



Facultad de ciencias económicas y empresariales, ICADE

# **La revolución de la tecnología blockchain y las criptomonedas. Análisis de los proyectos más potentes según “sectores” y lo que pueden suponer para el futuro de la economía.**

Nombre: Gonzalo Romeo Sánchez

Tutor: Javier Rivas Compains

## **Resumen**

La *blockchain* ha existido desde los años 90, cuando se elaboró y ejecutó el primer trabajo con esta tecnología. Desde entonces, ha pasado desapercibida hasta hace unos años, concretamente el 2008, cuando apareció el proyecto de moneda digital Bitcoin. Una persona o grupos de personas publicaban, bajo el seudónimo de Satoshi Nakamoto, un documento con las bases para implementar un sistema de pago digital descentralizado directamente entre usuarios. A partir de ese momento, nace el concepto de las criptomonedas, que se va haciendo más conocido según se van creando mas proyectos con la tecnología. Hoy en día, se podría decir que es uno de los temas más populares, debido a su carácter revolucionario que permite conectar a las personas de una manera directa sin entidades centrales, todo gracias a la tecnología *blockchain*. Este hecho abre un abanico de posibilidades sobre los proyectos que se ejecutan y que se pueden desarrollar sobre la cadena de bloques. Ahora queda analizar cual es el potencial de esta tecnología y que tipo de revolución puede suponer en el futuro de la economía, afectando a diferentes sectores de actividad.

## **Palabras Clave**

*Blockchain*, Criptomonedas, descentralización, revolución, cadena de bloques, Bitcoin.

## **Abstract**

The blockchain has existed since the 1990s, when the first work with this technology was developed and executed. Since then, it has gone unnoticed until a few years ago, specifically in 2008, when the Bitcoin digital currency project appeared. A person or groups of people published, under the pseudonym of Satoshi Nakamoto, a document with the basis for implementing a decentralized digital payment system directly between users. From that moment on, the concept of cryptocurrencies was born, which became better known as more and more projects were created with the technology. Today, it is arguably one of the most popular topics, due to its revolutionary character that allows connecting people in a direct way without central entities, all thanks to blockchain technology. This fact opens a range of possibilities about the projects that are executed and that can be developed on the blockchain. Now it remains to analyze what is the potential of this technology and what kind of revolution it can mean in the future of the economy, affecting different sectors of activity.

## **Key words**

Blockchain, Cryptocurrencies, decentralization, revolution, Bitcoin.

## Índice

1. Introducción
  - 1.1 Objetivos
  - 1.2 Metodología
  - 1.3 Estado de la cuestión
  - 1.4 Problemática
  - 1.5 Estructura
2. Introducción tecnología Blockchain
  - 2.1 Explicación técnica Blockchain
  - 2.2 El porqué de la tecnología
  - 2.3 Relación con las criptomonedas
3. Criptomonedas
  - 3.1 Introducción
  - 3.2 Sector 1: Reserva y transferencia de valor
  - 3.3 Sector 2: *Smart contracts* y Dapps
  - 3.4 Sector 3: DeFi (Decentralized Finance)
  - 3.5 Sector 4: *Gaming* & NFTs
4. Conclusión
5. Bibliografía y anexos

## **1. Introducción:**

### **1.1 Objetivos**

El objetivo de este trabajo es analizar la revolución que pueden suponer estas tecnologías en el mundo del futuro, todo desde un punto funcional y no de la inversión. Es cierto que estos activos pueden suponer grandes oportunidades de inversión, pero el objetivo de este trabajo no va sobre eso, sino de lo que esta tecnología podría suponer en el futuro de la economía. Se buscará analizar y evaluar los proyectos más prometedores dentro de cada “sector” (*DeFi*, Contratos inteligentes, Activos de pago, NFTs, etc) y estudiar su potencial impacto tanto en la economía como en la vida en general. Los objetivos mencionados previamente, se buscarán obtener de la siguiente manera: Para poder analizar y entender el impacto real que puede suponer esta nueva tecnología en el mundo empresarial, se llevará a cabo una investigación de tipo cualitativa sobre la tecnología *blockchain* y sus usos en diferentes ámbitos. Las principales fuentes de datos serán los artículos académicos, en los que se buscará todo tipo de información acerca de esta tecnología, que aborde desde varios puntos de vista los aspectos positivos, así como los negativos. Dichos artículos serán extraídos de plataformas como Google scholar o la propia biblioteca de la universidad.

### **1.2 Metodología**

Este trabajo es una investigación académica orientada a conseguir los siguientes objetivos relacionados con la tecnología *blockchain* y las criptomonedas:

- Analizar con profundidad la tecnología *blockchain* para poder entender sus posibles casos de uso, así como el potencial de esta nueva técnica.
- Una vez entendida la tecnología, investigar y analizar los diferentes proyectos que se están desarrollando sobre esta y, otra vez, entender y evaluar el potencial de estos.
- Por otra parte, estudiar en profundidad las criptomonedas ligadas a los diferentes proyectos para determinar el valor “real” del token.
- Por último, continuar con el objetivo principal del trabajo, que es estudiar si la *blockchain* y las criptomonedas pueden suponer una revolución tan grande como la que tuvo internet en su día.

### 1.3 Estado de la cuestión

A lo largo de la historia de la humanidad, siempre hemos sido reticentes a cualquier tipo de revolución. Toda innovación ha conocido en sus inicios la oposición de la gran mayoría de la población. Esto se debe, desde mi punto de vista, al desconocimiento desde el cual afrontamos los cambios los seres humanos. Es mucho más fácil rechazar algo a lo que no estás acostumbrado, que informarte y analizar si de verdad que merece la pena el cambio. De esto hay muchos ejemplos que hoy en día son un éxito pero que en su momento fueron duramente criticados. Uno de los ejemplos más importantes sería el de los ordenadores, de los cuales se decía que nunca iban a tener un uso personal y que solo valdrían para las empresas. A este ejemplo se le suma el de los teléfonos móviles, el internet, el coche eléctrico, etc. Y así muchas más innovaciones que fueron muy criticadas al principio, pero que acabaron suponiendo una revolución. Pues en esa fase es en la que se encuentra actualmente la tecnología *blockchain*. Está claro que no todo lo que tiene que ver con esta tecnología tiene el éxito asegurado, sin embargo, creo que lo más responsable y lógico es tratar de entenderla y analizar la tecnología para así poder valorar su verdadero potencial.

La mayoría de la gente piensa que el origen de la tecnología *blockchain* se remonta al año 2008, cuando un desconocido o grupo de desconocidos bajo el seudónimo de “Satoshi Nakamoto”, publicaron un artículo que definía las claves para crear e implementar una moneda digital: El Bitcoin. Sin embargo, el verdadero nacimiento de esta tecnología se remonta al año 1991, cuando apareció el primer trabajo sobre las transacciones de forma descentralizada, utilizando la criptografía y la tecnología de bloques. Mas tarde en 1998, Wei Dai elaboró una solución descentralizada para poder realizar pagos electrónicos, sin la necesidad de una entidad intermediaria. A partir de ese momento, fue cuando el famoso artículo de Satoshi Nakamoto fue publicado, llegando a convertirse el proyecto en una realidad el 3 de enero de 2009. Esto marcaba el inicio de una nueva era en internet que tendría como principal protagonista a las criptomonedas (*La historia del Bitcoin*, s.f).

La gran revolución de las criptomonedas nace de la posibilidad de no depender de que una entidad central que controle tu dinero y por tanto tus transacciones. Aunque es cierto que hay ciertas criptomonedas que sí registran tus transacciones, como Ripple, la gran mayoría aportan ese aspecto diferencial respecto al dinero tradicional. Hoy en día, cualquier transacción que hagamos, ya sea online o física, está controlada por varios agentes. Por un lado, tienes a las entidades bancarias que recogen y apuntan la transacción con todo tipo de detalles y por otro

lado, las entidades gubernamentales que llevan un control de cuanto, como, donde y cuando gastas tu dinero. Hay un creciente escepticismo alrededor de la reserva de valor del dinero emitido por los bancos centrales, especialmente en momentos como los actuales de políticas de altísima expansión monetaria y su consecuente inflación. Esto está llevando cada vez a más gente a ver como una verdadera oportunidad la alternativa de las criptomonedas, y por consiguiente cada vez a más empresas. Sin embargo, a pesar del indudable potencial que las criptomonedas ofrecen como reserva de valor alternativo a las divisas tradicionales, hoy en día hay que decir que no está el mercado de las criptomonedas asentado lo suficiente como para cumplir ese papel. Actualmente, las criptomonedas son más un bien especulativo que otra cosa, que la gente utiliza para poder sacar un retorno mucho mayor del que sacarían con un activo convencional. Esto se debe a la pequeña capitalización de estas monedas virtuales, su enorme liquidez, y la amplísima adopción de este bien digital, que las hacen muy vulnerables a la especulación, hecho que siembra dudas sobre ellas. Además, entierra a los ojos de muchos analistas una realidad quizá mucho más trascendente para su futura viabilidad, como es que hay una creciente adopción institucional de criptomonedas como Bitcoin o Ethereum por parte de entidades financieras tan reconocidas como Grayscale, Golman Schacs, o empresas como Microstrategy o Tesla.

Por otro lado, y lamentablemente siempre mezclado con esta merecida fama de burbuja especulativa, cada vez hay más gente y empresas que empieza a entender la materia como tecnología excelente para desarrollar proyectos con mucho potencial, más allá del beneficio económico a corto plazo. Para poder entender bien el potencial de este nuevo mundo, hay que diferenciar entre el concepto de criptomonedas y la tecnología *blockchain*. Digamos que, la cadena de bloques es la tecnología que sustenta la posibilidad de que los proyectos se desarrollen de forma descentralizada. Mientras que las criptomonedas, son el token específico de cada ecosistema, y su uso varía según el tipo de proyecto. Esto será explicado en profundidad más adelante.

Por lo tanto, se puede concluir el estado de la cuestión de esta tecnología de bloques, habiéndose explicado su nacimiento y los posibles usos que puede tener. Además, se explica el potencial que pueden tener los proyectos más allá de las criptomonedas.

## **1.4 Problemática**

Estamos en la época del internet 4.0, el conocido como el internet de las cosas. Es precisamente en este momento, en el que empiezan a surgir nuevas tecnologías que podrían revolucionar nuestras vidas. En este contexto aparece la *blockchain*. Algo revolucionario no solo en cuanto a tecnología sino también en cuanto a uso. Queda claro que las mayores ventajas competitivas de la *blockchain* son la descentralización y la desintermediación. Esto nos lleva a centrar el estudio de este trabajo, a la importancia e innovación que supondría esa descentralización en diferentes sectores económicos que conocemos hoy en día. Esta nueva tecnología permite revolucionar muchos tipos de sectores. El más conocido es el del intercambio o reserva de valor, con el Bitcoin. Sin embargo, hay muchos otros tipos de proyectos, que están desarrollados sobre la *blockchain* y que operan en diferentes sectores, como por ejemplo el sector del dinero, con las *stable coins*, o el de los juegos, que funcionan totalmente sobre este tipo de plataformas. Prácticamente cualquier cosa que se pueda hacer online tiene el potencial de hacerse en la *blockchain*, pero con la ventaja de la descentralización. Es precisamente aquí, donde se encuentra el factor revolucionario. Y es que, a día de hoy, puede parecer un poco descabellado pensar que todo a lo que tenemos acceso en la red actualmente, controlado por una empresa, pueda algún día estar controlado por sus usuarios. De esta manera y como explicación básica, el mantenimiento, control y distribución estaría gobernado por los propios usuarios, siguiendo una serie de normas marcadas en el protocolo de la red.

