



UNIVERSITAS
Miguel Hernández

FACULTAD DE CIENCIAS SOCIALES Y JURÍDICAS DE ELCHE
GRADO EN ADMINISTRACIÓN Y DIRECCIÓN DE EMPRESAS

Curso 2022/2023



CRIPTOMONEDAS Y BLOCKCHAIN:

**POSIBILIDADES DE IMPLANTACIÓN E IMPACTO ECONÓMICO Y
FINANCIERO**

Junio 2023

Autor: Eric Miralles Orozco

Tutorizado por: Prof. Dra. Juana Aznar Márquez

Índice

Resumen	2
Justificación	3
Introducción	5
Objetivos.....	6
1.Dinero, funciones y propiedades.....	7
1.1 Origen e historia del dinero.....	7
1.2 Propiedades y funciones del Dinero	9
1.3 Como se crea el dinero. El papel de los bancos centrales y comerciales.	10
2.Blockchain	14
2.1 Aplicaciones de la Blockchain	16
2.1.1 Criptomonedas y pagos:	16
2.1.2 Smart Contracts	17
2.1.3 Identidad Digital	17
2.1.4 Propiedad intelectual y derechos de autor	18
2.1.5 Votación y elecciones	19
2.1.6 Cadena de suministros	19
3.Criptomonedas	20
3.1 Clasificación de Criptomonedas	20
4. Regulación de las Criptomonedas	28
4.1 Marco Europeo.....	29
4.2 Enfoques en la regulación de los criptoactivos	34
4.2.1 Caso de España	35
5.Viabilidad de las criptomonedas en la economía y las finanzas.	37
5.1 Bitcoin	38
5.1.1 Funcionamiento de Bitcoin.....	39
5.1.2 Bitcoin: Divisa o Reserva de valor.....	40
5.1.3 Otras implicaciones de la adopción de Bitcoin	46
5.2 Ethereum.....	48
5.2.1 Protocolos DeFi en Ethereum y utilidades.....	49
Conclusiones	52
Bibliografía.....	55

Resumen

Este trabajo pretende aportar y complementar la información existente sobre las criptomonedas, tratando de realizar un análisis sobre cómo estas pueden influir en la economía y las finanzas tradicionales.

Para ello, primeramente, se realiza una revisión sobre el origen del dinero y su evolución a lo largo del tiempo, desde los primeros medios de intercambio hasta las monedas fiduciarias actuales.

Se conocerá cuáles son las funciones y las propiedades que debe tener un activo para funcionar eficazmente como dinero, así como el mecanismo que tienen los bancos centrales y comerciales para crear dinero y gestionar la oferta monetaria.

A continuación, se analizará la tecnología sobre la que se sustentan las criptomonedas, la Blockchain. Para ello se explicará su funcionamiento y cómo se consigue la descentralización y la privacidad por la que las criptomonedas son famosas. Sin embargo, las criptomonedas no son la única aplicación de la Blockchain. Para conocer el potencial de esta tecnología se comentarán las principales utilidades que se pueden construir gracias a la Blockchain, como los contratos inteligentes, la identidad digital o la cadena de suministros.

Una vez conocida la Blockchain, se presentarán los principales tipos de criptomonedas, clasificadas según la función para la que se concibieron. En este apartado se detallará en qué consisten las diferentes criptomonedas y cuáles son las utilidades que tienen, desde funcionar como un medio de pago, hasta criptomonedas que permiten desarrollar aplicaciones digitales de todo tipo en su ecosistema.

En este punto se analizará la regulación y normativa existente sobre las criptomonedas en el marco de la Unión Europea y en el caso de España. Conocer los distintos enfoques que están adoptando los legisladores es clave para tratar de vislumbrar el futuro que puedan tener las criptomonedas, ya que el marco jurídico que se proporcione podría tanto impulsar como restringir la adopción de esta tecnología.

En la siguiente parte del trabajo se estudiará la viabilidad de la implantación de las criptomonedas a nivel económico y financiero, poniendo el foco de atención las dos criptomonedas más extendidas y con mayores repercusiones en estos ámbitos, Bitcoin y Ethereum.

Se estudiará el funcionamiento y el propósito por el que Bitcoin fue creado y se analizará la posibilidad de que Bitcoin pueda llegar a convertirse una nueva forma de dinero. Para ello será necesario comprender en qué medida Bitcoin cumple con las funciones y propiedades que debe tener el dinero y cuáles son sus limitaciones. Además, se darán a conocer algunas otras implicaciones que puede tener Bitcoin de llegar a ser adoptado.

