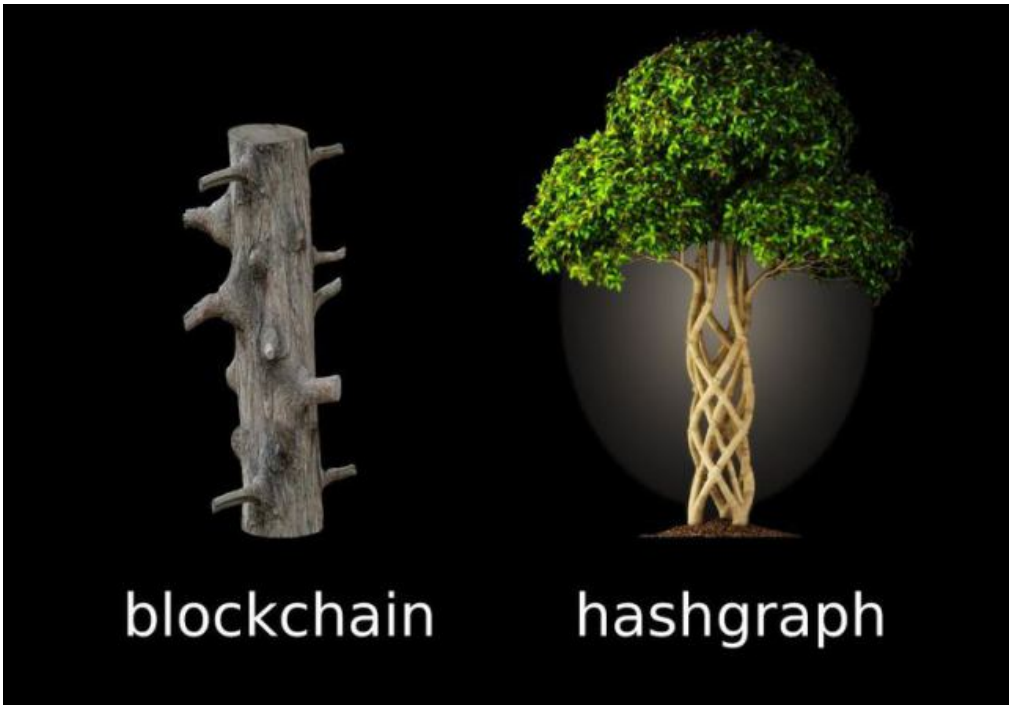

Figura 13. Comparativa gráfica entre blockchain y Hashgraph. Recuperado de SWIRLDS (2018). *HASHGRAPH CONSENSUS: DETAILED EXAMPLES*. Recuperado de: http://www.swirlds.com/downloads/SWIRLDS-TR-2016-01.pdf

Hashgraph se basa al igual que Tangle en el concepto matemático *directed acyclic graph*, o grafo directo acíclico en castellano, que se puede definir como un gráfico que no tiene ciclos, es decir que no constituye un circuito cerrado, pero sí posee una dirección concreta. (Techopedia).

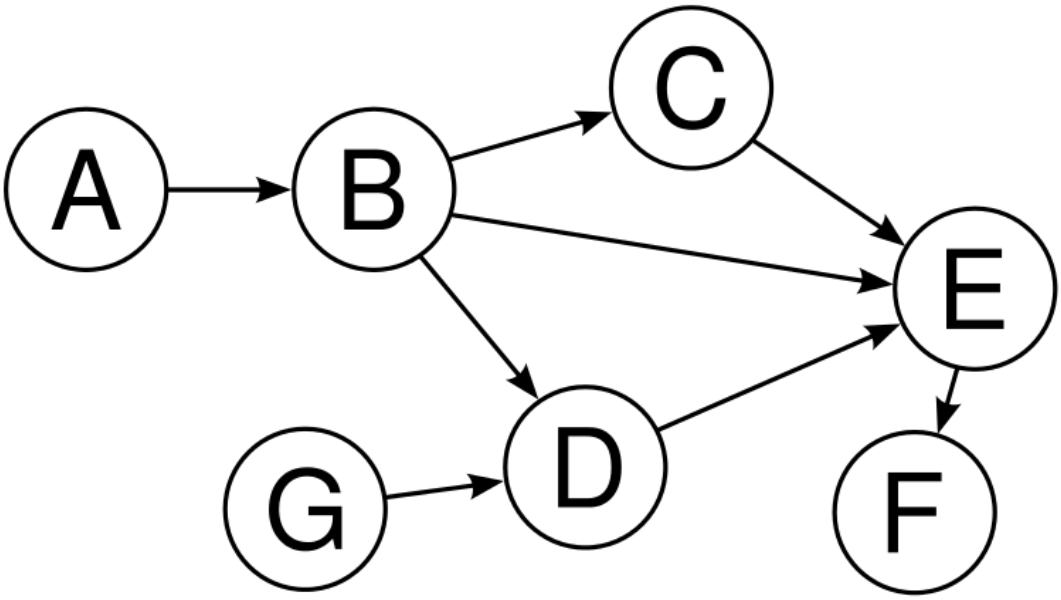

Figura 14. Representación de un grafo directo acíclico. Recuperado de SWIRLDS (2018). *HASHGRAPH CONSENSUS: DETAILED EXAMPLES*. Recuperado de: http://www.swirlds.com/downloads/SWIRLDS-TR-2016-01.pdf

Hashgraph por su parte es un algoritmo de consenso que ofrece los mismos beneficios que el blockchain pero que además permite hacerlo de una manera más justa, segura y rápida gracias a una técnica fundamental para este tipo de tecnología, *gossip consensus*.