## **2. Introducción tecnología Blockchain**

### **2.1 Explicación técnica Blockchain**

Para poder entender bien cómo funciona la cadena de bloques, hay que tener en cuenta una serie de conceptos básicos, que son el pilar fundamental de esta tecnología. Estos conceptos nos dan una idea general de lo que es la *blockchain*, cómo funciona y porque es algo novedoso. La cadena de bloques es, en su concepción más básica, una base de datos descentralizada e inmutable, sin un repositorio central, mantenida y controlada por las reglas impuestas por los usuarios de la red. A partir de esta definición, aparecen los conceptos clave, que veremos a continuación y con profundidad más adelante en el trabajo.

El primero de estos conceptos es el de la descentralización. Y es que, aunque ya lo hemos mencionado mucho anteriormente, no deja de ser muy importante de cara al verdadero valor de la *blockchain*. Una de las grandes ventajas que ofrece la cadena de bloques es la de poder transmitir y almacenar información sin necesidad de una entidad central. Es decir, todo funciona de manera *peer-to-peer* dado que la red es mantenida y controlada por los usuarios, para los usuarios.

Por otro lado, se encuentra la idea de la inmutabilidad, que es, básicamente, la condición por la que los datos introducidos en la cadena son prácticamente inalterables, y por lo tanto no se pueden cambiar.

También es importante el consenso y operatividad dentro de la red. Al tratarse de una tecnología que basa su utilidad en la descentralización, es de gran importancia la manera en la que se concreten y pacten las normas de funcionamiento de la red. Como se ha mencionado anteriormente, debido a que no hay un organismo central, la cadena de bloques debe tener algún sistema que permita a sus usuarios tomar decisiones. Este sistema varía en función del tipo de *blockchain* del que se trate. Entre los métodos más famosos se encuentran el PoW (*Proof of Work*) y el PoS (*Proof of Stake*).

Como última noción a tener en cuenta, para tener una idea básica de la cadena de bloques, es la de la seguridad. Factor tremendamente importante dentro de esta tecnología, y más si cabe, teniendo en cuenta que todo está en manos de los usuarios sin una autoridad central que se encargue de este apartado. Esto nos lleva a que la cadena de bloques utiliza como método de seguridad la criptografía.

Cabe mencionar que la *blockchain* no está solo restringida al Bitcoin. Esto puede parecer una obviedad, pero es importante mencionar que esta tecnología es mucho más que solo Bitcoin. En efecto, hay más tipologías de aplicación de *blockchain* generalmente conocidas, en función del uso que se le dé. La primera categoría sería la inicial y la más conocida. La relacionada con las divisas, es la que engloba a las criptomonedas. Esta es la más extendida, sin embargo, hay otras que guardan muchísimo potencial sobre las posibles aplicaciones de la cadena de bloques; las *blockchains* con funcionalidad de contratos inteligentes. En este caso, encontramos por ejemplo la red Ethereum, la cual permite la creación y ejecución de *Smart contracts* o contratos inteligentes, lo que abre un abanico de posibilidades. De esto hablaremos más adelante en el trabajo, dado que es uno de los puntos más importantes de la cadena de bloques. Y, por último, tenemos la aplicación de la *blockchain* a ámbitos sectoriales públicos o privados sobre la base

de cadenas de bloques “cerradas o *permissioned*”, que involucren la necesidad de tratar con muchos datos, y que estos deban ser compartidos por todo un ecosistema de empresas y usuarios heterogéneos como, por ejemplo, los asuntos gubernamentales, de la seguridad social, hacienda, etc (Da Silva et al., 2019). También es aplicable a ámbitos como el de los seguros, con el pago automático o las coberturas que dependan de valores como el eurodólar. Esto aprovecharía mas la parte de los contratos inteligentes de la *blockchain*.

Una vez entendidos estos conceptos, pasamos a explicar cómo funciona en profundidad esta tecnología, y cómo estas ideas crean conjuntamente una red de datos infranqueable.

Como ya hemos mencionado, “la cadena de bloques es una base de datos que es compartida por una gran cantidad de usuarios en forma *peer-to-peer* y que permite almacenar y distribuir información de manera inmutable y ordenada” (Dolader, Bel y Muñoz, 2017). Normalmente, para poder añadir información a una cadena de bloques hace falta un consenso entre la mayoría de las partes de la red. Esta es una condición clave de cara a la seguridad de la red. Para poder alterar la información de esta necesitas controlar más del 50% del sistema, por lo tanto, la seguridad no es un tema relacionado tanto con el ámbito tecnológico, sino más con la estadística, debido a su gran cantidad de usuarios. Una vez añadida la información a la cadena, y habiendo transcurrido cierto tiempo, ese contenido se considera prácticamente inmutable. Solo bajo excepciones que supondrían cambios en la red, se podría cambiar el contenido de esta, dando lugar al concepto de *fork*. Un *fork* es una bifurcación en la cadena de bloques, provocada por el intento de añadir un bloque fraudulento o incorrecto a la cadena. Existen dos tipos: *soft forks* y *hard forks*. Ambos cambios en la red suponen una actualización de software por parte de los mineros. Sin embargo, en el caso del *soft fork*, la actualización de software es compatible con versiones anteriores, por lo que las solo haría falta que la mayoría de mineros actualizasen a la nueva versión. Aquellos que no lo hicieran, seguirían siendo capaces de validar transacciones, viendo únicamente reducida su capacidad de minar nuevos bloques. Por otro lado, un *hard fork* implica una actualización de *software* no compatible con las anteriores versiones, por lo que para seguir validando y operando en la red sería necesario disponer de la última versión. Aquellos mineros que rechazasen la actualización quedarían apartados de la cadena, generando así dos *blockchains* diferentes, que seguirían funcionando de manera paralela y totalmente separada, mientras recibieran soporte de sus mineros. Un ejemplo de un *hard fork* es el de Bitcoin y Bitcoin Cash, que ocurrió en 2017, debido a unos cambios en la red que no fueron aceptados por todos los mineros (Banafa, 2020).

La información se va añadiendo a la red en forma de bloques, de ahí el nombre de cadena de bloques. Estos bloques contienen la información y se cierran tras alcanzar un número determinado de transacciones, que varía según el protocolo. Aquí juegan un papel clave los mineros. Los mineros son los encargados del mantenimiento de la red, mediante la validación y creación de nuevos bloques. Más en profundidad, los mineros son nodos de la red que participan en el proceso de escritura y validación de los bloques en la *blockchain* a cambio de una recompensa normalmente económica (Dolader, Bel y Muñoz, 2017). Para poder añadir ese bloque con su información, los mineros restantes tienen que asegurar que su versión coincide con la que se pretende añadir a la cadena. De manera que, si la versión no le cuadra a la mayoría de los nodos, la transacción es rechazada y la acción de añadir el siguiente bloque pasa a otro minero. En este punto aparece una pregunta lógica, si al añadir un bloque, el minero recibe una recompensa, ¿por qué no lo hace todo el mundo? Y si es así, ¿cómo se elige quien lo añade? Bien, pues lo cierto es que solo un nodo puede añadir un nuevo bloque a la red.

La manera de elegir quién lo agrega depende del método de consenso que esté establecido. Los más conocidos son el de PoW (*Proof of Work*) y el de PoS (*Proof of Stake*) aunque también hay otros tipos. Sin embargo, y con el fin de ceñirnos al objetivo del trabajo, estudiaremos solo esos dos tipos de métodos de consenso.

El bitcoin en concreto emplea el más famoso, el conocido como *Proof of work* o prueba de trabajo. Este proceso funciona de tal manera que, para que un nodo pueda agregar un bloque a la red antes que los demás, debe ser el primero en completar un rompecabezas matemático y por lo tanto averiguar el *hash*. Este problema dependerá del tipo de *blockchain*, pero tiene una dificultad ajustable que, en el caso del Bitcoin, se va ajustando para poder cumplir con la media de 10 minutos por emisión de bloque. Esto es de gran importancia debido a que, como ya hemos mencionado, al cerrar un bloque se reparte una recompensa, en este caso bitcoin, por lo que, para cumplir con la emisión de Bitcoin prevista, hace falta un sistema de autoajuste de dificultad. Esto se debe a que cuanto más capacidad computacional tenga un usuario, más fácil tendrá el encontrar el *hash*. Es por ello que existe esa medida, para poder mantener la media de los 10 minutos por bloque y cumplir así con la previsión de la emisión de Bitcoin. La manera en la que esto funciona es la siguiente; un minero aplica su fuerza computacional para intentar encontrar el *hash* antes que nadie. Este número llamado *hash* no se puede descubrir ni calcular de manera analítica, por lo que la única manera de hallarlo es a través de cientos de miles de intentos. Esta es la razón por la que a más capacidad de computación más probabilidad de encontrar el *hash*.

Este método de consenso tiene algunos inconvenientes, lo que está haciendo que muchos proyectos migren a otro tipo de método como el de PoS, del cual hablaremos a continuación. Entre las mayores desventajas de este mecanismo, se encuentra la gran cantidad de energía que consume. Para hacernos una idea, el consumo de energía de la red de Bitcoin supera la de países como Noruega. En la lista mundial de consumo por países, Bitcoin se encontraría en el puesto 29, tan solo 13 puestos por detrás de España, situada en la posición 16 (Pastor, 2021). Este consumo ha sido protagonista de muchas de las críticas que se le achacan a este nuevo instrumento financiero. No obstante, hay un debate sobre el origen de la energía que consume Bitcoin. Si se habla de porcentajes, entre el 50% y el 75% de la energía consumida por Bitcoin proviene de energías renovables (Clementín, 2022).

Por otro lado, se encuentra el problema del potencial ataque del 51%. Debido a la naturaleza de su red y su mecanismo de consenso (PoW), cabe la posibilidad de que la red fuera controlada por un solo individuo o colectivo. Esto se debe a que, cuando se quiere añadir un bloque nuevo, todos los nodos aseguran por mayoría que la versión que se va a añadir es igual que la suya. Por lo tanto, si alguien consiguiera controlar el 51% de la red, podría agregar a la cadena la información que quisiera. Esto es altamente improbable, debido a la gran cantidad de mineros que forman parte de la red. No obstante, cabe mencionarlo como potencial riesgo. Como último gran inconveniente, se encuentra el de las *Mining Pools*. Estas son “asociaciones” de mineros que unen sus fuerzas de computación para así poder incrementar sus posibilidades de conseguir la recompensa, la cual distribuyen entre los miembros de la *pool*. Esto puede no parecer un gran problema, sin embargo, lo es, dado a que ataca directamente al espíritu de la *blockchain*; la descentralización. El hecho de que se junten mineros para sumar fuerzas no hace más que fomentar la centralización, y es que, aunque sea muy complicado conseguir suficiente poder como para controlar la red, sí que cabe la posibilidad de que se creen pocas granjas de mineros con mucho porcentaje de la cadena.

Una vez tratado el principal método de consenso con sus pros y sus contras, pasamos a analizar la otra alternativa más extendida, aunque no la única que existe.

Esta otra alternativa es la de PoS, la cual es la que utilizan redes como la de Ethereum. Este modelo de consenso funciona de manera diferente al de PoW y difiere en una serie de puntos respecto a este mecanismo. El *proof of stake*, conocido en español como prueba de participación, es un estándar que funciona en base a la cantidad de monedas de la red en cuestión, que el minero tiene depositadas. En función de cuanto *stake* tenga el minero en la red,

tendrá más probabilidad de cerrar un bloque, y por lo tanto hacerse con la recompensa. Sin embargo, esto es un arma de doble filo, dado que la cantidad que el validador tiene depositada depende del “comportamiento” de este en la red, es decir, ese depósito está sujeto a lo bien que haga su trabajo el minero. Si llegase el caso de un comportamiento malicioso por parte de este validador, los fondos serían retirados, perdiendo así el capital, además de la capacidad de validar en la red. La gran ventaja que tiene es el ahorro energético que supone respecto al PoW. Esto se debe a que ya no es necesario utilizar grandes esfuerzos computacionales para resolver un problema matemático y así ser el primero en cerrar el bloque.

