



Facultad de Ciencias Económicas y Empresariales

**LA IMPLEMENTACIÓN DEL
BLOCKCHAIN Y LAS CRIPTODIVISAS
EN EL SISTEMA FINANCIERO Y LAS
FINTECH.**

Autor: Gonzalo Jesús Sánchez Ríos.

Tutor: Javier Rivas Compains.

Clave: 201705580

MADRID | Junio de 2022

Índice

Resumen.....	1
Abstract.....	1
1. Introducción.....	2
2. La tecnología Blockchain.....	4
2.1.1. Tipos de redes blockchain.....	6
2.1.2. La firma digital.....	8
2.1.3. La minería.....	9
2.1.4. El Consenso.....	9
3. Las criptomonedas.....	13
3.1. Clasificación de las criptomonedas.....	13
3.2. Criptomonedas más relevantes.....	16
4. FinTechs.....	27
5. Implementación de las redes Blockchain en el sistema financiero.....	30
5.1. Blockchain en las transferencias interbancarias.....	30
5.2. Financiación de empresas a través de ICOs.....	32
5.3. Otras mejoras.....	34
6. Futuros retos y obstáculos de la tecnología blockchain.....	37
7. Consideraciones.....	39
8. Conclusiones.....	41
Bibliografía.....	47

Resumen.

El vertiginoso crecimiento de la tecnología Blockchain y el cada vez más habitual uso de las Criptomonedas como elemento de transacción en las operaciones del mercado y como método de inversión, hace necesario el análisis y estudio de como esta tecnología se está abriendo paso y adquiriendo un muy relevante papel dentro del sistema financiero “tradicional” y en el ámbito de las Fintech.

De esta forma, el objetivo de este trabajo es estudiar el funcionamiento de la tecnología Blockchain, la aplicación que esta puede tener en los sistemas financiero y el funcionamiento de los mercados, así como el estudio del concepto de la criptomoneda, los diferentes y más relevantes tipos de criptomonedas existentes junto a una evaluación de los diferentes proyectos tras estas criptomonedas y el papel que estas tienen y pueden llegar a tener en los sistemas financieros.

Palabras clave: Blockchain, criptomonedas, finanzas, Fintech

Abstract.

The dizzying growth of Blockchain technology and the increasingly common use of cryptocurrencies as a transaction element in market operations and as an investment method, makes it necessary to analyze and study how this technology is making its way and acquiring a truly relevant role within the "traditional" financial system and in the field of Fintech.

Thus, the objective of this work is to study the functioning of Blockchain technology, the application it can have in the financial systems and the functioning of the markets, as well as the study of the concept of cryptocurrency, the different and most relevant types of existing cryptocurrencies together with an evaluation of the different projects behind these cryptocurrencies and the role they have and can have in the financial systems.

Key words: Blockchain, cryptocurrencies, finance, Fintech

1. Introducción.

El sistema financiero tradicional ha estado dominado históricamente por grandes entidades bancarias que establecían sus propias reglas del juego a las cuales las personas debían someterse si quería formar parte del necesario sistema financiero. Aunque hoy en un alto grado las entidades financieras juegan un papel esencial, surge en 2008, una revolucionaria idea que pretendió cambiar el statu quo e implementar un sistema que permitiera desplazar a las entidades financieras y establecer un procedimiento fiable y seguro que conectara a las personas, la tecnología blockchain.

Este trabajo nace con el objetivo de profundizar en el estudio de las redes blockchain, una de las tecnologías con mayor potencial disruptivo de los últimos años. Estudiaremos las distintas posibilidades de transformación que las redes blockchain tienen en el sector financiero y con respecto a las Fintech, y su posible contribución a mejorar los procesos y sistemas en los que se basa la economía mundial.

Hoy en día, disponemos de una extensa literatura acerca de la tecnología blockchain, por lo que dedicaremos la parte inicial de este trabajo, a realizar una revisión de esta para poder arrojar claridad acerca del propio concepto de la tecnología blockchain, su origen y tratar de explicar su funcionamiento para poder comprender las distintas implicaciones que estudiaremos más adelante.

Analizaremos los diferentes tipos de redes existentes y los conceptos en los que se basan para poder establecer diferencias entre las principales redes actuales y tratar de concluir acerca de los proyectos con mayor potencial.

Posteriormente, estudiaremos el concepto de Fintech una relativamente novedosa forma de aplicar la tecnología al sistema financiero que abre un gran abanico de posibilidades a la implementación de la tecnología blockchain a los servicios financieros.

Uno de los pilares de este trabajo, consiste en estudiar las posibles implementaciones que la tecnología blockchain tiene en la transformación del sistema financiero actual. De esta forma, analizaremos el papel que juega esta tecnología en las transacciones internacionales y como puede optimizar y hacer más eficiente los movimientos de capital. Estudiaremos también como la tecnología blockchain emerge

como una inédita forma de financiación para nuevos proyectos (ICOs), que ofrecen nuevas posibilidades para novedosos proyectos sobre todo en el mundo de las start ups.

Finalizaremos el trabajo haciendo un análisis de los obstáculos a los que actualmente se enfrenta la tecnología blockchain y los aspectos que un futuro pueden poner en peligro la implementación de esta tecnología.

Para la elaboración de este trabajo, nos apoyaremos en la metodología deductiva. Utilizaremos fuentes secundarias de investigación a través de técnicas cualitativas. En concreto, acudiremos a la revisión no sistemática de fuentes de investigación, bases de datos y publicaciones académicas para obtener la información necesaria que permita la elaboración de este trabajo.

2. La tecnología Blockchain.

El concepto de blockchain como tal no es fácil de definir en una cuantas palabras o líneas, una tecnología tan compleja y disruptiva requiere de un análisis parte por parte de todos los conceptos que la conforman para poder llegar a comprender y definir verdaderamente su utilidad y potencial.

Si queremos ofrecer una definición que nos permita hacernos una primera idea de que es el blockchain, podríamos decir que es una base de datos distribuida entre “varios” participantes (nodos), que se encuentra protegida criptográficamente y cuyos datos están organizados y almacenados en bloques relacionados entre sí matemáticamente (Kuchovsky, Gómez, Díez, & Molero, 2017).

Son muchas las características que han provocado el enorme crecimiento e implantación de esta tecnología en casi todos los sectores de la economía y en la vida en general, pues encontramos aplicaciones del blockchain en el campo de la medicina, el derecho, etc. Por ello, vamos a comenzar analizando estos atributos que hacen de esta tecnología una fuerza disruptiva que puede cambiar la forma en la que entendemos el mundo.

*Las redes blockchain permiten la gestión de datos, órdenes, transacciones, activos y tokens, mediante un sistema de registro **distribuido** y **descentralizado** que se anota en bloques de información que se encadenan secuencialmente creando una cadena de bloques o registros **inmutable e inalterable**, **compartida** colaborativamente entre todos los miembros de cada red de blockchain, y que son verificados por dichos miembros de la red, actuando como «nodos» de la misma. De esta forma, se crea un procedimiento de registro, que funciona mediante criptografía **consensual**, en modo equivalente a un libro contable —en este caso digital—, del que hay tantas copias idénticas como miembros de la red (Palomo-Zurdo, 2018).*

Esta definición que nos ofrece PALOMO-ZURDO sobre que es la tecnología blockchain pone de manifiesto alguna de las características que hacen único a este sistema de gestión y almacenamiento de la información.

- Son redes **distribuidas**.
- Son redes **descentralizadas**.

- Son redes **compartidas**.
- Ofrecen un registro de información **inmutable e inalterable**.

Por **distribuido**, entendemos que todas estas transacciones que se producen en las redes blockchain se producen y replican en cada uno de los nodos que forman parte de la red, siendo estos recompensados por su participación y colaborando con la veracidad y confianza de las transacciones y la veracidad de estas.

Por otro lado, el hecho de que sea un sistema **descentralizado** implica que no hay ningún tipo de entidad o persona jerárquicamente superior a los nodos que participan en las redes, la información está en manos de todos los nodos y no hay ningún participante que tenga el monopolio o en control exclusivo sobre esta información. Además, el hecho de que la red sea descentralizada implica que los servicios o las aplicaciones desarrolladas sobre la red van a continuar estando disponibles, aunque un servidor o grupo de servidor fallara o dejara de funcionar, lo cual tiene grandes implicaciones en la eficiencia y seguridad de este tipo de red (Modi, 2018)

La **inmutabilidad e inalterabilidad** de la información recogida en este tipo de redes es uno de los elementos de mayor valor de esta tecnología ya que es uno de los pilares en los que se basa este sistema, la confianza en que la información es veraz y que ninguna persona u organización va a poder modificarla. Más adelante, explicaremos como se consigue que esta información se mantenga inalterada a pesar de las grandes amenazas a las que está sometida.

La **criptografía consensual** es el elemento fundamental que permite que todos estos sistemas funcionen, es la forma en la que todos los participantes, los nodos, se pongan de acuerdo en que la información incluida en la red es válida y veraz para que esta pueda ser registrada en la red y constituya unos de los bloques de la cadena.

Aunque son dos conceptos absolutamente entrelazados debemos hacer una distinción y analizar por un lado que es la criptografía y por otro que es el consenso, para poder llegar a comprender mejor en qué consiste esta criptografía consensual.

Entendemos por criptografía el proceso a través del cual, por medio de un algoritmo o clave de cifrado, un mensaje es transformado sin tener en cuenta el

contenido del propio mensaje para que sea lo más difícil de entender para aquella persona que no sepa descifrar el algoritmo, es decir, aquella que no disponga de la clave de descifrado (Kuchovsky, Gómez, Díez, & Molero, 2017). Aquí es donde entra en juego la popular función *hash*, que es un algoritmo matemático que transforma una cadena de bits de cualquier tamaño en una cadena de bits de un tamaño fijo sin poder acceder a la cadena original después de ser transformada (Zozaya, Franzoni, & Incera, 2017). Lo que hace la función hash es dividir el contenido de la información que ha de procesar en bloques de caracteres y someter cada uno de estos bloques a un proceso de encriptación creando un código alfanumérico, que está compuesto por un bloque que hace referencia al hash anterior, el propio hash generado y un *nonce*¹ (number that can only be used once) que se añade como medida de seguridad.

Tras este procedimiento de codificación de la información tiene lugar el proceso de minado a través del cual los nodos validan y agrupan la información en bloques que posteriormente son incorporados a la cadena de bloques.

Después de haber llevado a cabo ambos procesos, todos los nodos deben de ponerse de acuerdo sobre la veracidad de la información registrada y ahí es cuando aparece el segundo de los elementos dentro de la criptografía consensual, el consenso.

El consenso es una parte fundamental del blockchain que se sustenta en un protocolo común dentro de la red a través del cual se verifican y confirman información y se asegura la irreversibilidad de esta y, además proporciona a cada uno de los usuarios una copia de todas las operaciones realizadas en la red (Kuchovsky, Gómez, Díez, & Molero, 2017).

2.1.1. Tipos de redes blockchain.

Habiendo analizado las características más importantes del blockchain es importante conocer los diferentes tipos de redes blockchain y las diferencias que existen entre ellas. En este sentido, encontramos una clasificación que distingue tres tipos de redes: públicas, privadas e híbridas.

Las públicas fueron las primeras redes blockchain que existieron y son aquellas que son accesibles en internet para cualquier persona, como, por ejemplo, las redes en

¹ El nonce funciona en combinación con el hash como un elemento de control para evitar la manipulación de la información de los bloques.

las que esta soportado Bitcoin o Ethereum. Las características más importantes de las redes públicas son:

- Permiten que cualquier persona pueda formar parte de la red sin restricciones.
- La red funciona de una forma completamente abierta y transparente estando todos los datos desde el inicio de la red disponible a cualquier persona.
- No hay entidades centralizadas que controlen la información y regulen cómo funciona la red.
- Este tipo de red se mantiene económicamente depende del propio sistema de la red y por el cobro de las comisiones por las transacciones en la red. (Bit2me, 2022)

Al ser redes abiertas, cualquier persona con los conocimientos suficientes puede tener acceso a los datos, el software y el desarrollo de esta red, lo cual se puede observar desde dos puntos de vista diametralmente opuestos. Por un lado, como una red basada en la colaboración y ayuda entre los usuarios que van a velar por la protección de los datos y las transacciones. Y, por otro lado, al ser abierta, como una red plagada de posibles intentos de hackeo o uso fraudulento con el que sujetos pueden atacar a la información contenida en estas redes, para obtener, de forma fraudulenta, beneficios económicos o de cualquier tipo. Aquí es donde una especial importancia los protocolos de consenso que impidan la manipulación de la información recogida en estas redes.