Gossip Consensus o Gossip about Gossip: Este tipo de consentimiento o validación se basa en que los nodos distribuyen aleatoriamente en la red toda la información que saben, pero que él no sabe, de tal manera que este sistema es rápidamente escalable porque esto mismo lo van replicando todos los nodos creando un sistema cada vez más grande y eficiente. Así, los nodos se van transmitiendo pequeñas cantidades de información que, una encima de la otra, van creando una compleja red de validación. Los nodos transportan la información concerniente a las transacciones, pero también los dos hashes correspondientes a los eventos generados por ambos nodos.

Este sistema permite sobre todo atacar de manera directa el problema de la escalabilidad del Bitocin. Mientras Bitcoin procesa hasta 7 transacciones por segundo, un sistema Hashgraph puede procesar hasta 250.000 transacciones por segundo. Teniendo en

cuenta que empresas como Visa procesan en torno a 50.000, este sistema se debe de tener en cuenta para el futuro.

En términos de justicia en la red se podría decir que es más justo ya que no existe el sistema de proof of work en este tipo de red lo que implica por una parte que no hay mineros que tengan intereses en la red y por otra que no se consuman las ingentes cantidades de energía que se consumen con los sistemas de proof of work. Si bien es cierto que este problema ya está más o menos resuelto con el sistema de Proof of Stake, todavía muchas empresas de blockchain no han sido capaces de atacar el problema de la escalabilidad de la misma manera que Hashgraph, aunque aún se conciba a largo plazo el proyecto.

En términos de seguridad, se puede argumentar que es más seguro ya que ningún nodo puede controlar la blockchain ni impedir que se incluyan nuevos bloques en la plataforma. Igualmente, ningún miembro puede revertir las transacciones que ocurren en la blockchain. También es importante remarcar que en blockchain el minero tiene cierto control sobre el orden de las transacciones, ya que puede retrasar la entrada de la transacción o incluso nunca meterla. Esto en Hashgraph no ocurriría debido al sistema de consenso que implementan que provoca que las operaciones se registren según van ocurriendo en la red. (Danneman, 2017).

El sistema que utiliza Hashgraph para garantizar se llama por ellos mismos Asynchronous Byzantine Fault Tolerance, o en castellano, el BFT que tratamos al principio, pero asincronizado.

Uno de los mayores problemas que se le acusa a esta plataforma es el hecho de estar patentada, lo cual hace que la tecnología ya esté centralizada, y en un segundo punto y relacionado con el primero, el hecho de que no es de código abierto, lo que hace que esta tecnología no sea accesible a todo el mundo a diferencia de lo que ocurre con el blockchain. (Lansanta, 2017)

A continuación, podemos observar en la **Figura 15** la explicación gráfica de cómo funcionaría el sistema de Hashgraph.