Podemos dar por finalizada la breve explicación de la tecnología *blockchain*, necesaria para entender y afrontar este trabajo de investigación de manera adecuada.

## **2.2 El porqué de la tecnología**

Una vez explicado brevemente el funcionamiento de esta tecnología pasamos a analizar, desde mi punto de vista, por qué puede suponer una potencial revolución. Todo esto además de identificar las mejoras necesarias para que pueda llegar a completar su potencial.

Hoy en día la información es uno de los activos más valiosos. Las empresas valoran cada vez más tener información de los consumidores, para poder desarrollar sus estrategias de la mejor manera posible. Nuestros datos son comercializados sin ningún tipo de pudor, mientras nosotros utilizamos sus plataformas gratuitas, ya sean redes sociales, páginas webs, correo electrónico, etc. Y es que cuando algo es gratis, significa que nosotros somos el producto.

Por otro lado, todos nuestros datos, por sensibles que sean, están controlados y asegurados por un tercero. Por ejemplo, nuestra cuenta bancaria depende de la seguridad del banco, por lo que, si hay un ataque, nosotros como usuarios debemos fiarnos de sus métodos. Por no mencionar que cuando depositamos nuestro dinero en el banco, no tenemos la certeza de donde se encuentra, ni que se hace con él.

Asimismo, dado que todos estos servicios que utilizamos en internet son propiedad de una compañía, la cual vela por sus propios intereses, los usuarios no tenemos control ninguno sobre las decisiones tomadas sobre estas plataformas. En el caso de que Meta, por ejemplo, decidiese cerrar la app Instagram, los usuarios no tendríamos más remedio que aceptarlo. A esto hay que sumarle que, cuando invertimos en una empresa, los beneficios que generan no son para sus inversores. El inversor se beneficia indirectamente de los resultados de la empresa, pero solo

porque en el mercado hay alguien dispuesto a pagar más de lo que inicialmente se pagó por la misma acción, debido al rendimiento de la compañía. Ciertamente, que existen los dividendos, que son la manera más directa de lucrarse de los beneficios de una organización, sin embargo, estos suelen suponer un porcentaje minúsculo de los resultados totales, además de ser de carácter voluntario por parte de la empresa.

Considerados algunos de los problemas que suponen las empresas y servicios que consumimos hoy en día, procedemos a analizar como la tecnología *blockchain* puede suponer una solución a estas cuestiones.

El objetivo de este trabajo es el de entender como la cadena de bloques puede revolucionar diferentes sectores en el ámbito tecnológico. Más adelante en el trabajo, se procederá a analizar en profundidad y por “sectores” (referido a sectores de actividad como el de los pagos online, los juegos en línea, los Smart contracts, nfts...) el verdadero valor que esta tecnología puede aportar al mundo empresarial del futuro. Por el momento, cabe mencionar que los problemas expuestos anteriormente son fruto de los siguientes motivos: la centralización de los datos y la toma de decisiones, la no participación de los usuarios, la seguridad y la falta de transparencia. Pues bien, la tecnología *blockchain* puede solucionar todos estos problemas en diferentes sectores. Esto se debe a la naturaleza de esta tecnología que, como bien se ha explicado anteriormente, se cimenta sobre los pilares de: descentralización, transparencia, inmutabilidad y seguridad.

Para que esta tecnología llegue a implantarse de manera exitosa, tienen que ocurrir todavía una serie de hechos.

Para empezar, debe existir una regulación acorde a la naturaleza de la red. Es decir, todo lo relacionado con este mundo debe estar regulado, por el bien de los consumidores. Pero siempre desde un punto de vista lo menos intrusivo posible, dado que si no iría contra el espíritu de la tecnología. Asimismo, la población debe educarse y aprender de este nuevo mundo. Es normal que a día de hoy la gente no tenga conocimiento sobre estos temas, dado que es una práctica en auge. No obstante, es de suma importancia tener un mínimo entendimiento sobre la materia.

Por otro lado, la tecnología debe seguir creciendo, dado que cuanto más crece en número de usuarios más segura y robusta es. Si sigue creciendo al ritmo actual, llegará un punto en el que será prácticamente imposible para los gobiernos, imponer restricciones y mucho menos prohibir su uso. Tratado el tema de los problemas que se pueden solucionar con esta tecnología, pasamos relacionarla con las criptomonedas.

## 2.3 Relación con las criptomonedas

Si hay algo por lo que es conocida la tecnología *blockchain*, es precisamente por las criptomonedas. La popularidad de las monedas digitales ha estado aumentando muchos en los últimos años. Todo empezó en 2009, con la creación del Bitcoin, y sigue hasta la actualidad donde el mundo de las criptomonedas ha aumentado e incorporado sectores como el de los NFTs (*Non Fungible Tokens*), las DeFi (*Decentralize Finance*), los *smart contracts*, las *stable coins*, los juegos en la red, etc. Y es que, cada uno de estos conceptos tiene su propio aprovechamiento de las ventajas de la tecnología en cuestión.

A pesar de que la separación entre el concepto de criptomonedas y *blockchain* ya se ha abordado previamente en el trabajo, hay que diferenciarlos. Siendo la *blockchain*, la tecnología sobre la que funcionan todos estos proyectos. Mientras que, las criptomonedas son los tokens de esos proyectos en cuestión, y su uso varía en función la naturaleza de los mismos. Por ejemplo, en la red de Bitcoin, el token BTC es posiblemente lo más importante, dado que la utilidad de la red reside en la transferencia de valor como sistema de pago. Al contrario que en la red de Ethereum, donde su token, el *Ether*, no es ni de lejos lo más importante de la misma. Dado que el valor principal de este protocolo es el de la creación y ejecución de *smart contracts* sobre la misma red.

Por lo que el token, juega más un papel de moneda de cambio dentro del ecosistema Ethereum. Simplificándolo mucho, las criptomonedas son los tokens de los proyectos desarrollados sobre la tecnología *blockchain*, y su uso e importancia dependerá del tipo de actividad que se desarrolle en la red.

A continuación, elaboraremos un estudio de los proyectos con mayor importancia y potencial de los principales sectores de este nuevo mundo. El objetivo final será el de comparar y entender los proyectos más prometedores, eligiendo de un grupo reducido en base a popularidad con un criterio subjetivo, para finalmente conseguir analizar el impacto del mundo de las criptomonedas en el futuro de la economía.

### 3. Criptomonedas

#### 3.1 Introducción

En este trabajo utilizaremos el concepto de “criptomonedas” para referirnos a los diferentes proyectos que se analizarán. Para proseguir con el análisis, vamos a seleccionar los sectores dentro del mundo *blockchain*, que pueden tener un mayor impacto en el futuro. Los sectores a analizar son los siguientes:

- i. **Reserva y transferencia de valor:** en este grupo se encuentra el Bitcoin, entre otros. Aquí también podemos encontrar las *stable coins*.
- ii. **Smart contracts y Dapps:** el proyecto más famoso dentro de este grupo es Ethereum, aunque también hay muchos otros que apuntan a quitarle el puesto como Cardano, Polkadot, Solana, etc.
- iii. **DeFi (Decentralized finance):** Este sector es el de las finanzas descentralizadas y es el principal competidor del mundo financiero tradicional, además de uno de los sectores con más potencial.
- iv. **Gaming & NFTs:** Los conocimos como *non fungible tokens* son precisamente eso, contenido no fungible en la red. Su aplicación está muy relacionada con el arte y la moda.
  - a. Juegos: este último es un sector que está creciendo muchísimo en los últimos años y básicamente trata del desarrollo de juegos sobre la *blockchain*. Representa una gran oportunidad para el mundo de los NTFs.

De cada uno de estos sectores de actividad se estudiarán las diferentes aplicaciones con el fin de analizar su potencial, así como el de los proyectos dentro de cada sector, según sus ventajas y desventajas.

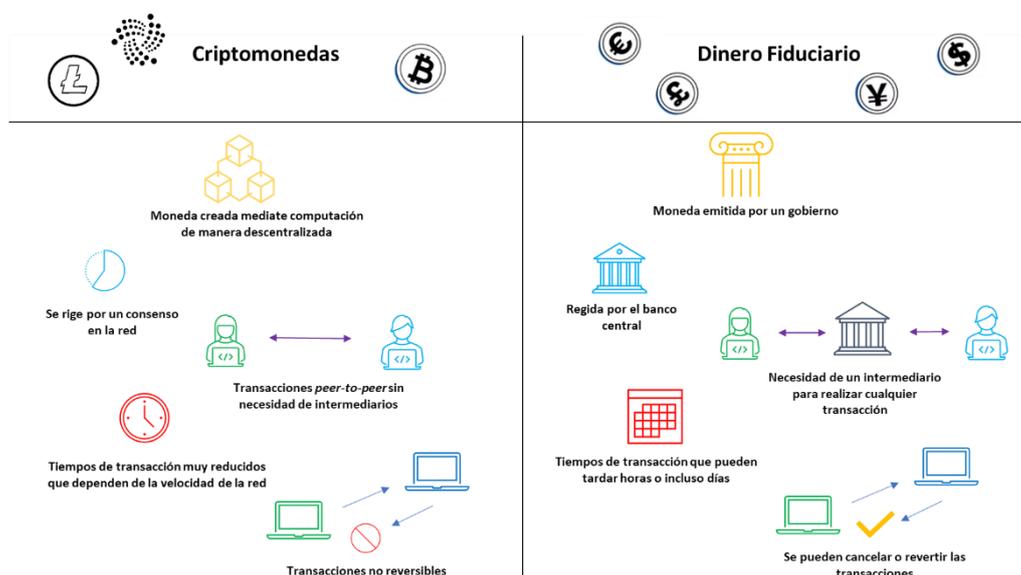
#### 3.2 Sector 1: Reserva y transferencia de valor

Hoy en día, estamos más acostumbrados a realizar todas nuestras operaciones comerciales a través de la tarjeta y cada vez menos con dinero en efectivo. Como demuestra un informe referido al 2020 del Banco de España, el porcentaje de los españoles que prefiere el pago en efectivo ha disminuido al 35,9% frente al 54% que prefiere tarjeta (de los encuestados)

(Biurrun, 2021). En España El dinero digital adquiere más importancia, debido en gran medida, al crecimiento del *e-commerce*.

El dinero convencional, nace con la intención de ser un medio para el intercambio de bienes y servicios. Una unidad de medida central, que permite acordar el valor de las cosas entre los involucrados en el intercambio. El dinero convencional además de servir como medio de intercambios entre bienes y servicios tiene otros usos, entre los que se encuentran, servir como unidad de cuenta, servir como reserva de valor y servir como medio de pago diferido (Grillet, 2019). Ahora bien, ¿dónde reside realmente el valor del dinero? Antiguamente se utilizaba el patrón oro como método de respaldo a la moneda de un país. Es decir, los bancos centrales tenían que garantizar que la moneda del país era totalmente convertible en oro, por lo que, si un ciudadano lo reclamaba, tenía derecho a recibir la cantidad correspondiente de oro por su dinero. De esta manera, se pretendía que el valor de la moneda del país estuviese directamente relacionado con una determinada cantidad de oro, que los bancos debían guardar. Bajo este método, la moneda quedaba soportada por un activo de valor refugio. Sin embargo, el patrón oro fue suspendido en el 1971 por el presidente de los Estados Unidos, Richard Nixon (EFE, 2021). A partir de ese momento, la divisa de un país queda en manos de los bancos centrales y los gobiernos, sin estar respaldado por nada.