Las redes privadas tienen unas características muy similares a las redes públicas, pero presentan una diferencia fundamental y es que en estas existe un elemento central que controla todas las operaciones que se producen dentro de la red. Las características más importantes de este tipo de red y que le diferencian de las públicas son:

- El acceso a este tipo de redes está restringido a la autorización por el usuario central que controla la red.

- El acceso a las operaciones registradas en esta red es privado y sólo puede accederse mediante autorización.
- El mantenimiento económico de estas redes corresponde a la entidad que hace uso de esta red.

Por último, encontramos un tipo de red a medio camino entre las dos anteriores, las redes híbridas o federadas. Este tipo de redes tratan de incluir las mejores cualidades de los dos tipos de redes y son muy frecuentes en organizaciones de gobierno de los países. En este tipo de redes:

- El acceso a la red requiere de autorización por parte del usuario que controla la red.
- El acceso al libro de registro de las operaciones realizadas en la red es público, cualquiera puede acceder a la información. (Bit2me, 2022)

2.1.2. La firma digital.

Pese a que tienen una similar denominación, no debemos confundir la firma digital ligada a las redes blockchain, con la firma electrónica que utilizamos para demostrar nuestra identidad en documentos electrónicos, aunque en esencia su finalidad sea la misma.

La firma digital en esencia es muy similar y tiene el mismo objetivo que la firma convencional que todos tenemos. En el contexto de las redes blockchain, la firma digital actúa como una clave criptográfica que permite identificar a los usuarios en las transacciones realizadas en la red, asegurar que las transacciones se realizan entre los usuarios correctos y que la información contenida en estas transacciones no pueda ser interceptada ni manipulada en el proceso de la transacción (Modi, 2018).

La firma digital se compone de dos “llaves” una privada y una pública y cada una tiene una función determinada. La llave privada permite al usuario y solo a este, firmar el mensaje que quiere transmitir a través de la red. La llave pública, que es conocida por todos los usuarios, va a permitir verificar que el usuario que envía cierta transacción es el que lo firma, porque todos van a poder comprobar que esa llave pública está asociada al usuario en cuestión. Estas dos claves están estrechamente

relacionadas así porque, además de funcionar de forma conjunta, la clave pública es generada a través de la clave privada.

2.1.3. La minería.

El proceso de minería es muy similar al de la llevanza de contabilidad, el minero es el responsable de por registrar todas las transacciones que se realizan en la red. En cada una de las redes blockchain existe un gran número de mineros, los cuales compiten entre sí para ser los primeros en registrar las transacciones y recogerlas en bloques que serán encadenados en la blockchain, ya que el primero en registrar el bloque de transacciones recibirá una recompensa que puede ser, por ejemplo, en forma de criptomoneda.

El proceso de minería es uno de los elementos esenciales en el funcionamiento de la red blockchain y es de gran dificultad y comprensión. Vamos a tratar de explicar de la forma más didáctica posible cómo funciona el proceso de minería.

El proceso de minería consiste en cada uno de los mineros lleva a cabo un continuo cambio en el valor del nonce hasta encontrar el hash que descifra el “rompecabezas” que protege la transacción. En el momento en el que un minero de con el valor correcto del nonce, este lo publica en la red para que el resto de los mineros puedan verificar que es el valor correcto través de un mecanismo de consenso (Proof of Work o Proof of Stake, entre otros). Una vez que un minero ha “descifrado” una serie de transacciones que han sido verificadas por el resto de los mineros, se agrupan en un bloque que será incorporado a la cadena de bloques (Modi, 2018).

2.1.4. El Consenso.

El mecanismo de consenso es uno de los elementos más importantes en las redes blockchain, pues es el proceso que permite a los mineros de la red ponerse de acuerdo acerca de la validez y veracidad de una determinada transacción, sin el cual, estas no son aprobadas y por tanto no pueden ser incluidas en los bloques de la cadena, es decir, si no existe consenso entre mineros no funciona la red.

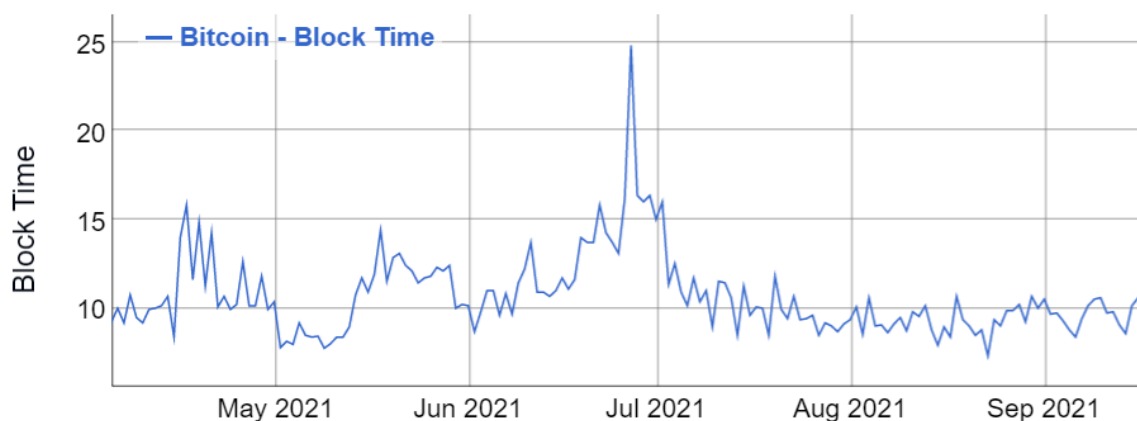
Para obtener este consenso, existen diferentes mecanismos o algoritmos utilizados en las distintas redes blockchain existentes, de los que vamos a tratar de explicar los más relevantes.

Por ejemplo, en la red Bitcoin el mecanismo de consenso se denomina Proof of Work o PoW. Este algoritmo aparece por primera vez en el white paper “Hashcash - A Denial of Service Counter-Measure” publicado por Adam Back y, en esencia, consiste en que los mineros han de resolver un extremadamente complejo puzle matemático, tan complejo que es probable que los mineros no quieran tratar de resolver dicho puzle. Esta operación de resolución supone, aparte del enorme esfuerzo, grandes costes de recursos computacionales, pero la comprobación es relativamente sencilla. Por lo tanto, un minero que con fines fraudulentos quiera modificar la cadena de bloques, va a tener que realizar un muy costoso proceso que es muy fácil de comprobar por el resto de los mineros si es correcto o no, y que, además, posteriormente el resto de los nodos honestos votarán por mayoría si se valida o no la transacción (Pralhad & Kaur, 2019).

En este caso, aparece el problema del 51% y es que, si más de la mitad de los nodos encargados de comprobar las transacciones tuvieran fines fraudulentos, podrían ponerse de acuerdo para aprobar transacciones que no son válidas ni veraces.

Otro de los problemas que tienen el PoW es en relación con el tiempo que tarda en realizarse la prueba consensual y el registro en cadena de bloques. Como podemos observar en la siguiente imagen, el tiempo medio en la red Bitcoin (que usa PoW) es de 10 minutos llegando a alcanzarse incluso picos de 25 minutos.

Fig.2. Tiempo medio de registro en cadena de bloques del Bitcoin

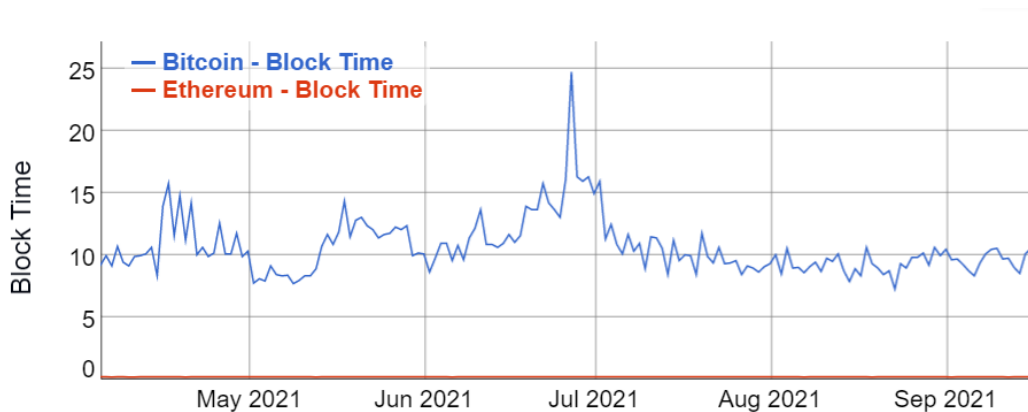


Fuente: bitinfocharts.com

De cara a su implementación, por ejemplo, como medio de micropagos, Bitcoin se enfrenta a un enorme problema en cuanto a los tiempos de verificación de transacciones. Si para cualquier pago de nuestra vida cotidiana como en un restaurante o

tienda, debemos esperar en el mejor de los casos 10 minutos, los usuarios no se vana mostrar interesados en usar este tipo de red. Sobre todo, cuando existen otras redes en las que este problema desaparece como podemos observar en el siguiente gráfico:

Fig.3. Tiempo medio de registro en cadena de bloques del Bitcoin y Ethereum



Fuente: bitinfocharts.com

Podemos observar como en la red Ethereum que usa el protocolo Proof of Stake, el tiempo medio en el registro de la cadena de bloques se encuentra en una media estable de en torno a 22 segundos, lo cual le ofrece una enorme ventaja frente a la red Bitcoin que, como sabemos, utiliza PoW.

El protocolo Proof os Stake (PoS), en lugar de dar el puzle a resolver a todos los nodos como en PoW, lo asigna de forma aleatoria entre todos los nodos, pero dentro de esta aleatoriedad tiene en cuenta ciertos elementos, por lo que no es del todo aleatorio.

Es importante hacer una breve explicación de un concepto esencial dentro de este protocolo, el coinage. Coinage, es básicamente la cantidad de un token o criptomoneda que se tiene en propiedad multiplicada por el tiempo que se tiene. Es decir, si un usuario dispone de 10 tokens que ha mantenido durante 10 días, su coinage es 100 (King & Nadal, 2012).

Este concepto es importante porque en PoS, se va a asignar la tarea de descifrar el puzle matemático en función del tiempo y de la cantidad de tokens de que dispongan los usuarios. Lo que se trata de conseguir con este sistema es que los usuarios tengan el mayor número de tokens y que lo mantengan durante el mayor tiempo posible. De esta forma, el sistema seguirá un procedimiento aleatorio en el que los usuarios que

dispongan de una mayor participación en la red van a tener una mayor probabilidad de ser elegidos para validar las transacciones y recibir la recompensa asociada, aunque no se asegura que sean elegidos los que tengan más participación, “únicamente” aumentan su probabilidad de ser elegidos (Pralhad & Kaur, 2019).

Con este tipo de mecanismo, el ataque del 51% que hemos mencionado relativo al protocolo PoW deja de tener sentido, ya que sería necesario tener el 51% o más del total de las monedas de la red, y teniendo en cuenta que cuando se producen ataques de este tipo a la red el valor de la criptomoneda asociada tiende a caer, no tendría sentido para la persona que posee más de la mitad de esta criptomoneda realizar un ataque que reduzca el valor de su activo (Bit2me, 2022).