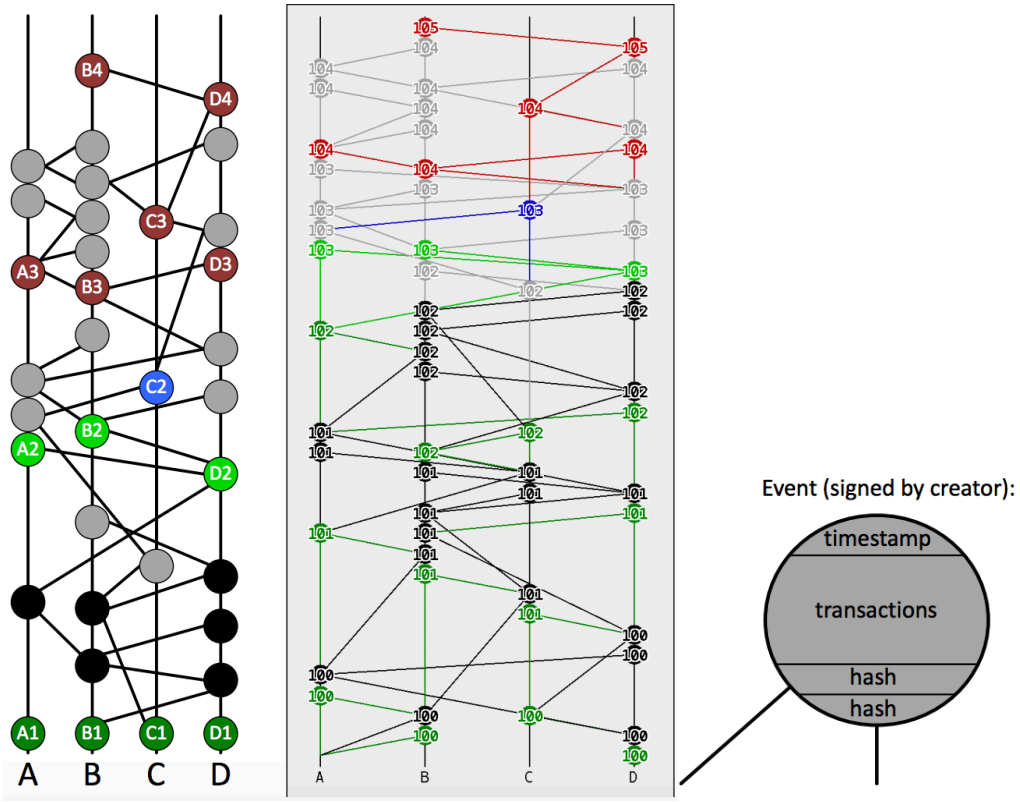

Figura 15. Red de Hashgraph (Hashgraph). Recuperado de SWIRLDS (2018). *HASHGRAPH CONSENSUS: DETAILED EXAMPLES*. Recuperado de: http://www.swirlds.com/downloads/SWIRLDS-TR-2016-01.pdf

Tangle: En respuesta a ciertos problemas que surgen las blockchains como la escalabilidad o la centralización del control de la plataforma que puede ocurrir cuando los mineros se alían, nace de la mano del protocolo IOTA una nueva tecnología de verificación denominada Tangle, pero, ¿en qué se diferencia Tangle de una blockchain al uso? En primer lugar, es importante decir que Tangle nace de la idea de automatizar el intercambio de información entre cosas u objetos, es decir, explotar la tendencia tecnológica del Internet of Things (IOT). Si ahora lás máquinas son capaces de transmitir información entre ellas, el propósito de IOTA es que también sean capaces de transmitir valor, creando un sistema financiero desarrollado por máquinas que intercambian activos monetarios. El protocolo se basa en el token IOTA y la tecnología Tangle. Esta tecnología no tiene bloques y cada participante en el mercado es responsable de verificar las transacciones de otros usuarios. En palabras de Colin Harper, columnista de la web CoinCentral "Visto como que toda transacción es responsable del éxito de la siguiente, no es necesario establecer un sistema de

comisiones ya que no hay una tercera parte involucrada". Aquí es donde cambia la historia con respecto al blockchain ya que IOTA utiliza una tecnología llamada Tangle que está basado en un concepto matemático llamado *directed acyclic graph* (o gráfico directo acíclico en castellano) al igual que comentábamos previamente con Hashgraph.

Vamos por partes: en primer lugar, a pesar de que IOTA se puede utilizar como cualquier otra criptodivisa del mercado, en principio está pensada para conectar dispositivos, y esta es la idea con la que nace el proyecto y que defiende fervientemente uno de sus cofundadores David Sonstebo. Por otra parte el Tangle en sí funcionaría como un ***entramado*** de validaciones en las que unas confirman a las precedentes.

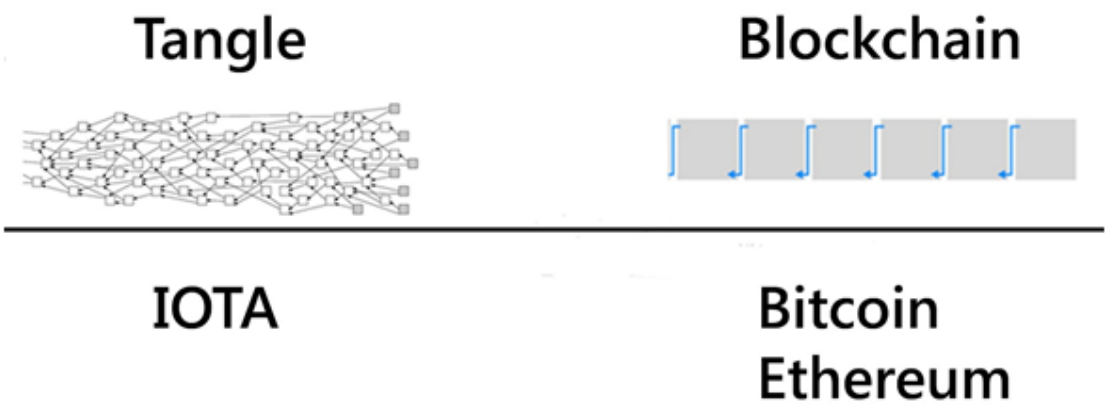

Figura 16. Diferencia entre la Tangle de IOTA y el sistema blockchain de Bitcoin o Ethereum (IOTA Support) Ukcryptocurrency.com. (2018). *Tangle vs Blockchain – UKcryptocurrency*. Recuperado de: https://ukcryptocurrency.com/iota/tangle-vs-blockchain/.