Esto ha generado una serie de problemas, entre los que se encuentra la inflación, que es, la pérdida paulatina del valor del dinero, debido a la emisión desmesurada de moneda por parte de los bancos centrales. El dinero fiduciario tiene unas características que generan la necesidad de un sistema alternativo de transferencia de valor. En este marco aparecen las criptomonedas. A continuación, se muestra un breve gráfico con las principales diferencias entre las criptomonedas y el dinero fiduciario:



Bitcoin surge en 2008, como moneda digital orientada a favorecer el comercio electrónico. Con ella, los usuarios pueden realizar transacciones, desde cualquier lugar del planeta de manera directa y segura. Este hecho marca el comienzo de las criptomonedas.

El uso inicial que tuvo el Bitcoin fue de medio de pago digital. Hoy en día, sigue manteniendo ese registro, sin embargo, mucha gente lo considera también un activo refugio de valor. Tanto es así, que se considera al Bitcoin como el oro 2.0.

Para que un activo sea buen refugio de valor, debe tener una serie de características.

Una reserva de valor es un activo capaz de retener valor a lo largo del tiempo. En caso de comprar una buena reserva de valor a día de hoy, tendrás un razonable grado de certeza que su valor no se depreciará con el paso del tiempo. En el futuro, esperarás que el activo valga tanto (o más) que ahora. (¿Es Bitcoin una Reserva de Valor?, 2020)

Según esta definición, un buen refugio de valor debe ser duradero. Es necesario que se mantenga en el tiempo. También, debe ser escaso, lo que ayuda a que no se devalúe. De acuerdo con esta información el Bitcoin cumple con las condiciones para ser considerado una buena reserva de valor. Por una parte, el Bitcoin tiene la creación de monedas limitada a 21 millones por el protocolo marcado en la red. Esto lo convierte en un activo deflacionario y escaso. Por otro lado, la criptografía y el funcionamiento de la *blockchain* permiten al Bitcoin ser un activo duradero en el tiempo. A todo esto, hay que añadirle la gran cualidad de la descentralización además de la facilidad de transferencia, a diferencia del oro.

No obstante, muchas personas se preguntan: ¿cómo puede un activo tan volátil ser un refugio de valor? Bien, lo cierto es que Bitcoin es un activo con mucha volatilidad. A lo largo de su historia ha sufrido caídas de hasta el 30%-40% en cuestión de horas, y no es de extrañar que su precio varíe un 5% en un día relativamente normal. Esto en parte se debe a que, a pesar de ser la moneda con más capitalización de mercado, unos 847 millones de dólares (27-03-2022), sigue teniendo una capitalización muy baja si la comparamos con la del oro, la cual ronda los 10 mil millones de dólares. La realidad es que, a pesar de ser un activo muy volátil, la tendencia a medio-largo plazo del Bitcoin siempre ha sido alcista. Es más, no hay ningún otro activo que haya promediado una tendencia alcista constante tan grande como la del Bitcoin. Si recordamos la definición de un buen activo refugio, “...tendrás un razonable grado de certeza que su valor no se depreciará con el paso del tiempo. En el futuro, esperarás que el activo valga tanto (o más) que ahora” (¿Es Bitcoin una Reserva de Valor?, 2020), a pesar de que su precio varíe mucho, el BTC es un activo que, en mi opinión, sí que puede hacer de valor refugio. En este sentido, no

hay muchos competidores dentro del mundo de las criptomonedas que le haga frente al Bitcoin. El más cercano quizás, es el de *Litecoin*, el cual es conocido como la plata de internet.

La reserva de valor es un aspecto que prácticamente solo Bitcoin tiene, o por lo menos que se le atribuya, sin embargo, no es el único uso que se le puede dar. La transferencia de valor es el otro uso importante que tiene, y es por el que la moneda fue creada. En este grupo sí que existen varias monedas capaces de competir, dado que prácticamente todas las monedas valen para transferir valor, teniendo en cuenta que todas cotizan en varios mercados y tienen varios cambios. No obstante, aquí nos vamos a centrar en las monedas que tengan un uso exclusivo de transferencia de valor como medio de pago. En este sector aparecen dos tipos de monedas.

Por una parte, tenemos las *stablecoins*, las cuales ejercen el papel de “puente” entre el dinero convencional y las criptomonedas. Esto se debe a que, las *stablecoins*, son monedas que están respaldadas por una divisa tradicional como el dólar. Se podría decir que son la representación de las divisas en forma de criptomoneda. “Una *stablecoin*, es una criptomoneda creada con la finalidad de que su valor permanezca estable. Para mantener esta poca variabilidad en su precio de mercado, necesitan un backup de respaldo” (*¿Qué es una Stablecoin?*, s.f). Dentro del grupo de las *stablecoins*, hay diferentes métodos que utilizan para mantener el precio de la moneda estable. Entre esos métodos se encuentran las monedas colateralizadas y las controladas por algoritmos.

Las colateralizadas son aquellas que están respaldadas por un activo, ya sea una divisa, criptomoneda o un bien. Dentro del grupo de estas monedas, a su vez hay que distinguir entre las respaldadas por monedas *fiat*, las respaldadas por otras criptomonedas o las respaldadas con un bien. Las tres utilizan el método de “ligar” la moneda al precio de otro activo más estable.

Luego tenemos el grupo de las no colateralizadas. Estas son controladas por los algoritmos, por lo que no están asociadas a ningún valor externo. Esto es posible gracias a los algoritmos y *smart contracts* dentro de la propia cadena, que simulan las funciones de un banco central, controlando la oferta y la demanda de la moneda para estabilizar el precio.

A expensas del tipo de *stablecoin*, estas monedas tienen como principal objetivo paliar la gran volatilidad del mercado de las criptomonedas. Funcionan como refugio estable para cuando el mercado se encuentra en momentos muy volátiles. Por otra parte, buscan facilitar el acceso a financiación dentro del ecosistema cripto. Estas monedas tienen una serie de ventajas y desventajas, las cuales nos ayudaran a tener una mejor idea de su uso, potencial y futuro.

Entre las ventajas nos encontramos con que las *stablecoins* tienen respaldo económico a través de activos reales, aportan estabilidad al mercado y ofrecen gran liquidez debido a la “tokenización”. Por el contrario, tienen también una serie de desventajas entre las que se encuentra la centralización de los esquemas de estas monedas, lo cual ataca directamente al espíritu de las criptomonedas. (¿*Qué es una Stablecoin?*, s.f).

Ahora que ha quedado visto el asunto de las *stablecoins*, pasamos a estudiar el otro tipo de monedas, las dedicadas exclusivamente a la transferencia de valor como principal utilidad. Las criptomonedas han abierto un nuevo escenario en lo que a transferir valor se refiere. Hoy en día, una persona puede transferir cantidades enormes de dinero de una punta del mundo a otra en cuestión de segundos, y todo estos con comisiones casi inexistentes. Uno de los ejemplos más claros en este ámbito es la moneda Dogecoin. Esta empezó como una broma entre sus creadores (solo basta ver que su símbolo es un perro), y ha acabado siendo una de las monedas con más capitalización de mercado. Este éxito se debe, entre muchas otras cosas, a las bajas comisiones de transferencia de la red. Ciertamente es, que esta moneda ha sido varias veces mencionada y aclamada por Elon Musk, lo que ha provocado grandes variaciones en su precio. Sin embargo, esta moneda nos sirve como buen ejemplo de lo que este nuevo mundo aguarda. La moneda que empezó como una broma tiene, además de una utilidad, un valor en el mercado el cual la convierte entre las más valoradas.

Las monedas en este segmento son muy numerosas, y más si se tiene en cuenta que casi cualquier moneda puede ser utilizada para ese registro. Es por ello, que en este apartado merece la pena estudiar el tema del Bitcoin como reserva de valor, así como las *stablecoins* y su importante papel dentro de este nuevo ecosistema. Tanto el Bitcoin como las *stablecoins*, y porque no las monedas como Dogecoin, aportan un importante pilar dentro del mundo de las criptomonedas, sobre todo en el relacionando con las finanzas; el mundo DeFi.

### **3.3 Sector 2: Smart contracts y Dapps.**

Los *Smart contracts*, son también conocidos como contratos inteligentes o autoejecutables. Son contratos en formato electrónico y autoejecutables que funcionan sobre la *blockchain*.

Estos contratos inteligentes son, en realidad, acuerdos en la red que dependen de una serie de cláusulas, las cuales funcionan mediante *scripts* o pequeños programas, que una vez ocurrido los eventos desencadenantes ejecutan automáticamente la condición del contrato, sin que haya

lugar a modificación, cancelación o no ejecución de la prestación. Adicionalmente, un *Smart contract* es un programa de ordenador que se auto verifica, autoejecuta y que es resistente a ataques maliciosos. Este concepto fue creado en 1994 por Nick Szabo. La idea de estos contratos es, que se puedan ejecutar sin la necesidad de una entidad o persona ajena (Echebarría M., 2017). Con ánimo de evitar complicaciones, no nos adentraremos en la explicación técnica sobre el funcionamiento de estos contratos más allá de lo ya explicado. Si que realizaremos un análisis cualitativo de los *Smart contracts* y sus posibles aplicaciones.

Hay una serie de características que forman la idea de los contratos autoejecutables, que explican lo que son, sus cualidades y el porqué de su utilidad. Procedemos a destacar las características más importantes de los mismos:

- I) **De carácter digital:** dado que se ejecutan en la *blockchain* y su campo de acción se limita a lo tecnológico, se puede afirmar que estos son de naturaleza digital.
- II) **Autoejecutables:** posiblemente la condición más importante que tienen los contratos inteligentes. Aptitud por la que se los denomina “Smart”, dado que se pueden ejecutar siguiendo unas pautas y sin la necesidad de un intermediario ni regulador.
- III) **Seguridad:** propiedad que viene dada por la propia naturaleza de la tecnología de bloques. Los *Smart contracts*, al funcionar sobre la misma adquieren dicha cualidad, la cual es de suma importancia cuando se habla de un contrato.
- IV) **Naturaleza condicional:** característica que explica su funcionamiento a partir del lenguaje de programación que utilizan. El código informático está normalmente constituido por unas instrucciones de tipo “si ocurre el suceso X, ejecuta Y; sino ocurre X, entonces no Y”.
- V) **Inmutabilidad:** particularidad muy mencionada en este trabajo, pero que no deja de ser de suma importancia. Esta es la condición por la que la información presente en la cadena de bloques no se puede modificar. Competencia que se extiende a los contratos, siendo una de las más importantes. (Fetsyak, 2020).

Habiéndose visto las características principales, así como una explicación general de lo que son los contratos inteligentes, pasamos a hablar de sus posibles aplicaciones, y posteriormente ver cuáles son los proyectos con más potencial dentro de este ámbito. Entre los posibles usos para los que se pueden utilizar los contratos inteligentes se encuentran los ámbitos donde hay procesos secuenciales de transacciones, como por ejemplo en una cadena de suministro. También se puede aplicar a entornos con grandes cantidades de datos, en los que los *Smart*

*contracts* parametrizan esos datos y ejecuten unas acciones en función de ellos. Un ejemplo de esto sería la intranet de una empresa. No obstante, el ámbito donde su uso va a ser más explotado es en lo relacionado con lo financiero y las transacciones de diferentes tipos. Las aplicaciones en este caso son múltiples, tales como préstamos, pagos condicionados, inversiones, depósitos, herencias, controles financieros, etc.