3. Las criptomonedas.

Las criptomonedas o monedas digitales tienen su origen en el año 2008 cuando una persona o grupo de personas bajo el seudónimo de “Satoshi Nakamoto” publicó el documento *Bitcoin; a Peer-to-Peer Cash System* en el cual aparecía explicado por primera vez el Bitcoin, la primera criptomoneda que vio la luz y que se sustentaba en tecnología blockchain (Nakamoto, 2008).

Por criptomoneda entendemos un activo digital que sirve como medio de intercambio dentro de una red, que está protegida por criptografía para asegurar así las transacciones, controlar la creación de unidades adicionales y comprobar la transferencia de estos activos. Las diferencias que pueden existir entre los diferentes tipos de criptomonedas pueden afectar al tipo de red blockchain en el que sustentan, el mecanismo de consenso que se utiliza o el algoritmo criptográfico utilizado en esta red, por ejemplo (K. Hardle, R. Harvey, & C.G. Reule, 2019).

Blockchain y criptomoneda son conceptos que frecuentemente se confunden y tratan de la misma forma, pero son completamente diferentes. Blockchain es la red o sistema informático en la cual se desarrollan las transacciones y se registra toda la información que sucede en la red. Mientras que la criptomoneda, es el elemento que se utiliza como medio de intercambio dentro de una concreta red blockchain.

3.1. Clasificación de las criptomonedas.

Aunque el origen de las criptomonedas se encuentra en el Bitcoin con el paso de los años han ido surgiendo cientos de monedas digitales, las cuales no son iguales entre sí. Podemos agrupar las criptomonedas en 7 grupos fundamentales:

- ***Mecanismos de transacción:*** dentro de este grupo encontramos a Bitcoin y una de las primeras alternativas a esta, Litecoin, que proporcionaba tiempo de adhesión de los bloques de 2.5 minutos comparados con los 10 minutos de Bitcoin (K. Hardle, R. Harvey, & C.G. Reule, 2019).
- ***Distributed computation token:*** aquí encontramos a Ethereum, la segunda gran criptomoneda actual.

- **Utility tokens:** estos son activos programables dentro de la red blockchain (K. Hardle, R. Harvey, & C.G. Reule, 2019). Es el tipo de criptomoneda más utilizado en ofertas iniciales de moneda o ICOs (por sus siglas en inglés, Initial Coin Offering), y hacen referencia a un pre compra de servicios de una red blockchain, normalmente a descuento (Briggs, 2018). Este tipo de token es muy frecuente en la financiación de empresas y start ups.

Un ejemplo de este tipo de token es Golem, que permite a los usuarios de una red comprar poder computacional a otros usuarios o vender el exceso de poder computacional a otros usuarios (K. Hardle, R. Harvey, & C.G. Reule, 2019).

- **Security tokens:** estos son valores financieros regulados que ofrecen a inversores a través de STOs² que deben cumplir con regulaciones financieras jurisdiccionales ya que, estos tokens proporcionan a los inversores derechos financiero como participación en los beneficios, derechos de voto, etc. Estos derechos se registran en *smart contracts*³ y son negociados en una bolsa regulada soportada por blockchain (Newtown Partners, 2019)
- **Fungible tokens:** estos son aquellos que exactamente iguales entre todos ellos, son intercambiables y divisibles. (Karandikar, Chakravorty, & Rong, 2021). Un ejemplo de esta clasificación es Bitcoin, ya que todos los tokens de la red Bitcoin son iguales entre sí y tienen el mismo valor, se intercambian entre los usuarios de la red y pueden ser divididos, es decir, se puede intercambiar una determinada porción de un token de esta red.
- **Non Fungible Tokens:** a diferencia de los anteriores, los NFTs son totalmente únicos e irremplazables y no pueden ser intercambiados entre sí en la red. Este tipo de token recibe su valor como consecuencia de su

² Una STO (Security Token Offering) es un tipo de oferta pública en la que los valores digitales, los tokens de seguridad, se venden en intercambios de tokens de valor.

³ Los smart contracts son básicamente acuerdos registrados en programas informáticos que aseguran el cumplimiento de los compromisos registrado en la red por dos o más partes.

propia unicidad (W. Chohan, 2021). Los NFTs son de gran ayuda a la hora de probar la autoría y autenticidad de diferentes elementos en la red. Como ejemplo gráfico de este tipo de token encontramos unos de los más famosos y valiosos NFTs, los Cryptopunks, recogidos en la siguiente figura (Fig. 2):

Fig.2. Cryptopunks NFT



Fuente: Cryptoshitcompra.com

- **Stablecoins:** estas son monedas que nacen con el objetivo de minimizar el alto riesgo de volatilidad que tienen otras como BTC o ETH. Estas son criptomonedas cuyo precio se va a mantener fijo unidades de una moneda tradicional u otros activos (Berentsen & Schär, 2019). Estas son monedas que están colateralizadas con otros activos que permiten reducir su volatilidad. Dentro de las stablecoins encontramos una subclasificación.
 - Garantizadas con moneda fiduciaria: como Tether que está ligada al dólar americano o LBXPeg que está ligada a la libra esterlina.
 - Garantizadas con activos reales: como DGX (Digix Gold) que esta colateralizada por el oro o SRC (Swiss Real Coin) colateralizada por bienes raíces suizos (K. Hardle, R. Harvey, & C.G. Reule, 2019).

Habiendo analizado el concepto de criptomoneda y las diferentes clasificaciones en las que se pueden enmarcar, pasamos a analizar y estudiar algunas de las más relevantes hoy en día.

3.2. Criptomonedas más relevantes.

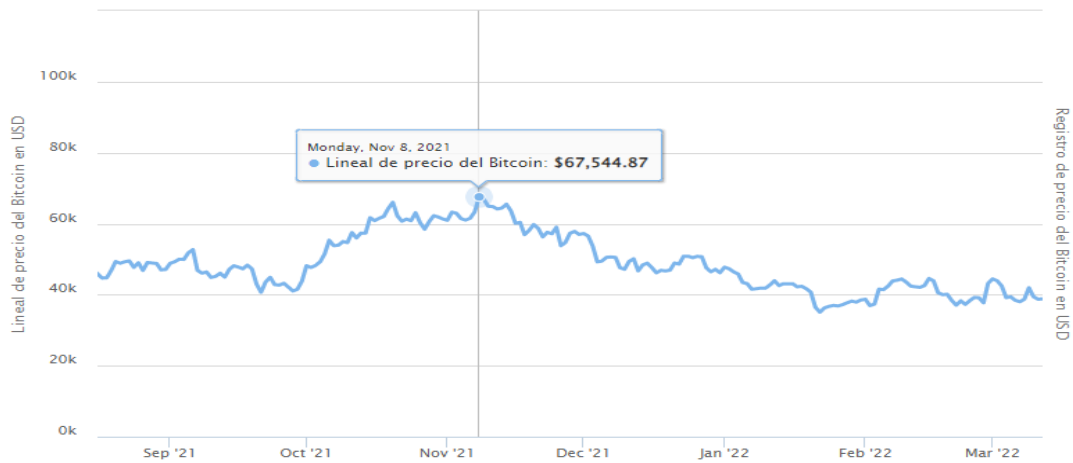
3.2.1. BTC (Bitcoin).

Como no podía ser de otra forma, cuando hablamos de las criptomonedas más relevantes tenemos que comenzar hablando del Bitcoin o BTC. Como hemos señalado anteriormente, Bitcoin surge como la primera criptomoneda en el año 2008 a raíz de la publicación del white paper de Satoshi Nakamoto, Bitcoin: a Peer-to-Peer Cash System.

Antes de la aparición del Bitcoin, el único sistema de pagos electrónicos existente en el mundo dependía en su totalidad de la actuación de terceras entidades intermediarias que servían como mediadoras y aseguraban el teórico éxito de las transacciones, basado todo ello en un sistema de confianza hacia estas entidades. Este sistema conlleva costos de mediación y gestión que incrementan el coste de las transacciones para los interesados e implica un cierto riesgo de fraude e incertidumbre respecto de las entidades mediadores y de la contraparte de la operación (Nakamoto, 2008).

En este contexto surge Bitcoin, con el objetivo de crear un sistema que prescindiera de estas entidades de mediación, elimine los costes asociados a esta y acabe con el riesgo de fraude y la incertidumbre en las operaciones. Bitcoin consigue esto por medio del uso de la tecnología blockchain, a través de complejos mecanismos criptográficos y del reparto de la información entre todos los usuarios de la red que hace enormemente complejo y costoso la alteración de la cadena de bloques, evitando así la actuación de hackers y fraudes.

Para comprender la entidad y relevancia que el bitcoin tiene en la economía actual, acudimos a ciertos datos o cifras que son muy reveladoras sobre la magnitud de esta criptomoneda. Actualmente 144 millones de personas son tenedoras en alguna proporción de Bitcoin, aunque una gran cantidad de estas se concentra en un relativamente pequeño grupo de usuarios. Otro de los elementos que más revela la dimensión de esta criptomoneda es su precio. Actualmente, el bitcoin tiene un precio de 35,492.85 euros o 38,729.90 dólares estadounidenses. Aunque, el día 8 de noviembre de 2021 el bitcoin registró su máximo histórico por un valor de 67,544.87 dólares estadounidenses.



Fuente: buybitcoinworldwide.com

Sin embargo, solo tres meses después, el día 22 de enero de 2022 registró su mínimo en los últimos 6 meses alcanzando un valor de 35,085.14 dólares estadounidenses.



Fuente: buybitcoinworldwide.com

Observando estos datos parece lógico preguntarse cuáles son las razones del crecimiento, expansión y éxito de esta concreta criptomoneda a que a niveles de precio se encuentra muy alejada de otras criptomonedas y redes que a priori son más avanzadas y ofrecen (redes de segunda generación) más servicios que Bitcoin. También es interesante analizar qué aspectos hacen que los inversores se decidan por el Bitcoin en lugar de monedas tradicionales como tradicionalmente se ha venido haciendo. Algunas de las características que hacen que Bitcoin destaque respecto a otras criptomonedas son:

- Es **descentralizada** y **no existe ninguna autoridad** que controle la red ni las operaciones que se desarrollan en ella a diferencia de lo que ocurre con las monedas como el euro o el dólar que están controladas por gobiernos y bancos centrales (Aljabr, Sharma, & Kumar, 2019). El valor del Bitcoin varía en función de la demanda que existe, no por decisiones de terceras entidades que lo controlen.
- Los usuarios que utilizan Bitcoin mantienen su **anonimato** en las transacciones que realizan dentro de la red Bitcoin, la veracidad de la transacción se realizará comprobando las claves públicas y privadas de los usuarios que formen parte de la transacción, pero sin la necesidad de que revelen su identidad.
- El **suministro** de esta criptomoneda es **limitado**, es decir, existe un número máximo de Bitcoin que van a ser generados. Este número es 21 millones de Bitcoin y es inmutable pues está así establecido en el código de la red. Esto hace que el Bitcoin sea un activo más valioso frente a las monedas tradicionales y otras criptomonedas que no tienen un límite en su creación, porque estas pueden ser emitidas por gobiernos y bancos “sin límite” lo cual hacen que cada unidad tenga menor valor (Aljabr, Sharma, & Kumar, 2019).
- A diferencia de las **transacciones** tradicionales que requieren largas y costosas comprobaciones, las transacciones realizadas en la red Bitcoin son **globales e instantáneas**.
- La **seguridad** es uno de los elementos diferenciadores de Bitcoin respecto de los medios y transacciones tradicionales. En Bitcoin solo el propio usuario es conocedor de su clave privada, lo cual unido al complejo sistema criptográfico utilizado en la red hace que sea prácticamente imposible el acceso a hackers o los problemas informáticos puesto que la información está repartida entre diferentes nodos y no en una única unidad central (Aljabr, Sharma, & Kumar, 2019).