Para diferenciar bien entre lo que es la tecnología blockchain (como puede ser la de Bitcoin) de lo que es el sistema Tangle remarcamos sus características y diferencias principales:

- **Centralización**: Como decíamos antes, uno de los mayores problemas que ve Tangle con respecto a blockchain es el tema de que a pesar de que la red este

descentralizada, el hecho de que los mineros se agrupen en *pools* o grupos de inversión, provoca que al final la red se acabe convirtiendo en un espacio centralizado, por dos razones:

-

  - En primer lugar, aproximadamente el 75% de los bloques que se generan en la red Bitcoin son generados por los 8 *pools* más grandes del mundo. Si bien es verdad que todos parten de la base de garantizar la descentralización, si en cualquier momento quisieran agruparse podrían influir en el desarrollo de la red.
  - En segundo lugar, casi todos estos *pools* están localizados en China, lo que expone al inversor no solo al riesgo de la propia inversión sino también al riesgo regulatorio de un país como China. Si en China por ejemplo pasan a prohibir las criptomonedas, esto afectaría de manera dramática al desarrollo global de la red.

La solución que ellos proponen es simplemente la de cambiar este sistema por un sistema en el que no existan los bloques, y que cada transacción que tu realices sirva para validar dos transacciones aleatorias más. De esta manera si seguimos la cadena lo que podemos ir viendo es que constantemente se van validando más y más transacciones, creando un hilo de validaciones. De esta manera estás provocando que cuanta más gente hay en la red, más eficaz es el sistema.

- **Criptografía**: IOTA plantea el caso de que en el futuro existan algoritmos que permitan desencriptar la criptografía actual a través de ordenadores cuánticos. Si bien es verdad que esto todavía no existe, que exista en el futuro es una posibilidad que se debe contemplar y una medida preventiva que tiene que existir.

  Tangle por su parte dice ser *quantum resistant* de tal manera que ni cuando exista ese tipo de ordenadores se podrá hackear la red.

- **El problema de los micropagos:** en redes blockchain las *fees* son muy altas, o más que muy altas, son suficientemente altas como para que no se permitan realizar micropagos. Este es el propósito con el que nace IOTA en términos de eficiencia. La idea principal de este proyecto es que las máquinas se puedan pagar unas a otras cantidades ínfimas pero correspondientes con el precio que deberían de tener, haciendo que la estructura de cobros y pagos sea mucho más eficiente y no se quede dinero en intermediarios por el camino. IOTA no cobra comisiones para hacer este proceso posible.

- **Escalabilidad:** el problema de la escalabilidad se basa en la cantidad limitada de transacciones que una red de Bitcoin puede procesar en un tiempo determinado. Es un problema que se genera a la capacidad limitada de los bloques y al tiempo que se tarda en crear el bloque. Este es un problema que Tangle soluciona gracias a su estructura de validaciones

Diferencias básicas entre ambos sistemas (Phil- ZXX, 2017):

- IOTA es una criptodivisa, Hashgraph es un algoritmo. Hashgraph se asemejaría más a Tangle que a IOTA. IOTA utiliza Tangle para encontrar el consenso
- IOTA tiene código abierto, mientras que Hashgraph está patentado y no es de código abierto. Esto centraliza la tecnología como previamente discutíamos, pero no quiere decir que en el futuro no pueda pasar a ser de código abierto.
- IOTA requiere PoW para las verificaciones, Hashgraph no.
- En Tangle no hay un orden único de transacciones mientras que en Hashgraph esto sí que ocurre.

Estos son a día de hoy los dos sistemas que más opciones tienen de sustituir a la tecnología blockchain, pero sinceramente y en mi opinión personal son mucho más complejos de entender que el blockchain, lo que provoca que la gente desconfíe con mayor facilidad del sistema. El blockchain está ahora mismo en una de sus fases iniciales en cuanto a desarrollo tecnológico se refiere, y yo creo sin ningún tipo de duda que los problemas que intentan atacar Hashgraph y Tangle son problemas que en el

corto medio plazo empresas que operen bajo sistemas blockchain podrán cubrir sin mayores dificultades.

9- Conclusiones

Como conclusión al trabajo haré un breve análisis de cómo el estudio de la tecnología a lo largo del TFG me ha permitido valorar como está la situación hasta el día de hoy y como creo que va a evolucionar en el futuro próximo. Según lo que he expuesto en este TFG se ha podido ver que el potencial de esta tecnología es aún inimaginable y que el futuro pasa por la implementación de esta tecnología ya no solo a nivel privado sino también a nivel estatal e internacional. El estado de la tecnología todavía es muy prematuro y es por ello que prácticamente no hay ningún proyecto en actual funcionamiento.

Podemos extraer una serie de conclusiones tras el estudio de la tecnología. En primer lugar, el blockchain es efectivamente útil y revolucionario, los sistemas de registro habituales quedan obsoletos en todos los niveles en comparación con esta tecnología. Si bien es cierto que eso era algo que podía suponer antes de comenzar el trabajo, no ha sido hasta la efectiva realización de este cuando he visto realmente lo distinto que es comparado con los sistemas tradicionales y las numerosas ventajas que puede aportar

Todavía no conocemos el impacto del blockchain, pero sin lugar a dudas será enormemente disruptivo en todos los sectores, concretamente en el sector financiero, que es el que más hemos cubierto en este trabajo. Este enorme potencial de disrupción es debido al poco dinamismo el sector que ha mostrado en las últimas décadas. Sistemas como los de compensación y liquidación o de transferencias internacionales suponen un verdadero reto para las instituciones financieras a nivel mundial que han de reorganizarse internamente prácticamente en su integridad. Esto supondrá costes que el tiempo dirá si todas las empresas son capaces de cubrir. Igualmente, otra consecuencia directa de la implementación de la tecnología en las empresas financieras va a ser la remodelación ya no solo en términos departamentales sino también laborales. De implementarse y escalarse el uso de esta tecnología, los departamentos de *back office* pasan a ser prácticamente inservibles para las entidades financieras