Tras ver los *Smart contracts*, pasamos a ver un apartado más complejo y útil de este tipo de *blockchain*; las *Dapps*. Pero antes de hablar de las *Dapps*, debemos mencionar *solidity*. “*Solidity* es un “lenguaje” de alto nivel de tipado estático con el que se pueden programar smart contracts para la red de Ethereum” (*¿Qué es Solidity en los smart contracts de Ethereum Blockchain?*, s.f). Fue creado con el objetivo de facilitar la creación de *Smart contracts* en la red de Ethereum. Gracias a este lenguaje de programación, los desarrolladores pueden crear aplicaciones descentralizadas de código abierto sobre la red. Ahora sí, pensemos en una *Dapp* como una *app* tradicional pero que funciona sobre la *blockchain*. Para entender como es debido el concepto de *Dapp*, vamos a compararlo con una *app* tradicional. Ambos tipos de *apps* tienen dos partes llamadas *frontend* y *backend*. El *frontend* explicado de manera muy sencilla, es la interfaz que veía el usuario al utilizar la aplicación. En este sentido tanto las *apps* como las *Dapps* son muy parecidas. Las diferencias aparecen en el *backend*. En el caso de una aplicación tradicional, todo el funcionamiento de la *app* está centralizado, necesitando de una entidad para funcionar. En el caso de las *Dapps*, estas funcionan de manera descentralizada gracias a los *Smart contracts*, que se autoejecutan en la red. Dado que estos contratos inteligentes son públicos, cualquiera tiene acceso a la información sobre su funcionamiento, aportando transparencia al proceso. En las *Dapps*, cada usuario funciona a modo de nodo en la red. Esto quiere decir que hace el papel de registrar, validar y almacenar las transacciones de esta. Esto es posible, como hemos mencionado anteriormente, gracias a un contrato inteligente, el cual valida automáticamente la transacción si una condición se cumple. De esta manera los usuarios juegan un papel de nodo, pero de manera “pasiva” dado que se podría decir que la parte activa de control y funcionamiento la realizan los *Smart contracts* (*¿Qué son las DApps?*, s.f).

La primera red que implementó esto fue Ethereum, cuando su creador, Vitalik Buterin quiso transformar la red de Bitcoin en algo más complejo que solo transmisión de información. Sin embargo, no fue escuchado por sus desarrolladores, motivo por el que decidió crear su propio proyecto llamado Ethereum. Desde entonces, Ethereum ha revolucionado el concepto de la *blockchain*, dándoles un abanico de usos mucho más amplio, permitiendo la creación de programas informáticos sobre una plataforma descentralizada. Este hecho no tardó en atraer

competidores contra la red de Ethereum, la cual a pesar de ser la más grande de este tipo de cadenas, tiene cada vez más rivales que proponen soluciones a los problemas de esta. Estos émulos son conocidos los “Ethereum *killers*” dado que nacen con la idea de operar como Ethereum, pero resolviendo todos los problemas que esta red tiene.

Para continuar con el análisis, pasamos a estudiar los diferentes proyectos dentro de este sector, con sus respectivas ventajas y desventajas con el fin de llegar a una conclusión. Como no podía ser de otra manera, esta observación debe comenzar con la red Ethereum.

### **Ethereum**

La red Ethereum nace con el objetivo de ser una plataforma de desarrollo de aplicaciones descentralizadas a través de los *Smart contracts*, que permita a los desarrolladores un fácil desempeño con la misma. Como ya sabemos, Ethereum fue la pionera en este aspecto, y es por ello que, a día de hoy, su moneda Ether, se sitúa como segunda en la lista de criptomonedas con más capitalización detrás del Bitcoin. Este token de la red sirve como moneda de intercambio dentro del ecosistema Ethereum además de como combustible de la plataforma. Con combustible nos referimos a que es el incentivo que se otorga a los desarrolladores, por el mantenimiento de la red. El Ether es cobrado en forma de comisión, bajo el nombre de gas, con cada transacción. Es precisamente el gas lo que ha supuesto mayores problemas a la red Ethereum, que debido a su escasa velocidad de transacción por segundo y su creciente popularidad, ha generado precios en forma de gas totalmente desorbitados. Otro de los grandes problemas de esta plataforma era el mismo del Bitcoin, su mecanismo de consenso, dado que utiliza el PoW, que si recordamos requiere de una gran fuerza computacional que a su vez genera un gasto de energía tremendo. Bien, pues Ethereum planea corregir esos errores mediante la migración a su plataforma Ethereum 2.0. Esta nueva actualización, permitirá resolver la limitación de 30 transacciones por segundo a más de 100000, un cambio gigantesco que pretende frenar el avance de sus competidores. Por otro lado, también se cambia el método de consenso, pasando a ser PoS, por el cual los mineros desaparecen. Por tanto, a partir de ese momento, será necesario hacer *staking* de ethers para poder participar como nodo en la red. Una vez solucionados los problemas, la red Ethereum cuenta con ventajas que la hacen ser de los proyectos más prometedores, tales como su enorme escalabilidad, su creciente red de usuarios, o el impresionante número de proyectos que se desarrollan sobre su plataforma.

Hay varios proyectos que amenazan con quitarle la hegemonía a Ethereum. Entre todos estos proyectos he seleccionado los que, a mi juicio, tienen más posibilidades de competirle. Los principales competidores de Ethereum son Solana, Cardano y Binance Smart Chain (BSC).

Sirva como dato, para aquellos que cuestionan en valor de mercado del Ether, la siguiente simulación de una comparativa tipo PER (*Price Earnings Ratio*) utilizada para contrastar el valor de mercado de una acción convencional, relacionada con el revenue generado por ese negocio. Así, si recogemos el número de transacciones que se realizan actualmente en la red Ethereum, las valoramos al precio medio actual pagado por ese tipo de transacciones, y lo relacionamos con la capitalización del Ether, obtendríamos un PER de 24, más que razonable para una acción correspondiente a un negocio en crecimiento, y en el que todos los ingresos (no solo los que discrecionalmente la dirección del negocio en cuestión decidan distribuir) son repartidos entre los propietarios de Ether (o en otras palabras, a los accionistas).

	Monthly transactions Millions	Transaction Cost \$	Annual Yield per transactions M\$	Market CAP	Market Cap/ Annual Yield
Ethereum	38,9	4	1.867	45608	24

### Cardano

Este proyecto fue fundado en 2015 por la organización Input-Output Hong Kong (IOHK), que cuenta con la participación del cofundador de la plataforma Ethereum Charles Hoskinson. El principal objetivo de Cardano es el de operar los contratos inteligentes de manera más eficiente, sostenible e inclusiva que sus competidores (Montaner, 2021). El token de la plataforma *blockchain* de Cardano es el ADA. El token de ADA tiene un *supply* fijo como el BTC, limitado en 45 mil millones. Cardano está formado por tres entidades:

- i) Cardano foundation: entidad suiza sin ánimo de lucro que se encarga del ecosistema y la comunidad. Colabora con organizaciones y entidades reguladoras en diferentes iniciativas.
- ii) IOHK: empresa de ingeniería informática especializada en la implementación de tecnologías *peer-to-peer*. Se encargan del mantenimiento de la red de cardano.

- iii) Emurgo: empresa encargada de integrar y ayudar a las empresas que tengan interés en utilizar la *blockchain* de Cardano. (McCracken, 2022).

La mayor diferencia de Cardano respecto a las demás cadenas es que, a diferencia de la mayoría, Cardano se centra en la investigación y desarrollo responsable antes de sacar e implementar una nueva tecnología. Esto es algo por lo que se ha criticado mucho a Cardano, al avanzar más lento respecto a sus competidores, sin embargo, no parece ser un mal enfoque, dado que muchas otras redes han tenido problemas debido a la precipitación. En cuanto a su lenguaje de programación, Cardano utiliza Haskell. Este lenguaje no es el más utilizado, no obstante, es de los más seguros.

Otra cosa que diferencia a Cardano es la manera en la que maneja sus reservas y la financiación de sus proyectos. Cardano tiene en su hoja de ruta disponer de unos fondos reservados en una cuenta descentralizada, que sea manejada por todos los usuarios de la red. El objeto de esta cuenta sería el de financiar los proyectos de la plataforma. Los fondos de dicha cuenta proceden de las comisiones de las transacciones de la red.

Por otro lado, a pesar de que puede parecer que Cardano no es muy descentralizada, debido a su estructura de fundación y colaboración con entidades, cabe mencionar que es de las más descentralizadas. Actualmente, Cardano tiene unas 3100 *staking pools* lo que la convierte en una de las cadenas de bloques menos centralizada (McCracken, 2022).

### **Solana**

Solana es otra de las grandes plataformas que compiten con Ethereum. Fue creada por Anatoly Yakovenko en 2018, fecha en la que se publicó su *white paper*. Es de las que más potencial tiene debido a una serie de características que explicaremos en breves instantes. El token de la red es el SOL, el cual no tiene límite de suministro. Para hacernos una idea, exponemos los números de Solana a la hora de operar:

- (i) Velocidad: 400 milisegundos por bloque
- (ii) Coste: 0,000005 SOL (<0,01\$) por transacción
- (iii) Descentralización: 2242 global nodes (Greyscale, 2021).

A pesar de sus grandes números en cuanto a velocidad y coste, Solana no es de las *blockchains* más descentralizadas. Esto ha provocado muchas críticas además de fallos en el sistema alguna vez. En cuanto a sus ventajas frente a las demás redes tenemos:

- a) Un equipo con experiencia previa en empresas como Qualcomm, Google, Dropbox o Apple.
- b) Una tecnología fácilmente accesible para todos, con gran escalabilidad y comisiones muy bajas.
- c) La comunidad de usuarios de Solana se caracteriza por ser una de las más extensas y activas.
- d) Un ecosistema dinámico que crece a gran velocidad y que permite la creación de diferentes tipos de *Smart contracts* y *Dapps*. (Greyscale, 2021).

No todo iban a ser ventajas, y es que, a Solana se le critica por una serie de inconvenientes que la penalizan frente a sus competidores. Entre estos se encuentran: el nivel de centralización, la incertidumbre regulatoria y la seguridad de la red.

Estos son los proyectos que, a mi parecer, merecen más la pena por una serie de razones. Cabe mencionar que hay muchas más plataformas de *Smart contracts* que no se han mencionado como: EOS, Polkadot, Avalanche, Polygon Stellar, etc. El objetivo de este apartado era el de analizar los proyectos que nos parecieran interesantes, para así poder sacar una conclusión sobre el mundo de los *Smart contracts*, las *Dapps* y la *blockchain*.

De este apartado extraemos que las plataformas de los contratos inteligentes y las *Dapps* tienen un potencial increíble. Son capaces, en muchos casos, de sustituir las comunicaciones como hoy las conocemos y llevarlos hacia un funcionamiento descentralizado a manos de los usuarios. La viabilidad de esta migración dependerá del tipo de servicio/operación/proceso y los usuarios que estén implicados, siendo posible en muchos casos, pero no en todos. Y es que, esto se aplica a varias estancias tales como las finanzas, los juegos, los pagos, el repositorio de información en la nube, el arte y todo tipo de aplicaciones. En este contexto las *blockchains* como Ethereum, Solana o Cardano juegan un papel clave en desarrollar una plataforma que sea eficiente, potente, escalable, descentralizada, barata en comisiones y sostenible. Es un sector que está creciendo mucho en los últimos años debido al gran potencial que tiene.