- No es necesaria **ninguna autorización o permiso** por parte de un banco o gobierno para poder utilizar y realizar transacciones con Bitcoin, únicamente en necesario tener acceso al software.
- La **eficiencia** es una de las notas características de Bitcoin. El hecho de que no exista una entidad central que verifique las transacciones hace que las operaciones realizadas a través de la red de Bitcoin, al ejecutarse directamente entre usuarios (Peer-to-Peer), sin existir horarios y con bajas comisiones por su carácter puramente digital, sean mucho más eficientes en tiempo y coste (Aljabr, Sharma, & Kumar, 2019).
- Quizá una de las características más importantes y la principal por la que surgió Bitcoin es la que **no es necesaria la confianza** en una entidad intermedia, las transacciones se validan y aseguran a través de la criptografía y minería y son automáticamente detectadas cuando no son correctas, por lo que los usuarios no tienen que confiar en ninguna persona o entidad que asegure el éxito de sus operaciones (Aljabr, Sharma, & Kumar, 2019).

Estas son algunas de las características que hacen que Bitcoin se diferencie y tenga el gran valor que vemos reflejado en su precio y demanda, pero como todo también tiene sus puntos negativos y críticas, incluso algunas de las características que hemos analizado como positivas desde otro punto de vista se perciben como aspectos negativos.

Así, el anonimato que hemos analizado como una de las características que atraen a los inversores hacia el Bitcoin, es a la vez un de sus principales críticas, pues este anonimato atrae a personas que como consecuencias de sus actividades ilegales buscan el anonimato que ofrece Bitcoin para cubrir su identidad en las transacciones realizadas producto de su actividad criminal (Luu & Imwinkelried, 2016).

En este sentido, es muy ilustrativo del problema con la criminalidad y el mercado negro asociado al bitcoin el caso de *The Silk Road*. *The Silk Road* es una web en la que se extendió el intercambio de bienes ilegales (mayoritariamente drogas) soportado por el navegador Tor, un navegador creado los gobiernos suecos y

norteamericano con el objetivo de realizar comunicaciones secretas sin dejar ningún tipo de rastro. Sobre este software se desarrolla The Silk Road, en la cual los usuarios pueden realizar intercambios de bienes ilegales quedando su identidad secreta para terceras personas y para los involucrados en la transacción. Así, y con el objetivo de no revelar su identidad por medio de transferencias bancarias, entra en juego el bitcoin y su carácter anónimo, que permite hacer efectiva la ocultación de la identidad en las transacciones ilícitas y criminales (Raeesi, 2017).

Aunque The Silk Road fue cerrada en 2013, este caso pone de manifiesto el vital papel que el Bitcoin puede jugar en entramados criminales que se puedan estar desarrollando actualmente o que pueden llegar a surgir en el futuro con el avance e implantación de estas tecnologías.

Otra de las grandes críticas que recibe continuamente el Bitcoin es en referencia a la volatilidad en su precio, que unido a la complejidad de su funcionamiento supone un alto riesgo para aquellas personas que no tienen un exhaustivo conocimiento sobre ella y operan en el mercado con fines especulativos. El valor del Bitcoin ha ido creciendo exponencialmente en los últimos años.



Fuente: CoinMarketCap

Tras una rápida mirada al anterior gráfico podemos ver como el precio del Bitcoin ha pasado de ser, en 5 años, de apenas 1,000 dólares a colocarse alrededor de los 40,000 dólares hoy en día. Y, aunque observamos que existen periodos de cierta

estabilidad en el precio del Bitcoin, existen ciertas etapas de extrema volatilidad en su precio que hacen de este un activo de extremado riesgo.

Por ejemplo, entre el 13 de abril de 2021 (\$63,503.) y el 25 de abril del mismo año (\$49,004.25), apenas diez días, el precio del Bitcoin se redujo en alrededor de \$14,000, subiendo a los \$58,803 apenas 15 días después a fecha de 8 de mayo de 2021 (entorno a \$8,000 de subida) y sufriendo una de sus mayores caídas en menos de 30 días posicionándose en \$34,616.51 el día 29 de mayo de 2021.



Fuente: CoinMarketCap

Un proceso similar se ha vivido a finales de este año 2021, cuando el pasado 8 de noviembre el Bitcoin alcanzó su máximo histórico por valor \$67,566 cayendo en apenas dos meses hasta \$35,030.

En un período de aproximadamente un mes y medio podemos observar cómo Bitcoin alcanzó su máximo histórico, fue experimentando consecutivas y considerables fluctuaciones en su precio hasta que se produjo una de las mayores caídas en su valor. Esto pone de claro manifiesto las enormes fluctuaciones que se producen en el precio de esta criptomoneda, el cual expone a inversores y a usuarios a un gran riesgo. Sin

embargo, hay autores que indican que con el paso del tiempo lo normal sería que los porcentajes de variación se reduzcan y la cotización de la moneda sea más estable (Rodas & Núñez, 2021).

Existen diferentes razones que motivan esta alta volatilidad entre las cuales destacamos las siguientes. En primer lugar, el Bitcoin al ser un concepto razonablemente nuevo se ve altamente afectado por noticias y novedades como pueden ser declaraciones de gobiernos sobre su uso y regulación, eventos geopolíticos incluso se han producido grandes variaciones en el precio de la moneda por declaraciones de ciertas personalidades en redes sociales. Otro de los elementos que produce grandes fluctuaciones son los movimientos en el mercado de las denominadas ballenas, que son ciertas entidades que poseen una gran cantidad de esta moneda y que cuando realizan grandes operaciones en el mercado provocan considerables variaciones en el precio. Por último, es importante destacar el tamaño del mercado ya que, al ser relativamente pequeño en comparación con los principales mercados existentes, los factores anteriores que afectan a la volatilidad se ven amplificados (Lloyd, 2020).

Otro de los problemas a los que Bitcoin se enfrenta es su falta de aceptación y el lastre que esto supone para la escalabilidad de la red Bitcoin. Y es que, a pesar de que la tecnología en la que está basada Bitcoin tiene infinidad de aplicaciones en prácticamente todos los sectores e industrias, existe una fuerte falta de conciencia sobre todo en aquellos países en que la moneda está prohibida y, frecuentemente se juzga de forma equivocada a la red de blockchain de Bitcoin como si fuera lo mismo que la criptomoneda, provocando que los grandes beneficios que tiene la tecnología tras Bitcoin sean ignorados (Pralhad & Kaur, 2019).

Por último, uno de los grandes inconvenientes y que provoca multitud de críticas hacia Bitcoin es lo costoso y perjudicial que puede llegar a ser para el medio ambiente la utilización de la red Bitcoin como consecuencia de su protocolo de consenso. Como hemos mencionado, el protocolo de consenso utilizado en Bitcoin es el Proof of Work, el cual requiere de un enorme consumo de recursos computacionales y energéticos para lograr el consenso de cada una de las transacciones realizadas que, teniendo en cuenta el número transacciones, supone una enorme demanda energética y de recursos que tiene un muy negativo impacto en el medio ambiente.

3.2.2 ETH (Ethereum)

ETH es la criptomoneda desarrollada y soportada sobre la blockchain Ethereum, y utilizada para la ejecución de transacciones en la red. Ethereum es una de las más extendidas redes blockchain en la actualidad y surge por medio del reconocido programador Vitalik Buterin que, observando todas las dificultades y críticas a las que se enfrentaba Bitcoin, decidió proponer una nueva red que tratara de solventar esos problemas añadiendo una importantísima novedad, la posibilidad para los desarrolladores de crear aplicaciones descentralizadas (DApps) en la red y la implementación de los “Smart contracts” (Pralhad & Kaur, 2019).

Así, Ethereum es considerada una red de segunda generación. En la red Ethereum existen dos tipos de cuentas. Por un lado, encontramos las cuentas de usuario que van a representar a los participantes de la red entre los que distinguimos a: *callers*, que son quienes solicitan la ejecución de los smart contracts; *deployers*, que son los encargados de desarrollar y desplegar los smart contracts en la red; y los mineros que son los encargados de la verificación de las transacciones y el mantenimiento de la red. El otro tipo de cuentas que participan en Ethereum son las cuentas smart contract, que representan al propio contrato inteligente dentro de la red (Wu, Ma, Huang, & Liu, 2019).

Analizando lo anteriormente expuesto en relación con Ethereum, es necesario analizar detenidamente y comprender que son los smart contracts y cuáles son las ventajas que estos ofrecen.

El concepto de smart contract fue creado en 1994 por el informático y jurista, Nick Szabo (Metcalf, 2020). Szabo los definió de la siguiente forma: “*Un contrato inteligente es un protocolo de transacción informatizado que ejecuta los términos de un contrato*” (Szabo, 1994).

Szabo definió una serie de objetivos generales relacionado con los smart contracts que incluían: satisfacer las condiciones contractuales habituales, minimizar las excepciones maliciosas y accidentales y, reducir en la mayor medida posible la necesidad de intermediarios de confianza. Además, se establecieron objetivos a nivel económico relacionado con la reducción de pérdidas derivada del fraude, reducción e

incluso eliminación de costes de arbitraje, ejecución y otros costes de transacción (Szabo, 1994).

Los contratos inteligentes, como hemos mencionado se implementan sobre la cadena de bloques. Las cláusulas contractuales definidas y aprobadas en el acuerdo se convierten en programas informáticos ejecutables registrados en la red. La ejecución de dichas cláusulas se va a registrar como una transacción almacenada en la blockchain, que va a ser inmutable gracias a las propiedades de la cadena de bloques que hemos analizado anteriormente. La conexión entre estas cláusulas convertidas en programas informáticas sigue los flujos lógicos típicos de la programación, por ejemplo, la declaración *if-else-if* que establece que, si una condición se cumple se de un cierto resultado y si no se cumple, se de otro. Para el caso de los smart contracts, en caso de que una de las cláusulas estipuladas en el acuerdo se cumpla o no, automáticamente se producirá un determinado resultado en función de si se ha cumplido dicha condición o no (Zheng, y otros, 2019).

De forma ejemplificativa, un sencillo ejemplo es el siguiente: A acuerda con B el pago de 2 ETH por la prestación de un servicio de asesoría legal por parte de B. Como cláusula se acuerda que en caso de impago por parte de A (incumplimiento del contrato), se impondrá una sanción a A (se le deducirán automáticamente de su saldo 2 ETH que serán enviados a B). Por lo tanto, si llega la fecha establecida y A no ha pagado, automáticamente se le deducirán a A la cantidad estipulada y B recibirá la contraprestación estipulada en el contrato.

Aquí surge una duda, ¿qué pasa si en el momento en que se impone la sanción a A, este no cuenta con los fondos necesarios para compensar a B? La solución es fácil, el sistema de doble depósito. Antes de formalizar el contrato se establece la obligación de que cada una de las partes deposite una determinada cantidad que será registrada como una transacción en la cadena de bloques. De esta forma, si llega el plazo pactado y alguna o ambas partes no cumplen las obligaciones contraídas, esos fondos son transferidos a la parte perjudicada o a otra cadena de bloques para que no las partes no puedan acceder a esos fondos asegurando así, el cumplimiento de las obligaciones por las partes (Atico, 2022).

Habiendo analizado el concepto y funcionamiento de los smart contracts, es importante definir y comprender las Dapps, para poder entender el potencial que tiene la red Ethereum.

Las Dapps son aquellas aplicaciones ejecutadas en un entorno completamente descentralizado basadas generalmente en la tecnología blockchain. Frente a lo que ocurre en las aplicaciones “tradicionales” que conocemos como Facebook o YouTube, en las Dapps no existe un único nodo central (Suárez & Freitag, 2020). Las Dapps pueden ser aplicaciones móviles o web en los que la validez de la información es corroborada a través de smart contracts (BBVA, 2022).

Las ventajas más relevantes de este tipo de aplicación son las siguientes. Por un lado, la seguridad ya que al estar desarrollada y corriendo en un gran número de nodos en lugar de un único servidor central, aunque uno o varios de esos nodos deje de funcionar, la aplicación se va a poder seguir ejecutando en el resto de los nodos. Al contrario de lo que ocurre con las aplicaciones tradicionales en las que, si el servidor de la aplicación deja de funcionar o “se cae”, la aplicación no funciona, como ha ocurrido en numerosas ocasiones con las caídas de aplicaciones como WhatsApp o Facebook (Saéz, 2022).