Dentro de sistemas alternativos de registro distribuido, blockchain fue el primero que fue verdaderamente eficiente y utilizable, pero otros como Hashgraph y Tangle son alternativas muy válidas al blockchain, y en los próximos años veremos si pueden ser complementarias u opuestas. Lo cierto es que yo, tras ver los pros y los contras de ambas, creo que en el futuro veremos cómo coexisten ambos sistemas de registro distribuido.

El mayor problema del blockchain es la escalabilidad, pero lo cierto es que todavía no ha habido tiempo suficiente de que las empresas desarrollen y prueben la tecnología en profundidad. Desde las esferas internacionales se pretende que el blockchain de, desde mañana mismo, soluciones a escala global cuando apenas tiene 10 años de historia y menos de 5 de investigación intensa por parte de organismos tanto públicos como privados. Sin la cooperación pública la iniciativa privada no tiene sentido ya que muchos de los procesos e ideas que hemos descrito previamente actualmente chocan de manera frontal con los requerimientos y regulaciones que existen a nivel internacional.

Lo que sí que se está viendo y que se refleja a lo largo del trabajo es que tanto los países como las organizaciones internacionales si bien es verdad que en ciertos casos están poniendo trabas al desarrollo de la tecnología, en la gran mayoría de los casos están afrontando la legislación, regulación y control de este tipo de actividades e inversiones de manera positiva. Al no tener un centro único de control el blockchain se convierte en una tecnología incontrolable a nivel estatal, con lo que yo estoy de acuerdo en que los estados se adapten y regulen el sistema, ya que, si no corremos el riesgo de crear dos sociedades paralelas, una viviendo en blockchain y otra estatal que vive al margen de este.

La combinación de los smart contracts con la tecnología blockchain es la verdadera revolución y darnos cuenta de esto es el mayor valor que puede aportar este TFG. En el momento en que como conscientes del enorme potencial de esto podemos ponernos en un plano superior y observar con perspectiva la cantidad de procesos que se simplifican, los costes que se ahorran y la simplicidad que otorga estos sistemas combinados correctamente. Los smart contracts permiten automatizar contratos eliminando por tanto

la intervención humana, si este proceso se escala a nivel mundial e institucional puede suponer una revolución en muchos sectores.

Como decíamos previamente el mayor reto a nivel mundial es el largo proceso de implementación e investigación de esta tecnología y la sustitución de los sistemas tradicionales de una manera fluida y segura para las personas y empresas.

Por último, a pesar de lo buena o útil que sea la tecnología la evolución e implementación de esta ha de ser gradual. Queda mucho por avanzar, mucho por investigar y mucho tiempo antes de que veamos a organizaciones y sociedades enteras operando a través de blockchain. El interés y la inversión en esta tecnología hasta el día de hoy ha sido enorme, pero solo será a través de la cooperación estatal con el mundo privado cuando la implementación del blockchain en la sociedad se podrá convertir en una realidad.

10- Anexo

En relación con lo dispuesto anteriormente en el punto 2, considero que es interesante añadir la estructura de código básica de un smart contract, aunque sea simplemente a efectos de mera ampliación de conocimiento. Un smart contract básico ERC20 desarrollado bajo código Ethereum tendría el siguiente aspecto (Ethereum):

1- contract **ERC20** {
2- function **transfer(address _to, uint256 _amount)** returns (bool success);
3- function **transferFrom(address _from, address _to, uint256 _amount)** returns (bool success);
4- function **balanceOf(address _owner)** constant returns (uint256 balance);
5- function approve(address _spender, uint256 _amount) returns (bool success);
6- function allowance(address _owner, address _spender) constant returns (uint256 remaining);
7- function **totalSupply()** constant returns (uint);
8- }

11- Bibliografía

Accenture. (2018). Banking on Blockchain. Recuperado de: https://www.accenture.com/t20170120T074124Z__w__/us-en/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Consulting/Accenture-Banking-on-Blockchain.pdf

Akolkar, B (2018). The First Day of Venezuela ‘s ‘Petro’ Token Sale Boasts $735M Raised – CoinSpeaker. Recuperado de: https://www.coinspeaker.com/2018/02/21/first-day-venezuelas-petro-token-sale-boasts-735m-raised/

Alastria.io. (2018). Alastria - National Blockchain Ecosystem. Recuperado de: https://alastria.io/

Alkan, C. V. (2018). Decentralized Objective Consensus without Proof-of-Work. Recuperado de: https://hackernoon.com/decentralized-objective-consensus-without-proof-of-work-a983a0489f0a

Anon, (2018). Influence the order and timestamps that are agreed. = A B. Recuperado de: http://www.swirlds.com/downloads/SWIRLDS-TR-2016-02.pdf

Arnold, M (2018). Five ways banks are using blockchain. Recuperado de: https://www.ft.com/content/615b3bd8-97a9-11e7-a652-cde3f882dd7b

Arroyo, M. y Bastardo, J. (2018). 10 cosas que debes saber sobre el Petro, el criptoactivo creado por el Estado venezolano. CriptoNoticias - Bitcoin, Blockchain y criptomonedas. Recuperado de: https://www.criptonoticias.com/adopcion/10-cosas-debes-saber-sobre-petro-criptoactivo-creado-estado-venezolano/.