### 3.4 Sector 3: DeFi (Decentralized Finance)

En el mundo financiero actual es cada vez más difícil acceder a financiación debido a la situación geopolítica actual. Dependemos, como usuarios, de terceros, cuartos, o incluso quintos intermediarios, para absolutamente todo. Pongamos como ejemplo cualquier situación ordinaria de un ciudadano de a pie: vas a realizar una compra de cualquier índole con tu tarjeta de crédito, y a pesar de que tú eres consciente de que dispones de liquidez en tu cuenta bancaria, dependes de los servidores del banco para que tramiten y autoricen el pago. Otra situación posible: tienes una cuenta de ahorro con dinero, con el objetivo de utilizarlo una vez te hayas jubilado. Bien, pues a día de hoy, con la inflación actual, tu dinero valdría alrededor de un 8% menos cada año, es decir, dependes de los gobiernos y entidades financieras para que tu dinero no se devalúe cada vez más. Proseguimos con otra situación para terminar de asentar el concepto: necesitas dinero para empezar a desarrollar un proyecto. En este caso dependes de que, en el caso más probable, una entidad bancaria, te conceda el crédito necesario. El problema real es que, actualmente, hay demasiados intermediarios en los sistemas financieros en general. La raíz de este problema nace con la interconectividad del mundo en el que vivimos. Una entidad bancaria, para poder conceder un crédito, necesita cumplir con unos estándares de riesgos, y partir de ahí, cobrar una serie de intereses. Todo esto se debe en parte, a que se trata de una empresa con accionistas, que esperan buen rendimiento por parte del banco. A su vez, se encuentran los usuarios que depositan su dinero en ese banco, los cuales confían en que sus depósitos estén seguros, por lo que el banco debe hacer unos controles de seguridad antes de prestar el capital. Si quieres comprar acciones en bolsa, necesitas un bróker que te las compre. Y así todo, y es que la presencia de tantos implicados no genera más que complicaciones y costes. Los costes de transacciones son el mejor ejemplo de esto. En una cadena de suministro, por ejemplo, los costes de transacción suponen un gasto muy importante para las empresas.

Bajo este contexto introducimos las finanzas descentralizadas, que no son más que operaciones financieras bajo el marco de la tecnología *blockchain*. Gracias a la tecnología de cadena de bloques, muchas operaciones financieras pueden realizarse sin la necesidad de tanta intervención, sino de una manera mucho más directa; en forma *peer-to-peer*. Se puede ser muy creativo a la hora de pensar en posibles usos de la cadena de bloques en el mundo financiero. Sin embargo, nos vamos a centrar en los principales usos o aplicaciones dentro de las finanzas. Dentro de todos los usos que se le pueden dar, se van a analizar los siguientes:

- (i) Medios de pago

- (ii) Inversión
- (iii) Financiación

La tecnología *blockchain* aporta al mundo financiero algunas importantes ventajas como la descentralización, la interoperabilidad, la innovación, y la transparencia. A continuación, explicamos en profundidad cada uno de ellos:

- b. Descentralización: ventaja *core* de esta tecnología, la cual ha sido tratada en varios apartados de este trabajo. La descentralización permite a los usuarios participar más fácilmente en el mundo financiero, operar sin la necesidad de intermediarios, acceder de manera más sencilla a financiación, reducir los costes, etc.
- c. Interoperabilidad: facilidad de comunicación y participación entre las diferentes *blockchains* y servicios.
- d. Innovación: al ser la mayoría de *blockchains* de código abierto (cualquiera puede participar y programar en ellas) favorecen a una innovación más diversa, accesible, fácil y barata. Esto incrementa las posibilidades de que avance el progreso tecnológico dentro de las cadenas.
- e. Sin fronteras: esta característica afecta sobre todo a los pagos y transacciones. Para que ocurra una transacción entre países, ambos tienen que operar bajo la misma moneda. Es decir, uno de ellos va a tener que vender su moneda para comprar la del país con el que quiere hacer negocio. Todo esto además de consumir tiempo y recursos, genera complicaciones que acaban incurriendo en costes y afectando a los mercados. Por otro lado, el tiempo que lleva realizar un pago, transferencia o compra a otro país suelen llevar días, debido a la cantidad de intermediarios que participan.
- f. Transparencia: otra condición clave cuando hablamos de la tecnología *blockchain* es la transparencia. Todo lo que ocurre sobre la cadena de bloques es visible para cualquier usuario. Esto permite la trazabilidad de las operaciones, aunque siempre manteniendo la privacidad de los titulares.

En el mundo de las finanzas descentralizadas hay muchos tipos de proyectos dedicados a diferentes actividades, sin embargo, todas ellas están relacionadas entre sí. Por ejemplo, uno de los usos más obvios dentro de este sector es el de los medios de pagos. En este sentido, hablamos del uso de las criptomonedas como intercambio de valor. No obstante, y como ya hemos visto anteriormente, prácticamente todas las criptomonedas pueden ser utilizadas como intercambio de valor, dado que cotizan en un mercado, tienen un valor y se pueden

intercambiar. No nos vamos a explayar más en esto dado que ya ha sido tratado anteriormente en el trabajo, aunque no está mal mencionarlo dado que es una parte importante del ecosistema de las finanzas descentralizadas. Por otro lado, y para que estos intercambios ocurran, son necesarios los *exchanges* descentralizados. Estos hacen el papel de las bolsas de valores tradicionales, solo que, de manera automática, descentralizada y de forma directa entre usuarios. La clave para que estos portales de intercambios funcionen reside en las conocidas como *liquidity pools* o bolsas de liquidez. Estas bolsas de liquidez son espacios que permiten a los usuarios depositar sus tokens a cambio de un interés normalmente fijo, con el objetivo de aportar liquidez a la red y conseguir así un funcionamiento normal de los intercambios. A pesar de que la actividad más obvia de estas bolsas descentralizadas es la del intercambio de valor, existen otras actividades de finanzas descentralizadas en el mundo de las *blockchain*. Nos referimos a las actividades típicas de las finanzas tradicionales, como son la inversión y la financiación, solo que aplicados al mundo de las criptomonedas. Es aquí donde reside el verdadero valor de las DeFi, dado que como hemos empezado diciendo en este apartado, hoy en día no es nada fácil para el ciudadano corriente acceder a financiación, ya sea para un proyecto, vivienda, gasto personal, etc. La manera que esto se consigue es un concepto parecido al del *crowdfunding* o “micromecenazgo”. “El crowdfunding o micromecenazgo, en castellano, es una red de financiación colectiva, normalmente online, que a través de donaciones económicas o de otro tipo, consiguen financiar un determinado proyecto a cambio de recompensas, participaciones de forma altruista” (VIVUS, 2020). Pues bien, la manera en la que estos dos conceptos se parecen es la siguiente: la financiación a través de los proyectos en la *blockchain* se obtiene mediante una financiación conjunta de muchos usuarios diferentes, con unos términos de contratos estipulados sobre el *Smart contract* de la red. Estos términos recogen conceptos clásicos de un préstamo como: titular, interés, fecha de pago, pagos estipulados, garantía, moneda, etc, solo que lo recogen en un contrato digital, que se ejecuta de manera automática sin necesidad de intermediarios. Esto facilita el acceso a la financiación, a la vez que el acceso a la inversión para pequeños inversores, permitiendo prestar solo la cantidad deseada, con unas condiciones ya establecidas y automatizadas. Uno de los usos con más potencial dentro de las DeFi es el de la financiación de proyectos a través de las ICOs (*Initial Coin Offering*), concepto muy parecido al de las IPOs. Un usuario o grupo de usuarios que quiera emprender un proyecto solo tiene que publicar el proyecto con un *White paper* en el que se explique la información importante sobre el mismo. De esta manera los inversores tienen la oportunidad de analizar la viabilidad del proyecto, y a partir de ahí decidir si invertir o no en él. Además, los inversores pueden invertir la cantidad que consideren en función del

potencial que le vean. Hablamos de gran potencial en este sentido dado que las DeFi pueden suponer un punto de inflexión en la financiación tradicional, en la que se dependa menos o incluso nada en las entidades financieras y más en los inversores personales.

En este apartado hay cientos de plataformas que operan en este mercado. Por lo que lo enfocaremos de una manera un poco diferente a lo que hemos venido haciendo a lo largo del trabajo. Expondremos un ejemplo de los diferentes tipos de plataformas del mundo de las finanzas descentralizadas, que reflejen de manera adecuada el potencial de estas.

### **AAVE Protocol**

El primer proyecto del que vamos a hablar va a ser el de AAVE Protocol, dado que fue el primero en introducir la idea de los préstamos e inversiones descentralizadas de manera eficiente y segura. AAVE inicialmente era conocida como ETHlend. Fue creada en el 2017 con el objetivo de llevar el mercado de préstamos al mundo descentralizado de las criptomonedas. Al principio, el protocolo ofrecía préstamos de manera descentralizada, con colaterales que el prestatario tenía que depositar. El gran valor de ETHlend en ese momento era la gran flexibilidad a la hora de exigir colaterales. Sin embargo, la evolución de la tecnología provocó que el mundo de las criptomonedas cambiara, lo que a su vez hizo que los desarrolladores de ETHlend decidiesen hacer progresar el protocolo ofreciendo una serie de avances tecnológicos. A partir de ese punto la plataforma paso a llamarse AAVE (¿Qué es AAVE? s.f). Uno de los cambios más significativos fue el de que, a partir de ese momento, los precios de los préstamos pasaron a estar en función de la oferta y la demanda del activo en cuestión. Esto es posible gracias a un algoritmo que calcula la liquidez del mercado y estipula los intereses a pagar. En esta plataforma un inversor puede depositar su dinero en una bolsa de liquidez y a cambio recibir unos intereses por proveer a la red de liquidez. Por otro lado, un usuario puede solicitar un préstamo con unas condiciones, a través de las cuales la plataforma busca a otro usuario que esté dispuesto a aceptarlas. Entre estas condiciones cabe destacar como importantes: el montante, los intereses y sobre todo el colateral. Este último siendo una gran baza por la que la plataforma destaca sobre las demás (¿Qué es AAVE? s.f).

Dentro del mundo de las finanzas descentralizadas AAVE es uno de los proyectos más importantes, con una capitalización de mercado a mayo de 2022 de 1,5 billones de dólares.

## Uniswap

Uniswap es un proyecto el cual tiene dividida a la comunidad respecto a si es una plataforma DEX (*Decentralized Crypto Exchanges*) o si sus servicios son suficientes para considerarla una plataforma DeFi. Lo cierto, es que la plataforma es mas conocida por ser un medio de intercambio descentralizado sobre la red Ethereum. De hecho, es la plataforma de intercambio



descentralizado más popular en el mundo DeFi. No obstante, el portal ofrece otro tipo de servicios a los usuarios a parte de los intercambios de Crypto activos.

La manera en la que funciona Uniswap es la siguiente: para poder ofrecer un cambio de cualquier token se debe abrir una bolsa de liquidez con un cambio par con otro token. Estos tokens deben ser del tipo ERC-20, lo que significa que funcionan sobre la red de Ethereum. Una vez abierta la bolsa de liquidez, los inversores depositan sus tokens a cada lado según deseen, y a cambio reciben una parte de esta *liquidity pool*. Esta *liquidity pool* genera unos beneficios a través de intereses por cada transacción que ocurre. Posteriormente estos ingresos generados son repartidos entre los “propietarios” de la bolsa en función del porcentaje de participación de cada uno, que se mide en base al *staking* que haya hecho cada usuario (*How Uniswap works*, s.f).

Una vez expuestos ejemplos de dos plataformas que reflejan los diferentes programas que hay en el mundo de las finanzas descentralizadas, pasamos a analizar y concluir lo recogido de este nuevo mundo financiero.