Otra de las ventajas que surgen gracias al uso de las Dapps es que al no existir una entidad central que controle el funcionamiento de estas aplicaciones, se reducen en gran medida los riesgos de censura injustificada, decisiones arbitrarias, etc., que se pueden llegar a producir en las aplicaciones tradicionales que son controladas y gestionadas por entidades privadas y que actúan en su propio beneficio. En las Dapps el control y la gestión de la aplicación se reparte entre todos los nodos que participan en esta, y estos serán los que tomen las decisiones en cuanto a su funcionamiento a través de mecanismos democráticos de votación.

En definitiva, lo que ofrecen los smart contracts y Dapps conjuntamente, son opciones de interacción y establecimiento de acuerdos entre partes, en los que no es necesaria la confianza ni entre las partes contratantes ni con una tercera entidad, son considerablemente más seguras y transparentes que los mecanismos convencionales y, por último, ofrecen un enorme ahorro de costes (costes de transacción, mediación, etc.) y un incremento notable en la eficiencia de las transacciones.

En este sentido, Ethereum es la red blockchain en la que se desarrollan más Dapps y smart contracts actualmente con ETH como medio de pago de las transacciones realizadas en dicha red. En la siguiente figura (Fig.3) podemos ver una tabla referente al número de Dapps, usuarios activos, smart contracts, etc. desarrolladas en las principales redes blockchain.

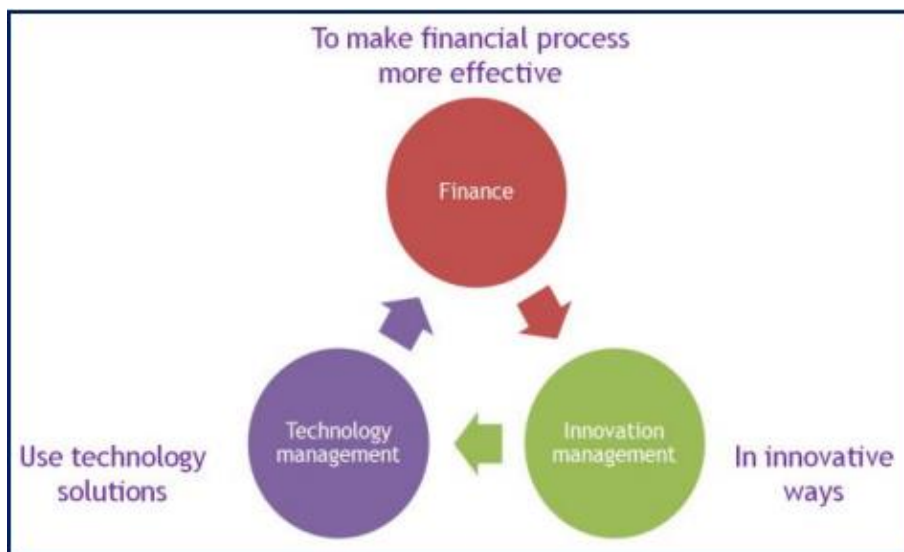
Fig.3. Plataformas más populares en el desarrollo de Dapps

Platforms					
Platform	Total DApps	Daily active users [?]	Transactions (24hr) [?]	Volume (24hr) [?]	# of contracts
Ethereum	2939	79.74k	142.94k	83.56k	4.87k
EOS	331	55.56k	423.06k	196.95k	549
BSC	195	[?]	[?]	[?]	327
TRON	88	1.1k	4.7k	603.5k	286
Klaytn	80	[?]	[?]	[?]	317
Steem	79	[?]	[?]	[?]	177

4. FinTechs.

El concepto FinTech (contracción de los términos Financial Technology, en inglés) o tecnología financiera hace referencia a la aplicación de tecnología para la provisión de servicios financieros (Anyfantaki, 2016). Podríamos definir la tecnología financiera como una disciplina transversal resultante de la combinación de finanzas, gestión tecnológica y gestión de la innovación, que tiene como objetivo el uso de soluciones tecnológicas de forma innovativa para mejorar la eficiencia de los procesos financieros (Leong & Sung, 2018).

Fig.4. Fintech, una disciplina transversal



Fuente: (Leong & Sung, 2018)

En un plano más práctico, entendemos por FinTechs aquellas compañías que usan las más innovadoras tecnologías para operar fuera de los tradicionales modelos de negocio dentro del sector financiero, tratando de cambiar la forma en la que se ofrecen los servicios financieros usando la más novedosa tecnología y los procesos de intercambio de información automatizados (Milian, Spinola, & Carvalho, 2019).

Hoy en día, estas nuevas compañías FinTech están adquiriendo una gran cuota de mercado que tradicionalmente ha pertenecido a los tradicionales prestadores de servicios financieros. Esta captación de clientes por parte de las FinTechs se debe a diferentes razones.

En primer lugar, las soluciones y servicios que ofrecen las FinTechs cubren las necesidades que anteriormente no satisfacían o no hacían de forma suficiente los tradicionales prestadores de servicios financieros (Gomber, Koch, & Siering, 2017).

En segundo lugar, estas compañías ofrecen a sus clientes nuevas oportunidades para vender sus productos y servicios por medio de nuevas tecnologías (Gomber, Koch, & Siering, 2017). Un ejemplo de estas nuevas oportunidades de ventas de productos y servicios es MarketInvoice, una FinTech que desarrollo una plataforma para a negociación online donde pequeñas y medianas empresas pueden vender sus facturas pendientes para financiar así su capital de trabajo (Lee, 2015).

Por último, las compañías con un alto bagaje tecnológico, como son las FinTechs, están mejor preparadas para ofrecer servicios en un entorno tan cambiante e innovador como en el que vivimos hoy en día en el sector financiero. Al producirse tantos y tan rápidos cambios, las empresas dedicadas a prestar servicios financieros deben estar preparadas para adaptarse a esas modificaciones. Las FinTechs disponen de unos modelos y estructuras de negocio mucho más ágiles e innovativas que los tradicionales prestadores de servicios lo que les permite adaptarse de forma más ágil y económicamente eficiente, poniendo en jaque a los competidores basados en modelos.

El papel que las FinTechs están jugando en el sistema financiero actual esta experimentando un crecimiento exponencial año tras año y, un buen ejemplo de la dimensión de este tipo de compañías es Ant Group.

Ant Group es una filial del gigante chino del comercio electrónico Alibaba. Ant Group se encuentra dividida en una seria de divisiones que ofrecen a sus usuarios diferentes servicios. Entre estos podemos destacar: Alipay, una plataforma de pagos online; Ant Fortune, un Marketplace financiero que ofrece servicios de inversión personalizado a sus clientes; MyBank, un banco exclusivamente digital enfocado a autónomos y pequeñas empresas; Zhima Credit, una plataforma de scoring financiero que utiliza los datos recabados por las empresas del grupo Alibaba para realizar sus valoraciones (Barros, 2020).

Todos estos servicios hacen de Ant Group el gigante financiero que hoy es en día, pues es la FinTech mejor valorada del mundo y la compañía unicornio más valiosa

del mundo, valorada en 150.000 millones de dólares estadounidenses superando a bancos como el Santander (Barros, 2020).

Fig.5. Comparación de la capitalización bursátil de Ant Group.



Fuente: CB Insights

5. Implementación de las redes Blockchain en el sistema financiero.

5.1. Blockchain en las transferencias interbancarias.

Una de las principales innovaciones y que está teniendo un mayor impacto en el sistema financiero es en relación con las transferencias de fondos entre cuentas, sobre todo en las transferencias internacionales. Habitualmente, una transferencia internacional se hace efectiva entre 2 y 5 días hábiles. Sin embargo, este plazo varía en función de varios factores (Merlo, 2016):

- En los países del Espacio Económico Europeo que comparten una divisa los plazos para hacer efectivas las transferencias oscilan entre **1 y 2 días hábiles** y en transferencias que involucran a países con diferentes monedas los plazos se elevan hasta **5 o 6 días hábiles**.
- Las instituciones financieras establecen unas horas límite para realizar transferencias en un mismo día. Si se supera este horario la transferencia se gestionará el siguiente día hábil.
- Las transferencias internacionales a menudo requieren de una tercera institución intermediaria que conecte a la entidad emisora y a la receptora lo cual demora el proceso.

Además de los problemas respecto a la demora en el proceso, las entidades financieras aplican a estas operaciones, en concepto de gastos de gestión y comisiones, tarifas de entre el 5% y el 20%.

A todo lo anterior, se le suma los problemas de seguridad y ciberataques que sufren las entidades bancarias y las plataformas de transferencia de fondos. Por ejemplo, la plataforma SWIFT (Society for Worldwide Interbank Financial Telecommunication), la principal red internacional encargada de administrar las operaciones entre bancos de todo el mundo, sufrió una serie de ciberataques en el año 2016 por los cuales, fueron sustraídos cibernéticamente 81 millones de dólares de la cuenta del Banco Central de Bangladesh en el Banco de la Reserva Federal de Nueva York (Revilla, 2016).

Antes esta situación, la tecnología Blockchain ofrece una serie de opciones que pueden ser de gran ayuda ante este problema y hacer más eficiente el proceso.

Como ya sabemos la red Blockchain es un libro mayor universal presente en una red distribuida que es accesible para todos en la red. De tal forma, cada nodo dispone de una copia completa de toda la base de datos y cualquier modificación tendrá que ser debidamente verificada por otros nodos/partes para validarla.

Esto implica que con la implementación de la tecnología blockchain en las transferencias de fondos sería necesaria la existencia de un consenso entre los nodos para efectuar las operaciones, y como hemos analizado estos sistema de consenso a través de diferentes procedimientos aseguran que el consenso alcanzado no sea fraudulento y por tanto elimina el riesgo de ciberataques como el sufrido por la red SWIFT, la más extendida red de transferencias entre bancos (Achanta, 2018).

Según Achanta (2018), la red Blockchain trae consigo los siguientes beneficios en el ámbito de las transferencias de fondos:

- Las operaciones se realizan entre las dos partes de la red sin la necesidad de que exista ningún tipo de entidad intermediaria que participe.
- Al no haber entidad intermedia, los costes se reducen al mínimo durante el proceso. Desaparecen las comisiones y gastos de gestión vinculados a la actuación de terceras partes.
- Por ser una relación directa entre las partes, el proceso se agiliza muy considerablemente (prácticamente inmediato) ya que no hay horarios ni fechas en las que no se puedan realizar las transacciones. Además, al no ser necesaria la actuación de entidades de control, se suprimen los procesos tradicionalmente realizados por estas, reduciendo así el tiempo de ejecución de la operación.
- Al ser operaciones realizadas en la red Blockchain, todos los datos de las operaciones están encriptados siendo imposible acceder a ellos sin conocer las claves de los usuarios involucrados, lo cual ofrece un alto nivel de seguridad.

En resumen, podemos ver como todos los problemas que hemos analizado respecto de las transacciones realizadas por procesos “tradicionales” (plazos, coste y seguridad) son eliminados con la implementación de la tecnología Blockchain.

Aunque como hemos analizado la tecnología Blockchain elimina los principales problemas actuales respecto de las transferencias de fondos, aún no es muy extendido su uso en esta materia.

Sin embargo, uno de los gigantes bancarios del planeta, el banco Santander, se ha unido a la red blockchain Ripple para lanzar una aplicación que permita pagos internacionales instantáneos y con bajas comisiones (Solé, 2018). Este nuevo servicio denominado “Santander One Pay FX”, permite a los clientes del banco realizar transferencias internacionales en la mayoría de los casos en el mismo día. Con este nuevo servicio el Santander se convirtió en el primer banco en ofrecer a sus clientes una aplicación basada en blockchain para el pago internacional de fondos (Banco Santander, 2018).