Banco Central Europeo (2018). Funciones del Banco Central Europeo. Recuperado de: https://www.ecb.europa.eu/ecb/tasks/html/index.es.html

Banco Central Europeo (2018). The Correspondent Central Banking Model CCBM. European Central Bank. Recuperado de: https://www.ecb.europa.eu/mopo/assets/ccbm/html/index.en.html

Bartlett, J. (2015). The Dark Net: Inside the Digital Underworld. Melville House

Bit2Me • El Blog de Bitcoin. (2018). Minar Bitcoins, ¿En que consiste y cómo funciona? Recuperado de: https://blog.bit2me.com/es/que-es-minar-bitcoins/

Bitcoinwiki (2018). Scalability in Bitcoin - Bitcoin Wiki. Recuperado de: https://en.bitcoin.it/wiki/Scalability

Buterin, V. (2018). Mastercoin: A Second-Generation Protocol on the Bitcoin Blockchain. Bitcoin Magazine. Recuperado de: https://bitcoinmagazine.com/articles/mastercoin-a-second-generation-protocol-on-the-bitcoin-blockchain-1383603310/

Cardano. (2018). Ouroboros Proof of Stake Algorithm. Recuperado de: https://cardanodocs.com/cardano/proof-of-stake/

Ciaian, P., Rajcaniova, M., y Kancs, D. A. (2016). The economics of BitCoin price formation. Applied Economics, 48(19), 1799-1815.

Coin and Crypto (2018). 5 alarming reasons Ripple might not be what you think. Recuperado de: https://hackernoon.com/4-alarming-reasons-ripple-might-not-be-what-you-think-9debc3c86985

Danneman, J. (2018) Blockchain just became obsolete, Hashgraph is here. Recuperado de: https://squawker.org/technology/blockchain-just-became-obsolete-the-future-is-hashgraph/

Del Rio, C. A. (2017). Use of distributed ledger technology by central banks: A review. Enfoque Ute.

Deloitte (2017). Key Charactheristics of blockchain. Convergence2017. Recuperado de: https://www2.deloitte.com/content/dam/Deloitte/in/Documents/industries/in-convergence-blockchain-key-characteristics-noexp.pdf

Downes, B. (2018). Overview y Analysis of ICO Regulatory Developments - Smith + Crown. Smith + Crown. Recuperado de: https://www.smithandcrown.com/overview-analysis-ico-regulatory-developments/

Draupnir, M (2016). What is the Bitcoin Mining Block Reward? Bitcoinmining.com. Recuperado de: https://www.bitcoinmining.com/what-is-the-bitcoin-block-reward/

EACH - European Association of CCP Clearing Houses. (2018). Members - EACH - European Association of CCP Clearing Houses. Recuperado de: http://www.eachccp.eu/members/

Esteve, V., Navarro-Ibáñez, M., y Prats, M. A. (2017). The gold standard and the euro: A reflection from a reading of A Tract on Monetary Reform. Cuadernos de Economía, 40(114), 247-255.

Finley, K., Rogers, A., Vogelstein, F., Geltzer, J. y Eden, S. (2018). IBM to Quit Making PCs. WIRED. Recuperado de: https://www.wired.com/2004/12/ibm-to-quit-making-pcs/

Gobierno de Venezuela. (2018). Whitepaper o Papel Blanco de Petro. Recuperado de http://www.elpetro.gob.ve/pdf/esp/Whitepaper_Petro_es.pdf

Gomez, F. (2018). Proof of Work vs Proof of Stake - Comparativa entre PoW y PoS. Recuperado de: http://www.criptomania.com/proof-of-work-vs-proof-of-stake/

Gord, M (2018). Smart Contracts Described by Nick Szabo 20 Years Ago Now Becoming Reality. Recuperado de: https://bitcoinmagazine.com/articles/smart-

contracts-described-by-nick-szabo-years-ago-now-becoming-reality-1461693751/

Hernández, M., Orbyt, E., Vivienda, S., TV, G., inmobiliarias, I., Byuacute;ho, E., Sergio, R., Plus, C., Myeacute;dico, D., Marca, A., eSports, M., Editorial, E., Editorial, U., Empleo, E. and Editorial, E. (2018). Más de 300.000 accionistas de Banco Popular han perdido toda su inversión. ELMUNDO. Recuperado de: http://www.elmundo.es/economia/empresas/2017/06/07/5937c259e2704e3c378b4585.html

Hiesboeck, M (2018). Blockchain is the most disruptive invention since the Internet itself and not just in finance. Recuperado de: https://www.digitaldoughnut.com/articles/2016/april/blockchain-is-the-most-disruptive-invention-since