Como hemos empezado diciendo en este apartado, las finanzas tradicionales han dependido siempre de demasiados intermediarios. Esto, aparte de generar lentitud e ineficiencias, provoca unos costes elevados, dado que cada interventor de una operación debe llevarse su parte. Además, para poder pedir un préstamo hoy en día, un ciudadano tiene que aportar demasiada información para evaluar la viabilidad de la operación, ya sea una financiación para un proyecto o un préstamo para temas personales. Esto se debe a que las empresas que emiten los prestamos

tienen unos inversores a los que contentar a través de resultados. Por otra parte, tradicionalmente un ciudadano corriente, no ha tenido acceso al mercado de deuda por su cuenta, dado que ese papel estaba reservado a corporaciones y gobiernos. En este sentido, internet juega el papel que ha ido ejerciendo desde que se creó, unir intereses de los usuarios. Las tiendas online de segunda mano, los e-commerce como Amazon, las redes sociales con sus algoritmos personalizados, etc. Esto ha ocurrido en prácticamente todos los sectores. Sin embargo, en este caso nos centraremos en las necesidades de compra con necesidades de venta. Pues bien, internet también ha contribuido a mejorar y flexibilizar el sector financiero, por ejemplo, con la aparición de empresas de microcréditos o plataformas de *crowdfunding*. Sin embargo, aquí vuelve a aparecer el mismo problema de siempre; los intermediarios. Y es que, si algo tiene de beneficioso la tecnología blockchain es la conexión directa entre usuarios de manera descentralizada. Esta combinación entre el internet y la descentralización de la *blockchain* es lo que hace que el mundo de las finanzas descentralizadas sea tan potente, hasta el punto de poder suponer una revolución en este sector en los próximos años.

### **3.5 Sector 4: gaming & NFTs**

La palabra NFT ha ido incrementando su popularidad de manera exponencial en los últimos años. El acrónimo NFT contiene las iniciales de *non-fungible token*, lo que en español significa: token no fungible. Como tal, la palabra fungible hace referencia a la propiedad por la que un activo se consume con el uso y puede ser reemplazado (Real Academia Española, s.f., definición 1). Básicamente, los bienes fungibles son aquellos que pueden cambiarse entre sí y que su valor reside en unidades como número, peso o medida. Por otro lado, los activos no fungibles son aquellos que no pueden sustituirse debido a su condición de unicidad. Un ejemplo de activo fungible sería el dinero, y un ejemplo de activo no fungible sería una pieza de arte como el cuadro de la Mona Lisa. A raíz de esta definición podemos asumir que un NFT es un activo en línea, el cual no se consume con el uso y no puede ser reemplazado de manera exacta. Su funcionamiento es el siguiente: Como bien sabemos, la tecnología blockchain, es una red descentralizada de ordenadores, que crean una cadena de bloques o nodos que contienen información. Cada bloque encaja con el siguiente, registrando la información del anterior, todo ello asegurado y protegido por la criptografía. La diferencia de los NFTs con las criptomonedas es que, los NFTs tiene una serie de datos únicos que están ligados al criptoactivo. Este grupo de datos está formado por un certificado que lo identifican como un activo único e irrepetible,

el cual está formado por las transacciones del activo, el autor, el origen, etc. Una vez aclarado el significado del acrónimo NFT, su funcionamiento y lo que es, pasamos a analizar el potencial impacto de este nuevo sector que nace en el mundo de las criptomonedas.

Los NFTs nacen a raíz de los contratos inteligentes en la red Ethereum. Dadas las cualidades de este tipo de criptoactivos, los NFTs son utilizados como una manera de demostrar propiedad sobre un activo único en la blockchain. De esta manera, el propietario de un NFT, independientemente del tipo de activo del que se trate, puede demostrar su condición de propietario e incluso ingresar unos beneficios procedentes de su explotación. Esto refleja una posible representación de la propiedad intelectual en la red.

Como venimos haciendo a lo largo del trabajo, nuestro objetivo en este apartado va a ser el de analizar el posible impacto de este tipo de activos en la economía del futuro. Para poder llevar a cabo este análisis, nos vamos a centrar más en los posibles usos que pueden tener los NFTs, así como los sectores a los que pueden afectar en el futuro. Es por ello que en este apartado no nos enfocaremos tanto en los proyectos con más potencial, si no en los NFTs en su conjunto.

En los últimos años, los NFTs han ido incrementando su popularidad de manera estrepitosa, generando una especulación a su alrededor que ha hecho que salgan muchos detractores de estos nuevos activos. La realidad es que, actualmente los NFTs son una máquina de especulación y dinero fácil, dado que la mayoría de la gente que opera con ellos no sabe ni su funcionamiento, ni lo que son. Se esconden bajo la idea de que los NFTs son arte digital, y que, como toda pieza de arte, el valor que se pague por ellas es subjetivo. Si bien es cierto que una gran parte del mercado de los NFTs es el arte digital, los usos que se le pueden dar a esta tecnología van mucho más allá del arte.

Cierto es que el mundo del arte ha supuesto el gran escaparate de los NFTs a nivel mundial. Se mueven cientos de miles de euros al día en la compraventa de estos activos. Esto ha generado una revolución en el mundo del arte, lo que ha provocado que muchísimas marcas a nivel mundial ya estén moviéndose para ofrecer productos en este nuevo mercado digital. Un ejemplo muy claro de esto, son las marcas mundialmente conocidas de Nike o Adidas, las cuales ya ofrecen diferentes artículos en forma de NFTs. Y es que, a esto, también se han sumado diferentes famosos de todo tipo, sacando colecciones de NFTs para sus fans. No cabe duda de que los NFTs han revolucionado el mundo del arte, y de que en este sentido el mercado va a seguir creciendo en el futuro. Sin embargo, vamos a analizar otros posibles usos que se les podrían dar a estos activos no fungibles, así como los sectores que se verían afectados.

Uno de los sectores, que a mi parecer aguarda más potencial, para estos activos es el del *gaming*. Este es un sector que también se ha ido desarrollando mucho en la *blockchain* en los últimos años, convirtiéndose en uno de los sectores con más potencial en el mundo cripto. El mundo de los juegos en línea sobre una base de datos descentralizada tiene cada vez más futuro. Si hay un sector que tiene verdadero potencial para adaptarse a la revolución de la *blockchain* es el del *gaming*, dado que cualquier juego en línea que conozcamos podría potencialmente desarrollarse sobre la *blockchain* de manera descentralizada. De esta manera, el desarrollo del juego pertenecería a sus usuarios, con una potencial fundación sin ánimo de lucro formada por los propios usuarios y encargada de ejecutar las decisiones tomadas por la comunidad. Bajo este marco, no habría una entidad que se beneficia de la venta del juego ni de los artículos dentro del mismo. Habría una comunidad de jugadores, en un juego desarrollado de manera conjunta, con una moneda nativa del juego con la que se podrían adquirir los artículos dentro de este. Esto daría un uso a la moneda del proyecto y por lo tanto un valor. Juegos como el Fortnite, son un ejemplo perfecto del mercado que existe con los artículos dentro de los juegos. Fortnite, al tratarse de un juego gratis, obtiene todos sus ingresos de las ventas dentro del propio juego, con artículos que en este caso no dan ventaja al que los posee, pero que sin embargo si le permiten diferenciarse de los demás jugadores. El Fifa, juego popularmente conocido en el mundo del fútbol, sería un ejemplo perfecto de lo que se conoce como *pay-to-win* o pagar para ganar. Esto se debe a que los jugadores del Fifa, sí que tienen la opción de gastar dinero en artículos que aportan una ventaja de juego frente a los demás usuarios. Tanto el modelo de negocio de Fornite como el del Fifa, tienen en común el gigantesco negocio que hay en el sector del *gaming* con las ventas dentro de los juegos. En este marco aparecen los NFTs. Todos esos artículos que se compran en los juegos podrían ser elaborados como NFTs. Con esta tecnología, los juegos en la *blockchain* podrían ofrecer esos artículos (personajes, sobres de artículos, trajes o disfraces, artículos audio visuales, etc.) en forma de NFTs, otorgando autenticidad, exclusividad y seguridad sobre el artículo que el usuario adquiere dentro del ecosistema del juego. Los beneficios generados por la venta serían distribuidos entre la comunidad con la moneda o token nativo del juego. Esto genera una economía alrededor de un juego en línea, aportando valor al token y sin la necesidad de una empresa central que lo maneje. Este uso de los NFTs aportaría, además, un argumento contra la mayor crítica que tienen los NFTs: su uso, dado que se dice que no sirven para nada más que para especular.

Como venimos diciendo, el sector de los juegos en línea es uno de los que más potencial tiene dentro del mundo de la *blockchain*, además de suponer una increíble oportunidad para los

NFTs. Sin embargo, los NFTs tienen otros usos que podrían situarlos como uno de los activos más útiles dentro de la tecnología *blockchain*. Si pensamos en el gran valor de los NFTs, pensaríamos en la cualidad de propiedad y exclusividad que el usuario tiene sobre el mismo. Esto abre un abanico de posibilidades con productos de hoy en día que podrían migrar hacia el mundo de las criptomonedas. Por ejemplo, las entradas de cualquier evento podrían ser sustituidas o mejoradas por la tecnología de los NFTs, dado que el objetivo final de las entradas es el de reconocer a la persona como propietaria de un derecho de acceso a un evento en cuestión. Actualmente, estos accesos dependen de terceras entidades para poder funcionar. Dependen, por ejemplo, de que los servidores de la compañía que los emite funcionen en el momento de canjearlos. Si aplicamos los NFTs para este tipo de productos, estaríamos prescindiendo de entidades intermediarias además de obtener las ventajas de seguridad y unicidad de estos criptoactivos. Por otro lado, los NFTs albergan un futuro a todo tipo de archivo digital con el que se comercia en internet. Este tipo de activos del que hablamos pueden ser canciones, películas, videos, obras de arte, cartas digitales, etc. Esta posibilidad abre la puerta a que pueda existir en el futuro, por ejemplo, un Netflix en la *blockchain*, donde la propiedad de la película o serie en cuestión pertenezca a la plataforma en forma de NFT, pero que se pueda arrendar a los usuarios. La plataforma sería de los usuarios y podría utilizar su moneda nativa para la comercialización de sus productos dentro de la misma. Esto podría ser el caso con todo tipo de activos digitales dando lugar a cientos de posibilidades. También daría la posibilidad a un artista a sacar ediciones limitadas de sus canciones, ofreciendo a sus fans oportunidad de tener un artículo exclusivo, de sus artistas favoritos. Se podría decir que, los NFTs son la pieza clave para que en un futuro pueda existir una plataforma de *streaming* como Spotify o Netflix en la *blockchain*. El impacto de los NFTs podría extenderse a muchísimos sectores de contenido digital que conocemos hoy en día.

A todos estos usos hay que añadirle el que podrían tener los NFTs en el Metaverso del futuro. Según el artículo publicado en Xakata por Fernández Yubal (2022) “El Metaverso es un mundo virtual, uno al que nos conectaremos utilizando una serie de dispositivos que nos harán pensar que realmente estamos dentro de él, interactuando con todos sus elementos”. Y es que el concepto del Metaverso hay que empezar a tomárselo en serio, dado que, por ejemplo una de las empresas más importantes del mundo como es Facebook, ha cambiado su nombre a Meta como decisión corporativa debido al desarrollo de este nuevo concepto. No solo Facebook ha apostado por esta idea para el futuro, si no que empresas como Google, Nvidia o Microsoft también han anunciado su intención de competir en este nuevo sector digital (Fernández, 2022).

En este complejo mundo virtual, los NFTs podrían jugar el papel de cualquier artículo que existiese en él. Desde ropa virtual hasta propiedades inmobiliarias en el mundo digital. Los NFTs aportarían las condiciones clave de seguridad, exclusividad y unicidad a los bienes del mundo digital del futuro. Aunque todavía está por ver el verdadero potencial que tiene el Metaverso, está claro que las empresas más grandes del mundo ya están invirtiendo en su desarrollo y que los NFTs podrían jugar un papel crucial.

Habiendo visto y analizado los principales usos que se le pueden dar los NFTs, así como los sectores a los que pueden afectar, podemos concluir que estos tipos de activos en la blockchain son mucho más que pura especulación. De asentarse y ponerse en funcionamiento de manera adecuada los NFTs podrían suponer una verdadera revolución en la economía que gira en torno al contenido digital, así como a otros sectores como el del arte y el del entretenimiento.