5.2. Financiación de empresas a través de ICOs.

La formación y crecimiento de pequeñas empresas suele estar muy limitado por la falta de financiación, en especial, las empresas tecnológicas que requieren de un gran capital esencial para su supervivencia (Colombo & Grilli, 2007). Una de las decisiones fundamentales de los proyectos de emprendimiento es encontrar y elegir una fuente de financiación, teniendo en cuenta el papel fundamental que puede tener en el futuro de la empresa.

En este contexto, en el mundo de las start ups se está comenzando a utilizar como forma de financiación las Initial Coin Offering (ICOs). A través de las ICOs, las empresas levantan fondos por medio de una venta previa de “tokens” que posteriormente ofrecen acceso a un producto o servicio determinado (Li & Mann, 2018). Lo que hacen estas empresas es asegurar a los inversores que estos tokens van a ser en el único medio de intercambio para poder acceder a los futuros productos y servicios, aunque no se establece ningún compromiso en cuanto al precio de estos futuros servicios (Catalini & Gans, 2019).

Una de las grandes ventajas que ofrece este modo de financiación es que al estar basado en la tecnología blockchain, los aspectos característicos de esta se trasladan al proceso de fundación de las empresas, es decir, transparencia, inmutabilidad, descentralización y apertura (Kher, Terjesen, & Liu, 2021)

Una de las principales ventajas de las ICOs, es la democratización del acceso a la inversión a escala global, posibilidad de diversificación y la posibilidad de participar en las fases iniciales de financiación de proyectos con gran potencial (Chen Y. , 2018) y, por otra parte, la inversión en activos que se intercambian en *crypto exchanges* (Montaz, 2020).

Sin embargo, también presentan ciertas desventajas y riesgos. Las ICOs pueden generar un coste de oportunidad para los emprendedores, ya que una parte considerable de los tokens del proyecto es vendida en la fase inicial, cuando la valoración del proyecto es baja (PwC, 2017).

Los inversores se someten a un alto riesgo ya que las ICOs suelen producirse en la fase de diseño de un proyecto, basado su *white paper*, lo que implica que a un no existe un innovación, producto o clientes (EY, 2018). Además, en los mercados secundarios (*crypto exchanges*) el valor de los tokens está sujeto a una gran volatilidad y especulación (Cappa & Pinelli, 2020). Por último, es muy difícil para los inversores evaluar correctamente los proyectos debido a los problemas de asimetría en la información (Chen K. , 2019).

De esta forma, podemos afirmar que las ICOs son una muy buena opción para la financiación de nuevos proyectos pero que presentan una serie de riesgos, sobre todo para los inversores, que han de evaluarse muy cuidadosamente antes de llevar a cabo una ICOs (desde el punto de vista del emprendedor) o una inversión en uno de estos proyectos.

Por ejemplo, Nostrum una empresa dedicada a la venta de comida preparada a sus clientes, decidió emitir una ICO para financiar sus proyectos creando su propia criptomoneda, el Meal Token, con la que pretendió captar 50 millones de euros a razón de 0,15 euros cada moneda. En el *white paper* del proyecto, además de ofrecer una detallada explicación de la inversión del dinero recaudado (multiplicar el número de

tiendas o permitir utilizar los Meal Tokens como forma de pago para clientes), se advertía de los riesgos asociados a la propia operación de financiación (Boar, 2018).

Otro ejemplo es el de la famosa empresa fotográfica Kodak que, en enero de 2019, decidió lanzar un ICO para crear su criptomoneda KODAKCoin con la que la empresa pretendía que los pagos se simplificaran y fueran más rápidos, puesto que al ser transacciones en las que los procesos de licencia tienen mucha importancia, a través de la tecnología blockchain, cada parte interesada (comprador, vendedor y propietario de los derechos) recibiría su parte simultáneamente según el smart contract recogido en la red blockchain de Kodak (Calvo, 2019).

5.3. Otras mejoras.

- **Sistemas de información de crédito bancario:**

En ocasiones los sistemas de información crediticia de las entidades bancarias presentan ineficiencias por la escasez y la mala calidad de los datos, la dificultad para que esos datos se transmitan entre entidades y por la falta de claridad sobre la propiedad de los datos de los usuarios.

Ante este problema, la tecnología blockchain ofrece una posible solución puesto que puede ser de gran utilidad para establecer la propiedad de los datos. Como sabemos la tecnología blockchain estaba basada en la criptografía que cifra la información y la mantiene inalterada. Esto, podría garantizar que la información es genuina y confiable además de reducir los costes ligados a la obtención y gestión de datos (Guo & Liang, 2016).

Esto permitiría a las entidades crediticias elaborar perfiles correctos de potenciales clientes, que permitieran tomar decisiones respecto a la concesión de créditos a los clientes.

- **Optimización de las *supply chain* (cadenas de suministro):**

Dentro de las cadenas de suministro existe una gran cantidad de inspecciones y transacciones manuales en procesos en los que hay involucrados un gran número de intermediarios, un riesgo elevado de transacciones ilegales, muy altos costes y una baja eficiencia (Guo & Liang, 2016).

En este sentido, la tecnología blockchain podría ser de gran ayuda para reducir los costes de las partes involucradas en las cadenas de suministro. Esta tecnología podría reducir enormemente las intervenciones manuales y utilizar *smart contracts* para digitalizar los procedimientos de la cadena. Teniendo a proveedores, compradores y bancos y sus transacciones registradas sobre la una red blockchain, los *smart contracts* podrían asegurar que los pagos se hicieran automáticamente siempre dentro de unos tiempos y resultados predeterminados, eliminando así la necesidad de intervenciones de personas y el papeleo en el proceso (Guo & Liang, 2016).

Por ejemplo, el gigante estadounidense de grandes almacenes Walmart, en el año 2016 se unió a IBM para crear una red destinada a rastrear y localizar el origen de los productos alimenticios que posteriormente se comercializarían en las tiendas, con el objetivo de poder localizar y frenar posibles enfermedades alimentarias o cualquier tipo de problema asociados a los alimentos. En la actualidad determinar cuál es el origen de estas posibles enfermedades es una tarea que en el mejor de los casos toma semanas y poner en conocimiento de todos los establecimientos que recibieron el producto un posible problema con este, es una compleja tarea (Hackius & Petersen, 2017).

Pero con la innovación propuesta por Walmart e IBM, toda la información relativa al origen, fecha de caducidad y detalles de envío se encuentra disponible a través de la red a la que están conectadas todas las tiendas, de forma que, si existe algún problema con un alimento, todos los establecimientos inmediatamente reciben el aviso y pueden retirar los productos inmediatamente.

- **Votaciones a través de blockchain.**

Entorno a los procesos democráticos de decisión a través de votación, siempre ha habido rumores o sospechas sobre su manipulación, ya sea en empresas o en estados (por ejemplo, en las elecciones de 2020 a la presidencia de Estados Unidos hubo un gran debate y desconfianza, por parte de un sector de la población, en relación con los resultados que dieron como vencedor al actual presidente Joe Biden).

En este sentido, la tecnología blockchain ofrece un sistema totalmente seguro pues, tan pronto como el voto es emitido, el voto queda registrado en la red sin que pueda ser modificado (inmutabilidad propia de las redes blockchain) y sin que la misma persona pueda volver a votar (Boar, 2018).

Este procedimiento tiene una aplicación en el sector público, por ejemplo, en votaciones como la mencionada anteriormente, a la presidencia del gobierno de estados, pero también tiene una gran aplicación en el sector privado.

Así, el Banco Santander introdujo una gran innovación al aplicar la tecnología blockchain en las votaciones de las juntas de accionistas. Las grandes empresas cotizadas, como el Banco Santander, tienen su capital dividido en millones de acciones a las cuales (no a la totalidad) les corresponde un derecho de voto que frecuentemente es delegado. Este sistema es complejo y dado a producir errores. Sin embargo, a través de la tecnología blockchain, el control de los votos es absoluto y totalmente seguro, lo cual minimiza enormemente los errores (Boar, 2018).

6. Futuros retos y obstáculos de la tecnología blockchain.

La tecnología blockchain como hemos analizado presenta un gran número de opciones y oportunidades que pueden tener un enorme y positivo impacto en el sistema financiero y la economía en general, pero es cierto que hay ciertos aspectos de esta que suponen una serie de obstáculos que son necesarios de analizar para poder concluir si es posible que esta tecnología termina por implementarse.

- **Conflictos legales:**

Los *smart contracts*, como sabemos, son contratos de ejecución automática que están programados sobre la red blockchain. Aunque estos presentan un gran número de ventajas, acarrear ciertos aspectos que limitan su aplicabilidad.

La mayor parte de los problemas de los smart contracts está relacionada comuna de sus principales virtudes, la inmutabilidad. Al no poder ser modificados a posteriori, si existe algún tipo de error en la programación de estos contratos, este se celebrará con ese error lo cual puede suponer unos gastos para las partes involucradas que no podrán evitarse por no poder alterar el contrato. Por otra parte, el hecho de que sea inmutable requiere que de inicio el contrato prevea todas alas posibilidades que pueden afectar a la relación contractual, lo cual parece imposible, pues no podemos conocer todos los posibles aspectos que podrían afectar al contrato. De ahí surge una fuerte crítica frente a los contratos tradicionales, que sí pueden ser modificados y adaptarse a la realidad de la relación contractual (Sánchez, 2020).

- **Escalabilidad:**

Las redes blockchain funcionan adecuadamente cuando el número de usuarios es relativamente reducido, a la hora de integrar blockchain como una tecnología que sustituya los sistemas actuales en los que sustenta el sistema financiero, estaríamos hablando de una integración masiva de usuarios, lo cual provocaría una ralentización de procesos que eliminaría una de sus principales ventajas, la rapidez y eficacia de la red.

- **Alto nivel de consumo de energía:**

Como analizamos al estudiar la prueba de consenso que utiliza la red de Bitcoin, Proof of Work, explicamos que se basaba en el poder computacional, lo que implica que

constantemente hay potentes ordenadores conectados a la red trabajando sin parar para poder llevar a cabo el minado. Esto se traduce un enormemente elevado consumo de energía que implica altos costes para los mineros y una gran demanda de energía muy relacionada con altos niveles de contaminación.

Esto está provocando que numerosas organizaciones se posicionen en contra de esta tecnología por sus consecuencias contra el medio ambiente y el consumo de energía.

- **Falta de regulación:**

Aunque como hemos analizado la tecnología blockchain por sí misma ofrece un alto grado de seguridad gracias a los sistemas de criptografía en los que se sustenta, el hecho de que no exista una regulación oficial o común entorno a las transacciones que se realizan sobre esta red provoca una gran incertidumbre entre los usuarios actuales y los potenciales o usuarios a los que se pretende llegar. Este factor está muy relacionado con los siguientes.

- **Percepción pública de tecnología:**

Al tratarse de una tecnología relativamente nueva y tan compleja, la mayor parte del público no la conoce o no sabe como funciona o ni si quiera se fía de ella por no comprenderla.

Además, la tecnología blockchain en sí carece de un buen marketing que ayude a entenderla y la traslade al público general lo cual ralentiza y dificulta la necesaria aceptación por parte del público (Iredale, 2021).

- **Vinculación con la actividad criminal:**

El hecho de que an las transacciones dentro de las redes blockchain se mantenga el anonimato de los usuarios atrae a un gran número de criminales que utilizan estas redes para hacer pagos vinculados con actividades criminales, lo cual afecta enormemente a la reputación, la percepción y la integración de esta tecnología dentro de los sistemas actuales en los que los usuarios comunes operan (Iredale, 2021).

7. Consideraciones.

Habiendo analizado en sí la tecnología, algunas de sus posibilidades de implementación en el sistema actual y los retos y dificultades a los que se enfrenta la tecnología blockchain, es interesante hacer una comparativa entre la parte digital más novedosa y la parte analógica que la tecnología blockchain pretende revolucionar.

En relación con las transferencias de capitales sobre todo en operaciones internacionales, es cierto que la tecnología blockchain ofrece una serie de características que mejoran y potencian los procesos, pero la principal diferencia que encontramos respecto al sistema actual es referencia a dos de los problemas que hemos mencionado con respecto al blockchain, la escalabilidad y la confianza o percepción pública.