Higgins, Stan (2018). Former Estonian President to Lead World Economic Forum Blockchain Group - CoinDesk. Recuperado de: https://www.coindesk.com/estonia-president-world-economic-forum-blockchain/

Hodge, M. (2018). Who is Satoshi Nakamoto? Bitcoin inventor whose identity remains a secret. The Sun. Recuperado de: https://www.thesun.co.uk/news/5037060/satoshi-nakamoto-bitcoin-inventor-richest-world/

Hodgson, C. (2018). The world's 2 billion unbanked, in 6 charts. Business Insider. Recuperado de: http://uk.businessinsider.com/the-worlds-unbanked-population-in-6-charts-2017-8/#the-vast-majority-94-of-adults-in-oecd-high-income-countries-said-they-had-a-bank-account-in-2014-while-only-54-of-those-in-developing-countries-did-the-middle-east-had-the-lowest-proportion-of-account-holders-with-only-14-on-average-1

IBM (2018). Blockchain Center in Singapore brings innovation to finance and trade - IBM Blog Research. Recuperado de:

https://www.ibm.com/blogs/research/2016/07/bringing-blockchain-innovation-singapore-asia/

ICO Watch List. (2018). Section 3: History and evolution of ICOs - ICO Education | ICO Watch List. Recuperado de: https://icowatchlist.com/education/history-and-evolution-of-icos

Icodata.io. (2018). ICOdata - ICO 2016 Statistics. Recuperado de: https://www.icodata.io/stats/2016

Icoinversiones.com. (2017). Mapa ICOs España – Ico Inversiones | Bitcoin y Criptomonedas. Recuperado de: http://icoinversiones.com/mapa-icos-espana/

Investopedia (2018). Society for Worldwide Interbank Financial Telecommunications - SWIFT. Investopedia. Recuperado de: https://www.investopedia.com/terms/s/swift.asp

Investopedia (2018). What is a Clearing House? Recuperado de: https://www.investopedia.com/terms/c/clearing house.asp

Iota.org. (2018). IOTA - Next Generation Blockchain. Recuperado de: https://iota.org/

JD Supra. (2018). The 4 Types of Blockchain Networks Explained | JD Supra. Recuperado de: https://www.jdsupra.com/legalnews/the-4-types-of-blockchain-networks-83225/

Kariuki, D. (2018). Alternatives to Proof of Work. Recuperado de: http://www.cryptomorrow.com/2017/08/28/alternatives-to-proof-of-work/

Kharif, O. (s.f.). Blockchain Is Pumping New Life Into Old-School Companies Like IBM y Visa. Recuperado de https://www.bloomberg.com/news/articles/2017-12-26/blockchain-pumping-new-life-into-old-school-companies-like-ibm

Khatwani, S. (2018). What Are Private Blockchains y How Are They Different from Public Blockchains? Recuperado de: https://coinsutra.com/private-blockchain-public-blockchain/

Konstantopoulos, G. (2018). Understanding Blockchain Fundamentals, Part 1: Byzantine Fault Tolerance. Recuperado de: https://medium.com/loom-network/understanding-blockchain-fundamentals-part-1-byzantine-fault-tolerance-245f46fe8419

Koranyi, B., y Evans, C. (2017). Blockchain immature for big central banks, BCE and BOJ say » Reuters. Recuperado de: https://www.reuters.com/article/us-blockchain-ecb/blockchain-immature-for-big-central-banks-ecb-and-boj-say-idUSKCN1BH2DH

Leising, M., & Robinson, E. (2018). All Eyes on Ripple. But What Is It?. Bloomberg Businessweek, (4556), 29-31.

Leloup, L (2018). The Rise of Bitcoin, the Birth of ICOs and the Future of Cryptocurrency. Recuperado de: https://www.finance-monthly.com/2018/01/the-rise-of-bitcoin-the-birth-of-icos-and-the-future-of-cryptocurrency/

Lightning.network (2018). Scalable, Instant Bitcoin/Blockchain Transactions. Recuperado de: https://lightning.network/

Maguire, S (2018). A List Of Countries With National Cryptocurrencies - Bitcoin Hub. Recuperado de: https://bitcoinhub.co.za/list-countries-national-cryptocurrencies/

Marr, B. (2017). Forbes Welcome. Recuperado de: https://www.forbes.com/sites/bernardmarr/2017/08/10/practical-examples-of-how-blockchains-are-used-in-banking-and-the-financial-services-sector/#45c642a41a11

McKinsey y Company. (2018). How blockchains could change the world. Recuperado de: https://www.mckinsey.com/industries/high-tech/our-insights/how-blockchains-could-change-the-world

Meola, A. (2017). How banks and financial institutions are implementing blockchain technology. Business Insider. Recuperado de: http://www.businessinsider.com/blockchain-technology-banking-finance-2017-9

Mik E. (2017) Smart contracts: terminology, technical limitations and real world complexity. Law, Innovation y Technology. Recuperado de: Academic Search Complete, Ipswich, MA.

Mik, E. (2017). Smart contracts: terminology, technical limitations and real world complexity. Law, Innovation and Technology, 9(2), 269-300.