#### **4. Conclusión**

Desde un primer momento, el objetivo de este trabajo ha sido el de analizar lo que la nueva tecnología *blockchain* podría suponer a la economía del futuro. La manera en la que se ha enfocado este trabajo ha sido la de explicar la tecnología de una manera clara y concisa, sin entrar en tecnicismo, con el fin de tener una idea clara de su funcionamiento a la hora de leer dicho documento. El trabajo se ha focalizado en la parte funcional de las potenciales oportunidades de esta tecnología, más que en el funcionamiento y explicación tecnológica de la misma. Esta ha sido la metodología empleada en todos los apartados de dicho estudio, con el fin de aportar el conocimiento y contexto necesarios para entender la lectura.

Hoy en día es pronto para determinar el verdadero potencial que recoge esta tecnología. Sin embargo, y tras haber realizado el estudio, sí podemos concluir que la tecnología de cadena de bloques va a suponer un punto de inflexión en muchos sectores de la economía. Esto se debe a que la *blockchain* aporta un nuevo ecosistema en la red basado en la descentralización, la seguridad y la transparencia, permitiendo prescindir de entidades centrales para su correcto funcionamiento. Es cierto que, a día de hoy faltan muchas cosas por concretar o mejorar sobre este nuevo mundo como, por ejemplo, la regulación dentro del mismo. Como hemos ido viendo a lo largo del trabajo, el impacto que podría tener en la economía va mucho más allá del Bitcoin. Son muchos los sectores que se verían afectados por una ciencia que permite a los usuarios

desarrollar plataformas de manera conjunta, descentralizadas, con un enfoque mucho más democrático. Hemos podido observar el impacto que tendría el Bitcoin sobre el sistema tradicional de pagos y reserva de valor. Se ha podido analizar las ventajas de las plataformas de los contratos inteligentes y las Dapps, permitiendo desarrollar verdaderos ecosistemas sobre ellas. También se ha estudiado el auge de las finanzas descentralizadas, aportando un concepto totalmente nuevo a un sector como el financiero. Y, por último, se ha planteado el uso que los NFTs podrían tener, provocando una revolución en otros tantos sectores masivos de la economía.

Cuando se creó el Internet también recibió críticas en varios aspectos, la gran mayoría venían debido a la escasa adopción que esta red tenía en sus comienzos. Dado que en ese momento estaba en su etapa de desarrollo y crecimiento. Sin embargo, con los años se fue mejorando y perfeccionando hasta el punto de convertirse en lo que es hoy en día. El mundo está conectado gracias al internet, y actualmente no concebimos un mundo sin él. Como ocurrió con la mayoría de los proyectos que fueron creados cuando internet empezó a funcionar, la mayor parte de los que existen actualmente en el mundo de las criptomonedas desaparecerán. Sin embargo, aquellos proyectos con fundamento, que tengan un protocolo y tecnología potente y un uso que verdaderamente aporte valor, sobrevivirán y se convertirán en verdaderos gigantes en el futuro. Con esto no quiero decir que el mundo de las criptomonedas vaya a suponer la misma revolución que el internet. No obstante, sí que comparten rasgos, y desde luego sí que tiene el potencial necesario para cambiar la economía del futuro.

Aun es pronto para saber con certeza el verdadero alcance de este nuevo concepto de conectividad. Sin embargo, es un mundo lo suficientemente grande como para analizar, dado que en muchos sectores va a suponer una revolución que cambiará por completo la manera de operar en ellos.

## Bibliografía

- 1) Dirk A Zetsche, Douglas W Arner, Ross P Buckley, Decentralized Finance, *Journal of Financial Regulation*, Volume 6, Issue 2, 20 September 2020, Pages 172–203, <https://doi.org/10.1093/jfr/fjaa010>
- 2) Zetsche, Dirk Andreas and Arner, Douglas W. and Arner, Douglas W. and Buckley, Ross P., Decentralized Finance (DeFi) (March 2020). IIEL Issue Brief 02/2020, European Banking Institute Working Paper Series 59/2020, University of Hong Kong Faculty of Law Research Paper No. 2020/010, University of Luxembourg Faculty of Law, Economics & Finance WPS, *Journal of Financial Regulation* - forthcoming, Available at SSRN: <https://ssrn.com/abstract=3539194> or <http://dx.doi.org/10.2139/ssrn.3539194>
- 3) Ametrano, Ferdinando M., Hayek Money: The Cryptocurrency Price Stability Solution (August 13, 2016). Available at SSRN: <https://ssrn.com/abstract=2425270> or <http://dx.doi.org/10.2139/ssrn.2425270>
- 4) Dolader, C., Bel, J. y Muñoz, J.L. (2017). *La blockchain : fundamentos, aplicaciones y relación con otras tecnologías disruptivas*. (Universidad) Universitat Politècnica de Catalunya <https://www.mincotur.gob.es/Publicaciones/Publicacionesperiodicas/EconomiaIndustrial/RevistaEconomiaIndustrial/405/DOLADER,%20BEL%20Y%20MU%C3%91OZ.pdf>
- 5) Clementín, F. (2022). Minería de bitcoin usa 58% de energías renovables. *Criptonoticias*. <https://www.criptonoticias.com/mineria/mineria-bitcoin-usa-58-energias-renovables/>
- 6) da Silva Momo, Fernanda, & Sordi Schiavi, Giovana, & Behr, Ariel, & Lucena, Percival (2019). Business Models and Blockchain: What Can Change?. *RAC - Revista de Administração Contemporânea*, 23(2),228-248.[fecha de Consulta 25 de Marzo de 2022]. ISSN: 1415-6555. Disponible en: <https://www.redalyc.org/articulo.oa?id=84061591005>
- 7) Palacios, Z.J., Vela, M.A. y Tarazona, G.M. (2015). Bitcoin como alternativa transversal de intercambio monetario en la economía digital. *Redes de Ingeniería*, 6(1), 106-128. <https://revistas.udistrital.edu.co/index.php/REDES/article/view/8617/10531>

- 8) Asdrúbal Grillet Correa. Universidad Central de Venezuela .Revista Venezolana de Análisis de Coyuntura, vol. XXV, núm. 1, pp. 41-56, 2019. ¿DINERO CONVENCIONAL O DINERO NO CONVENCIONAL?  
<https://www.redalyc.org/journal/364/36465108009/html/#fn1>
- 9) EFE. (2021, Agosto). Se cumplen 50 años del fin del patrón oro de Bretton Woods. El economista <https://www.eleconomista.es/mercados-cotizaciones/noticias/11359061/08/21/Se-cumplen-50-anos-del-fin-del-patron-oro-de-Bretton-Woods.html>
- 10) *La historia del Bitcoin*. (s.f). xtb.com. <https://www.xtb.com/es/educacion/la-historia-del-bitcoin>
- 11) *¿Es Bitcoin una Reserva de Valor?* (2020). Binance Academy <https://academy.binance.com/es/articles/is-bitcoin-a-store-of-value>
- 12) *¿Qué es una Stablecoin?* (s.f). Bit2Me Academy. <https://academy.bit2me.com/que-es-stablecoin/>
- 13) *¿Qué es AAVE?* (s.f). Bit2Me Academy. <https://academy.bit2me.com/que-es-aaave/#:~:text=AAVE%2C%20o%20anteriormente%20ETHLend%2C%20es,esquema%20que%20revoluciono%20este%20sector.>
- 14) *Real Academia Española*. (s.f.). *Cultura. En Diccionario de la lengua española. Recuperado en 6 de junio de 2022, de* <https://dle.rae.es/fungible>
- 15) McCracken, T. (2022). Cardano Deep Dive: Info you NEED about Cardano and ADA. *Coinbureau*. <https://www.coinbureau.com/review/cardano-ada/>
- 16) *¿Qué es Solidity en los smart contracts de Ethereum Blockchain?* (s.f). Bit2Me Academy. <https://academy.bit2me.com/que-es-solidity-smart-contracts-ethereum/>
- 17) *¿Qué son las DApps?* (s.f). Bit2Me Academy. <https://academy.bit2me.com/que-son-las-dapps/>
- 18) *¿Qué es Uniswap? ¿Cómo funcionan los Pools?* (2020). Cryptoplaza. <https://cryptoplaza.es/que-es-uniswap-como-funcionan-los-pools/>
- 19) Banafa, A. (2020). *Soft Fork y Hard Fork en Blockchain*. OpenMind BBVA. <https://www.bbvaopenmind.com/tecnologia/mundo-digital/soft-fork-y-hard-fork-en-blockchain/>
- 20) *How Uniswap Works*. (s.f). Uniswap Docs. <https://docs.uniswap.org/protocol/V2/concepts/protocol-overview/how-uniswap-works#:~:text=Uniswap%20is%20an%20automated%20liquidity,%2C%20censorship%20resistance%2C%20and%20security.>

- 21) ¿Qué son las 'stablecoins' y para qué sirven? (2021). BBVA.  
<https://www.bbva.com/es/que-son-las-stablecoins-y-para-que-sirven/>
- 22) Crowdfunding: ¿Qué es? ¿Cómo funciona?. (2021). VIVUS.  
<https://www.vivus.es/blog/crowdfunding-que-es-como-funciona>
- 23) Biurrun A. (Octubre 26, 2021). España ya prefiere pagar con tarjeta a hacerlo con dinero en efectivo. *La Razón*.  
<https://www.larazon.es/tecnologia/20211026/2exixsexo5euvkjctik3kxd3ym.html#:~:text=Este%20cambio%20de%20tendencia%20tambi%C3%A9n,un%2054%25%20de%20los%20encuestados.>
- 24) Montaner, D. ¿Quiénes son los principales competidores de Ethereum?. (2021). Criptomundo. [criptomundo.com/quienes-son-los-principales-competidores-de-ethereum/](https://criptomundo.com/quienes-son-los-principales-competidores-de-ethereum/)
- 25) Echebarría, M. (2017). *CONTRATOS ELECTRONICOS AUTOEJECUTABLES (SMARTCONTRACT) Y PAGOS CON TECNOLOGÍA BLOCKCHAIN*. Universidad de Valladolid
- 26) Wang, Q., Li, R., Wang, Q., & Chen, S. (2021). Non-fungible token (NFT): Overview, evaluation, opportunities and challenges. arXiv preprint arXiv:2105.07447.
- 27) Wang, Q., Rujia, L., Wang, Q., Chen, S. (2021). Non-Fungible Token (NFT): Overview, Evaluation, Opportunities and Challenges [Informe Tecnológico]. Arxiv Cornell University. <https://arxiv.org/abs/2105.07447>
- 28) Grayscale. (2021). *An Introduction to Solana*. <https://grayscale.com/wp-content/uploads/2021/12/grayscale-building-blocks-solana-1.pdf>
- 29) Fetsyak, I. (2020). *CONTRATOS INTELIGENTES: ANÁLISIS JURÍDICO DESDE ELMARCO LEGAL ESPAÑOL*. Universidad de La Rioja
- 30) Fernández, Y. (16 mayo 2022). *Qué es el Metaverso, qué posibilidades ofrece y cuándo será real*. Xakata. <https://www.xakata.com/basics/que-metaverso-que-posibilidades-ofrece-cuando-sera-real>
- 31) Kumar, B, Panda y Jena, D. (2018). An Overview of Smart Contract and Use Cases in Blockchain Technology. *9th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, pp1-4, doi: 10.1109/ICCCNT.2018.8494045.
- 32) Bitcoin como desastre medioambiental: que sea el mayor despilfarro energético de la historia depende de su futuro. (2021). Javier Pastor

<https://www.xataka.com/criptomonedas/bitcoin-como-desastre-medioambiental-que-sea-mayor-despilfarro-energetico-historia-depende-su-futuro>