En primer lugar, respecto a la escalabilidad, teniendo en cuenta el número de operaciones que se realizan por día y la importancia y urgencia que pueden tener, trasladar este volumen de operaciones a plataformas que pueden tener problemas a la hora de gestionarlas, puede resultar en un colapso financiero de muy negativas consecuencias. Por eso, hasta que la tecnología no se encuentre en un punto más avanzado y depurado parece lógico mantener el sistema actual que, aunque implica mayores tiempos de espera y costes, ofrece a los usuarios un sistema que se ha probado funcional y eficiente. La mejor opción podría ser la de un sistema híbrido que poco a poco se fuera adaptando a la nueva tecnología blockchain, como ya está haciendo el Banco Santander.

Por otra parte, la desconfianza hacia la nueva tecnología y la incertidumbre que la rodea, inclina la balanza hacia el sistema actual en el que la mayoría de los usuarios confían para gestionar su patrimonio.

En la comparación entre el mundo digital y analógico, existe un elemento social e incluso generacional. Debido a la complejidad de la tecnología, dentro de los que podríamos considerar como el usuario medio, el porcentaje de estos que verdaderamente comprende el funcionamiento de esta tecnología es muy reducido. También ocurre con aquellas personas de generaciones más avanzadas, que no con la tecnología blockchain si no con los sistemas tecnológicos actuales, presentan dificultades y, en ocasiones, imposibilidad para poder gestionar sus operaciones.

Es por esto por lo que, aunque la tecnología blockchain trae consigo una serie de positivas revoluciones a lo establecido actualmente y su implementación sería algo positivo para el sistema financiero en general, la convivencia con una parte del sector más tradicional es necesaria para poder atender las necesidades de todos los usuarios que forman parte del sector financiero.

8. Conclusiones.

Durante la elaboración de este trabajo hemos llevado a cabo una serie de estudios y análisis que nos han permitido entender y valorar los elementos positivos y revolucionarios de la tecnología blockchain, así como aquellos factores que pueden suponer complicaciones para la implementación de la tecnología. A continuación, comentaremos a modo de conclusión las ideas más relevantes que han sido desarrolladas en este trabajo:

1. Las características más importantes del blockchain que hacen de esta una tecnología diferencial son: la descentralización, la distribución y la inmutabilidad. Estas características permiten que esta tecnología, como hemos analizado, son las que sustentan la seguridad y veracidad de las redes blockchain.
2. Otro de los elementos esenciales que fundamentan el funcionamiento de esta tecnología, haciendo la tarea de verificar toda la información sobre las transacciones que se dan en la red, es el protocolo de consenso. Existen diferentes protocolos con los que funcionan las redes blockchain, siendo los más importantes el protocolo Proof of Work (PoW) y Proof of Stake (PoS). Habiendo analizado ambos mecanismos, parece que el futuro de la tecnología blockchain pasa por el uso del protocolo PoS en lugar del PoW (que utiliza blockchain), ya que elimina el problema de la excesiva demanda de energía y recorta el tiempo de comprobación de las transacciones con respecto al PoW.
3. Otros conceptos de gran importancia dentro de la tecnología blockchain son: la firma digital (distinta de la que usamos para realizar trámites, que permiten firmas o sellar para transmitirlo por la red sin que se pueda acceder, salvo por el destinatario de la operación, o ser modificado), la minería y el consenso (que permite verificar que las transacciones realizadas por los mineros son veraces)
4. Podemos diferenciar diferentes tipos de redes en función del tipo de acceso a la propia red: públicas (accesibles en internet por cualquier persona), privadas (necesaria autorización para acceder a la red) e

híbridas que combinan las principales características de las dos anteriores (solicitan autorización para acceder, pero el acceso al libro de registro de las operaciones es público).

5. Dentro del amplio concepto de la tecnología blockchain, existe uno de los elementos más relevantes y conocidos por el usuario medio, las criptomonedas. Las criptomonedas son activos digitales que sirven como mecanismo de intercambio dentro de las redes blockchain, mientras que la blockchain es la red o sistema informático en el que se sustentan. Es esencial conocer que son dos conceptos estrechamente relacionados pero muy diferentes.
6. Dentro de las criptomonedas encontramos diferentes modalidades: *mecanismos de transacción* (dentro de los que se encuentre Bitcoin), *distributed computation tokens* (donde se encuentra Ether, la criptomoneda de la red Ethereum), *utility tokens* (criptoactivo muy frecuente en la financiación de empresas y start ups), *security tokens* (estos son valores que ofrecen a los inversores diferentes derechos financieros), *fungible tokens* (como se desprende de su denominación, son criptoactivos todos iguales entre ellos, intercambiables y divisibles), *non fungible tokens* (son activos totalmente únicos e irrepetibles, muy útiles a la hora de demostrar la autoría y/o propiedad de elementos en la red) y, por último, *stable coins* (criptoactivos colateralizados que con otros activos que tratan de minimizar la alta volatilidad de los criptoactivos).

Por actuar como medio de pago en operaciones, los tokens que tienen función de mecanismo de transacción son los que un sentido más general van a tener una mayor utilidad en nuestro sistema financiero. Sin embargo, otros tokens como los non fungible tokens que tienen una funcionalidad mucho más específica, cumplen una función esencial para la protección de ciertos ámbitos económicos como los derechos de autor y las consecuencias económicas que derivan de estos. También, los utility tokens que también cumplen una función específica en el

funcionamiento de las ICOs que como hemos analizado tienen un enorme potencial a la hora de la financiación de empresas y proyectos.

Podríamos decir que cada uno de estos tipos cumplen una función específica que conjuntamente cubren una gran parte de los campos más importantes del sector financiero (transacciones, financiación, etc.).

7. Las criptomonedas actualmente más importantes a nivel de valor y proyección son: Bitcoin, criptomoneda que surge en 2008 y que es la protagonista de la revolución tecnológica que han provocado las redes blockchain y las criptomonedas y, Ether criptoactivo de la plataforma de segunda generación Ethereum, que introdujo una serie de novedades a la tecnología blockchain que dieron un gran valor a Ether.

Aunque Bitcoin sigue siendo a nivel de valor, popularidad y aceptación la criptomoneda más relevante, Ethereum con ofreciendo más posibilidades que Bitcoin (Dapps, smart contracts, etc.) y con un funcionamiento más sostenible, parece destinada a superar a Bitcoin.

Es por eso por lo que Bitcoin, para mantenerse dentro del enorme mercado de las criptomonedas, debería de reformular alguno de los aspectos en los que se basa y de las funcionalidades que ofrece para mantenerse al ritmo de nuevos proyectos que surgen constantemente.

8. Las Fintech hacen referencia a aquellas empresas que hacen uso de la tecnología financiera para ofrecer servicios financieros. El papel de las Fintech relacionado con la tecnología blockchain es muy importante en la transformación del sector financiero, porque precisamente estas empresas utilizan la tecnología e información financiera para ofrecer sus servicios.

Las Fintech van a tener una gran relevancia en todos aquellos aspectos en los que la transferencia de fondos sea necesaria, ya sea: préstamos y créditos en línea como crowdfunding y préstamos entre personas; los servicios de banca online de las entidades bancarias; pagos en línea, en un sistema cada vez más volcado al Ecommerce; plataformas de

inversión en línea, que permiten realizar inversiones a través de dispositivos móviles y ordenadores, como la conocida Robinhood o eToro.

9. En cuanto a las posibilidades de implementación de la tecnología blockchain y las criptomonedas en el sistema financiero:

- **Blockchain como sistema para realizar transferencias de fondos.** Sobre todo, en el ámbito de las transferencias internacionales que como consecuencias de diferentes factores que hemos analizado, son relativamente lentas e inseguras, la tecnología blockchain que ofrece un sistema caracterizado por la seguridad de los procesos en los que se basa y la velocidad de las transacciones, ofrece un sistema alternativo al actual más eficiente, rápido y seguro, y menos costoso en términos de comisiones.
- **Blockchain como alternativa a la financiación de empresas a través de ICOs.** La tecnología blockchain junto a las criptomonedas, abren un nuevo campo de posibilidades a la financiación de nuevos proyectos empresariales, sobre todo en el sector tecnológico. A través de estos mecanismos, las empresas reciben la financiación necesaria a cambio de tokens que en el futuro cuando la empresa esté en funcionamiento podrán intercambiarse por productos o servicios.
- **Sistemas de crédito financiero.** Gracias a la tecnología blockchain, la captación y veracidad de los datos es más segura y fiable, lo que permite que los perfiles sobre clientes en las entidades bancarias sean más precisos minimizando así los riesgos asociados a la concesión de créditos.
- **Mejora en las cadenas de suministro.** Las cadenas de suministro están formadas por una serie de procesos en los que existe una considerable intervención manual y “papeleo”. Así, la automatización de procesos y custodia inmutable que proporciona la tecnología blockchain, permite optimizar en gran medida estos

procesos, eliminando los fallos humanos y el mal hacer de individuos durante el proceso.

10. Por último, es importante destacar las dificultades a las que se enfrenta la tecnología blockchain en su proceso de implementación. Algunos de los obstáculos más importantes más relevantes son:

- **Problemas legales** por la falta de regulación y la poca tradición legal que existe en este ámbito.
- **Escalabilidad** debido al creciente número de usuarios de las redes blockchain, que a los niveles actuales ya comienzan a mostrar fallas en su funcionamiento.
- **Problemas medioambientales** por el alto consumo de energía necesario para el funcionamiento de redes como Bitcoin, debido al mecanismo de consenso en el que se basa.
- **Percepción pública**, debido a la complejidad y novedad de esta tecnología, el público común no llega a conocer el funcionamiento de esta tecnología y existe una considerable falta de fiabilidad por parte del público general.
- **Alto grado de vinculación criminal**, como consecuencia del anonimato que estas redes confieren a los usuarios y la falta de regulación y control, esta es una tecnología que se ha demostrado que es utilizada como mecanismo para realizar intercambios vinculados con actividades criminales.

11. A grandes rasgos, cuando comparamos la nueva y disruptiva tecnología blockchain con el sistema actual e incluso el trato personal, aún necesario en nuestro sistema, parece que el punto débil de uno es el fuerte de otro. Es decir, aunque la tecnología blockchain trae consigo grandes avances en seguridad, rapidez y ahorro de costes, como ya hemos analizado, esta sigue siendo una tecnología muy distante y compleja para la mayor parte del sector financiero que se muestra reticente a adoptarla. Esto hace que

el sistema más tradicional que, aunque sufre, entre otros, problemas de ineficiencias y falta de seguridad, sea aun absolutamente necesario para el mantenimiento y para la propia implementación de nuevas tecnologías en el sistema financiero.