Momoh, O. (2018). Proof of Stake (PoS). Investopedia. Recuperado de: https://www.investopedia.com/terms/p/proof-stake-pos.asp

Moore, F. (2018). Central banks are experimenting with blockchain technology — here's why. Business Insider. Recuperado de: http://uk.businessinsider.com/why-central-banks-using-blockchain-technology-could-be-beneficial-2018-1

Mougayar. M. (2018). Understanding Semi-private Blockchain Applications. Recuperado de: https://medium.com/@wmougayar/understanding-semi-private-blockchain-applications-6bbe91fc3596

Mourselas, C. (2017). ESMA warns ICOs may be covered by EU securities laws. Globalcapital, 19.

Naiz, T. (2018). History of the ICO Ecosystem: Top ICOs of 2017. BTCMANAGER. Recuperado de: https://btcmanager.com/history-ico-ecosystem-top-icos-2017/

Nakamoto, S. (2009). Bitcoin: A peer-to-peer electronic cash system. bitcoin.org. Recuperado de: https://bitcoin.org/bitcoin.pdf

NASDAQ.com. (2018). Byzantine Fault Tolerance: The Key for Blockchains. Recuperado de: http://www.nasdaq.com/article/byzantine-fault-tolerance-the-key-for-blockchains-cm810058

Nxt. (2018). Russia's central securities depository uses Nxt blockchain. Recuperado de: https://nxtplatform.org/russias-central-securities-depository-uses-nxt-blockchain-voting/

Orcutt, M. (2018). A cryptocurrency without a blockchain has been built to outperform bitcoin. MIT Technology Review. Recuperado de: https://www.technologyreview.com/s/609771/a-cryptocurrency-without-a-blockchain-has-been-built-to-outperform-bitcoin/

Palmer, D (2018). $850 Million Raised in ICO So Far, Says Telegram - CoinDesk. Recuperado de: https://www.coindesk.com/850-million-raised-in-ico-so-far-says-telegram/

Pasztor, J. (2018). Bitcoin Investing--An Ethical and Regulatory Quandary. *Journal Of Financial Service Professionals*, *72*(2), 30-33.

PwC. (2017). Global FinTech Report 2017. Recuperado de: https://www.pwc.com/jg/en/publications/pwc-global-fintech-report-17.3.17-final.pdf

Ridley, S. A. (2008). Regulation of Securities Trading (MiFID) and The Evolution of Exchanges, Clearing & Settlement. Financial Markets, Institutions & Instruments, 17(1), 121-136. doi:10.1111/j.1468-0416.2007.00137x.

Ripple. (2018). Banks - Global Payment Uses Cases | Ripple. Recuperado de: https://ripple.com/use-cases/banks/

Rosic, A (2018). Proof of Work vs Proof of Stake: Basic Mining Guide. Recuperado de: https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/

Santander Innoventures. (2015). The Fintech 2.0 Paper: rebooting financial services. Recuperado de: http://santanderinnoventures.com/wp-content/uploads/2015/06/The-Fintech-2-0-Paper.pdf

Seth, S. (2018). How the SWIFT System Works. Investopedia. Recuperado de: https://www.investopedia.com/articles/personal-finance/050515/how-swift-system-works.asp

Sherry, B. (2018). What Is An ICO? Investopedia. Recuperado de: https://www.investopedia.com/news/what-ico/

Skinner, C. (2018). The Finanser Interviews: Gottfried Leibbrandt, Chief Executive Officer, SWIFT - Chris Skinner's blog. Chris Skinner's blog. Recuperado de: https://thefinanser.com/2015/09/the-finanser-interviews-gottfried-leibbrandt-chief-executive-officer-swift.html/

Small, S. (2015). BITCOIN: THE NAPSTER OF CURRENCY. *Houston Journal Of International Law*, *37*(2), 581-641.

Stafford, P. (2018). FT Explainer: The blockchain and financial markets. Recuperado de: https://www.ft.com/content/454be1c8-2577-11e5-9c4e-a775d2b173ca

Stokes. M y Freire Ramos. G (2017). Smart Contracts. Actualidad Juridica (1578-956X), (46).

Swirlds (2018). Hashgraph consensus: Detailed examples. Recuperado de: http://www.swirlds.com/downloads/SWIRLDS-TR-2016-01.pdf

Treasurytoday.com. (2018). Ripple vs SWIFT: payment (r)evolution | Treasury Today. Recuperado de: http://treasurytoday.com/2017/07/ripple-vs-swift-payment-r-evolution-ttpv

Ukcryptocurrency.com. (2018). Tangle vs Blockchain – UKcryptocurrency. Recuperado de: https://ukcryptocurrency.com/iota/tangle-vs-blockchain/

Urrutia, C. (2018). Más de 10 millones de empleos y un 4% del PIB de la UE: El multimillonario e imparable negocio de los datos. ELMUNDO. Recuperado de: http://www.elmundo.es/economia/macroeconomia/2018/03/25/5ab6407de2704e7c518b4643.html

Vermuelen, J. (2017). Bitcoin and Ethereum vs Visa and PayPal – Transactions per second. Recuperado de https://mybroadband.co.za/news/banking/206742-bitcoin-and-ethereum-vs-visa-and-paypal-transactions-per-second.html