Bibliografía

- Achanta, R. (2018). *Cross-Border money transfer using Blockchain - Enabled by Big Data*. Infosys. Retrieved from <https://www.infosys.com/industries/cards-and-payments/resources/Documents/cross-border-money-transfer.pdf?msclkid=b3d269a2cf7811ec8d88af9f0a827f49>
- Aljabr, A. A., Sharma, A., & Kumar, K. (2019). *Mining Process in Cryptocurrency Using Blockchain Technology: Bitcoin as a Case Study*. Retrieved from https://www.researchgate.net/publication/338014144_Mining_Process_in_Cryptocurrency_Using_Blockchain_Technology_Bitcoin_as_a_Case_Study
- Anyfantaki, S. (2016). *The Evolution of Financial Technology (FINTECH)*. Economic Bulletin.
- Atico, G. (2022, febrero 16). Retrieved from El smart contract o contrato inteligente: <https://protecciondatos-lopd.com/empresas/smart-contract/>
- Banco Santander. (2018). *Santander launches the first blockchain-based international money transfer service across four countries*. Madrid.
- Barros, D. (2020). *Uncommon Finance*. Retrieved from ANT FINANCIAL, UNA "STARTUP" DE 150 BILLONES DE DÓLARES: <https://uncommonfinance.com/ant-financial-alipay/>
- BBVA. (2022, marzo 3). Retrieved from ¿Quién domina el mundo de las 'DApps'? : <https://www.bbva.com/es/quien-domina-el-mundo-de-las-dapps/>
- Berentsen, A., & Schär, F. (2019). *The Economics of Fintech and Digital Currencies*.
- Bit2me . (2022, Enero 7). Retrieved from ¿Qué es un Nonce?: <https://academy.bit2me.com/que-es-nonce/>
- Bit2me. (2022, enero 16). Retrieved from ¿Qué es Prueba de participación / Proof of Stake (PoS)? : <https://academy.bit2me.com/que-es-proof-of-stake-pos/>
- Bit2me. (2022). *Bit2me*. Retrieved from Cuántos tipos de blockchain existen: <https://academy.bit2me.com/cuantos-tipos-de-blockchain-hay/>
- Boar, A. (2018). Efectos de la tecnología blockchain en el sector financiero y empresarial. *Revista de Contabilidad y Dirección* , 27. Retrieved from

https://accid.org/wp-content/uploads/2019/04/Efectos_de_la_tecnolog%C3%ADa_blockchain_en_el_sector_financiero_y_empresarial_A_Boarlogo.pdf

Briggs, K. (2018). *Taming the Wild West: How the SEC Can Legitimize Initial Coin Offerings ("ICOs"), Protect Consumers from Bad Actors, and Encourage Blockchain Development*. 2 Bus. Entrepreneurship & Tax L. Rev. 424. Retrieved from <https://scholarship.law.missouri.edu/betr/vol2/iss2/9>

Calvo, M. (2019, julio 1). *Kodak lanza un sistema de gestión de documentos basado en Blockchain*. Retrieved from Blockchain Services: <https://www.blockchainservices.es/novedades/kodak-lanza-un-sistema-de-gestion-de-documentos-basado-en-blockchain/>

Cappa, F., & Pinelli, M. (2020). *Collecting money through blockchain technologies: first insights on the determinants of the return on Initial Coin Offerings*. Information Technology for Development. doi:<https://doi.org/10.1080/02681102.2020.1801564>

Catalini, C., & Gans, J. S. (2019). *INITIAL COIN OFFERINGS AND THE VALUE OF CRYPTO TOKENS*. NATIONAL BUREAU OF ECONOMIC RESEARCH. Retrieved from <http://www.nber.org/papers/w24418>

Chen, K. (2019). *Information asymmetry in initial coin offerings (ICOs): Investigating the effects of multiple channel signals*. Electronic Commerce Research and Applications. doi:<https://doi.org/10.1016/j.elerap.2019.100858>

Chen, Y. (2018). *Blockchain tokens and the potential democratization of entrepreneurship and innovation*. Business Horizons. doi:<https://doi.org/10.1016/j.bushor.2018.03.006>

CoinMarketCap. (2022, Marzo 14). Retrieved from <https://coinmarketcap.com/es/currencies/bitcoin/>

Colombo, M., & Grilli, L. (2007). *Funding Gaps? Access To Bank Loans By High-Tech Start-Ups*. Small Business Economics. doi:<https://doi.org/10.1007/s11187-005-4067-0>

- Cryptohitscompra*. (2022). Retrieved from <https://cryptoshitcompra.com/larva-labs-se-esta-preparando-para-una-posible-demanda-por-infraccion-de-derechos-de-autor-de-nft>
- Deloitte. (2019). *Security token offerings: The next phase of financial market evolution?*
- Díaz, Y., & Cueva, J. M. (2018). *Análisis de la función Hash Criptográfica en cadenas de bloques y su impacto en la seguridad de transacciones de datos*. *Redes de Ingeniería*. doi: <https://doi.org/10.14483/2248762X.14383>.
- EY. (2018). *Big risks in ICO market*. Retrieved from <http://www.ey.com/gl/en/newsroom/news-releases/news-ey-big-risks-in-ico-market-flawed-token-valuations-unclear-regulations-heightened-hacker-attention-and-congested-networks>
- Gomber, P., Koch, J.-A., & Siering, M. (2017). *Digital Finance and FinTech: current research and future research directions*. Retrieved from <https://link.springer.com/content/pdf/10.1007/s11573-017-0852-x.pdf>
- Guo, Y., & Liang, C. (2016). *Blockchain application and outlook in the banking industry*. *Financial Innovation*. doi:<https://doi.org/10.1186/s40854-016-0034-9>
- Hackius, N., & Petersen, M. (2017). *Blockchain in Logistics and Supply Chain: Trick or Treat?* Hamburg International Conference of Logistics (HICL). Retrieved from https://tore.tuhh.de/bitstream/11420/1447/1/petersen_hackius_blockchain_in_sc_m_and_logistics_hicl_2017.pdf
- Iredale, G. (2021). *Top 10 Blockchain Adoption Challenges*. 101 Blockchains. Retrieved from <https://101blockchains.com/blockchain-adoption-challenges/>
- K. Hardle, W., R. Harvey, C., & C.G. Reule, R. (2019). *Understanding Cryptocurrencies*. Berlin.
- Karandikar, N., Chakravorty, A., & Rong, C. (2021). *Blockchain Based Transaction System with Fungible and Non-Fungible Tokens for a Community-Based Energy Infrastructure*. Basel. doi:<https://doi.org/10.3390/s21113822>
- Kher, R., Terjesen, S., & Liu, C. (2021). *Blockchain, Bitcoin, and ICOs: a review and research agenda*. *Small Business Economics*. doi:<https://doi.org/10.1186/s40854-016-0044-7>

- King, S., & Nadal, S. (2012). *PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake*. Retrieved from <https://decred.org/research/king2012.pdf>
- Kuchovsky, C., Gómez, G., Díez, D., & Molero, I. (2017). *Blockchain: La revolución industrial de internet*. Barcelona: Grupo Planeta.
- Lee, S. (2015). *Fintech and Korea's Financial Investment Industry*. Korea Capital Market Institute.
- Leong, K., & Sung, A. (2018). *FinTech (Financial Technology): What is It and How to Use Technologies to Create Business Value in Fintech Way?* International Journal of Innovation, Management and Technology.
- Li, J., & Mann, W. (2018). *Initial Coin Offering and Platform Building*. SSRN Electronic Journal. . doi:<https://doi.org/10.2139/SSRN.3088726>
- Lloyd, J. (2020). *¿Qué factores causan la volatilidad de Bitcoin?* Retrieved from <https://es.beincrypto.com/aprende/que-factores-causan-volatilidad-bitcoin-btc/>
- Luu, J., & Imwinkelried, E. J. (2016). *The Challenge of Bitcoin Pseudo-Anonymity to Computer Forensics*. Thomson Reuters. Retrieved from <https://heinonline.org/HOL/LandingPage?handle=hein.journals/cmlwbl52&div=11&id=&page=>
- Merlo, I. (2016, Septiembre 2016). *¿Cuánto tarda una transferencia internacional en hacerse efectiva?* Retrieved from HelpMyCash: <https://www.helpmycash.com/blog/cuanto-tarda-una-transferencia-internacional-hacerse-efectiva/#:~:text=Habitualmente%2C%20una%20transferencia%20internacional%20suele%20hacerse%20efectiva%20entre,destinatario%20puede%20variar%20en%20funci%C3%B3n%20de%20dif>
- Metcalfe, W. (2020). *Ethereum, Smart Contracts, DApps*. Tokyo: Blockchain and Crypt Currency, Economics, Law, and Institutions in Asia Pacific. doi:https://doi.org/10.1007/978-981-15-3376-1_5
- Milian, E. Z., Spinola, M. d., & Carvalho, M. M. (2019). *Fintechs: A literature review and research agenda*. Sao Paulo: Department of Production Engineering, University of Sao Paul.

- Modi, R. (2018). *Introduction to Blockchain, Ethereum and Smart Contracts*. Medium. Retrieved from <https://medium.com/coinmonks/https-medium-com-ritesh-modi-solidity-chapter1-63dfaff08a11>
- Montaz, P. P. (2020). *Initial Coin Offerings*. PLOS ONE. doi:<https://doi.org/10.1371/journal.pone.0233018>
- Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*.
- Newtown Partners. (2019). *Security tokens: a primer*. Retrieved from https://www.newtownpartners.com/wp-content/uploads/2019/01/NTP-Security-Tokens-Primer_FINAL.pdf
- Palomo-Zurdo, R. (2018). «*Blockchain*»: *la descentralización del poder y su aplicación en la defensa*. Madrid: Instituto Español de Estudios Estratégicos.
- Pralhad, B., & Kaur, H. (2019). *A Comparative Analysis of Blockchain Platforms – Bitcoin and Ethereum*. Pune: International Conference on Computing Communication Control and Automation. Retrieved from <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9129332>
- PwC. (2017). *Introduction to token sales best practices*. PwC. Retrieved from <http://www.pwchk.com/en/financial-services/publications/introduction-to-token-sales-ico-best-practices.pdf>
- Raeesi, R. (2017). *The Silk Road, Bitcoins and the Global Prohibition Regime on the International Trade in Illicit Drugs: Can this Storm Be Weathered?* Glendon Journal of International Studies. Retrieved from <https://yourreview.journals.yorku.ca/index.php/yourreview/article/view/40388>
- Revilla, J. M. (2016 , abril 27). *La plataforma bancaria SWIFT sufre un ciberataque masivo*. Retrieved from ITespresso: <https://www.itespresso.es/plataforma-bancaria-swift-sufre-ciberataque-masivo150908-150908.html>
- Rodas, A., & Núñez, S. (2021). *El Bitcoin: una revisión de las ventajas y desventajas de las transacciones comerciales con dinero virtual*. Ciudad de México: Ciencia Latina Revista Científica Multidisciplinar. doi:https://doi.org/10.37811/cl_rcm.v5i6.1306

- Saéz, J. (2022). *IEBS*. Retrieved from Qué son las DApps o Aplicaciones Descentralizadas y varios ejemplos: <https://www.iebschool.com/blog/dapps-o-aplicaciones-descentralizadas-que-son-y-como-funcionan-finanzas/>
- Sánchez, J. A. (2020). *Blockchain y contratos inteligentes: aproximación a sus problemáticas y retos jurídicos*. *Revista de Derecho Privado*. Retrieved from <http://www.scielo.org.co/pdf/rdp/n39/0123-4366-rdp-39-175.pdf>
- Solé, R. (2018, febrero 1). *Banco Santander lanzara antes de abril una aplicación para mandar dinero bajo la blockchain de Ripple*. Retrieved from Hardwaresfera: <https://hardwaresfera.com/noticias/banco-santander-lanzara-abril-una-aplicacion-mandar-dinero-la-blockchain-ripple/>
- State of the Dapps*. (2022, marzo 8). Retrieved from DApp Statistics: <https://www.stateofthedapps.com/stats/platform/ethereum#new>
- Suárez, M., & Freitag, F. (2020). *Desarrollo de una aplicación descentralizada con Blockchain: Dapp para el acceso y modificación de información sensible*. Barcelona: Universidad Oberta de Catalunya. Retrieved from <http://openaccess.uoc.edu/webapps/o2/bitstream/10609/106746/2/msuareztaTFM0120memoria.pdf>
- Szabo, N. (1994). *Smart Contracts*. Retrieved from <https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html>
- W. Chohan, U. (2021). *Non-Fungible Tokens: Blockchains, Scarcity, and Value*.
- Wu, K., Ma, Y., Huang, G., & Liu, X. (2019). *A First Look at Blockchain-based Decentralized Applications*. Beijing: Key Lab of High-Confidence Software Technology. Retrieved from <https://arxiv.org/pdf/1909.00939.pdf>
- Zheng, Z., Xie, S., Dai, H.-N., Chen, W., Xiangping, C., Weng, J., & Imran, M. (2019). *An Overview on Smart Contracts: Challenges, Advances and Platforms*. Retrieved from <https://arxiv.org/pdf/1912.10370.pdf>
- Zozaya, C., Franzoni, A. L., & Incera, J. (2017). *Blockchain: un tutorial*. Ciudad de México.