Finalmente, por la parte de Ethereum, se verá cuales son las distintas funcionalidades y soluciones que se pueden construir sobre su ecosistema. Ethereum se presenta como una nueva forma de ofrecer servicios financieros, entre otras utilidades, por lo que se tratarán las principales implicaciones en este ámbito.

Con todo ello se procurará proporcionar una base de información actualizada, hasta el momento, que ayude a comprender las implicaciones que pueden tener las criptomonedas en los ecosistemas financieros y económicos.

Justificación

En los últimos años, las criptomonedas y la blockchain han generado un gran interés en la economía mundial, gracias a su capacidad de transformar el sistema financiero y monetario tradicional. Esta nueva tecnología ha sido objeto de numerosos estudios como el de Swan (2015), que analiza cómo la implementación de la tecnología blockchain en sectores como el financiero podría mejorar la eficiencia de los procesos y reducir los costos, lo que se traduciría en un impacto positivo en la economía.

Sin embargo, aunque se ha escrito mucho en este campo, la velocidad a la que evolucionan las criptomonedas y sus aplicaciones pone de manifiesto la

necesidad de un mayor número de análisis y trabajos como este, que puedan proporcionar información valiosa para aprovechar su potencial para transformar el sistema financiero tradicional y la economía global.

Esto cobra aún más importancia teniendo en cuenta que las criptomonedas son una tecnología que sigue generando mucha desconfianza en la población. Esto se debe sobre todo al auge especulativo de estos activos en los últimos años y a la existencia de un gran número de estafas que han tenido lugar aprovechando su “juventud” y la falta de regulación.

Si bien, también es cierto que el bajo nivel de educación financiera, sumado a la falta de información accesible y fiable, son factores que están condicionando la confianza de los usuarios para utilizar las criptomonedas de un modo no especulativo.

Es imprescindible, por tanto, comprender cómo los cripto activos como bitcoin pueden cambiar aspectos sumamente importantes a nivel global. Una de las cuestiones más debatidas es la posibilidad de emplear alguno de estos activos como sistema de pago capaz de sustituir al dinero fiduciario tradicional, lo que tendría un impacto directo en todas las esferas financieras de la sociedad, las empresas y los gobiernos.

De hecho, uno de los aspectos más interesantes a tratar es la posibilidad de utilizar las criptomonedas y su tecnología para conseguir una mejor inclusión financiera. Esto no solo tiene relevancia en las sociedades desarrolladas, sino que cobra especial importancia en los países emergentes y en vías de desarrollo, donde la bancarización y el acceso a servicios financieros es, en muchos casos, inexistente o de muy difícil acceso.

Así pues, el análisis sobre el impacto y las posibilidades que ofrecen las criptomonedas y la tecnología blockchain es importante en la actualidad para entender las implicaciones de esta revolución financiera. La realización de un trabajo en este campo puede proporcionar una mejor comprensión de cómo la

tecnología está transformando los sistemas financieros, la economía y la sociedad en general.

Introducción

Según datos de *CoinMarketCap* (2 de abril de 2023), portal de referencia para estadísticas de criptomonedas, la capitalización de mercado del global de todos los criptoactivos se encuentra en \$1,18 Trillones americanos, con un volumen diario de aproximadamente \$50 Billones americanos. Por capitalización total, esto correspondería al PIB de la 22ª economía del mundo. Además, durante el gran auge de las criptomonedas, en noviembre de 2021, la capitalización del mercado de criptoactivos superó los \$2,97 Trillones.

Figura 1 Capitalización de mercado total de los criptoactivos



Fuente: Recuperado de coinmarketcap.com¹

¹ Gráfico obtenido de <https://coinmarketcap.com/charts/>

Estos datos, aunque son ciertamente indicativos del movimiento de las criptomonedas, van ligados en gran medida a su precio, y, por tanto, a intereses especulativos. Sin embargo, no solamente ha crecido la capitalización de mercado. En el último informe “*Crypto Market Sizing Report 2022*” de Crypto.com (2023) se muestra la evolución en el número de usuarios de criptomonedas, llegando a 425 millones en diciembre de 2022. Además, estas cifras de crecimiento en el tiempo se comparan a menudo, por su similitud, con la evolución en usuarios que tuvo la adopción de internet desde sus inicios. Se calcula que la situación actual de la adopción de las criptomonedas sería similar a la de internet en 1998, cuando todavía le quedaba un largo recorrido por delante.

Estos datos ponen de manifiesto la rápida y cuantiosa evolución que ha tenido el sector de las criptomonedas, tanto por su aspecto especulativo como por la cantidad proyectos y funcionalidades distintas que se están desarrollando en su ecosistema. No cabe duda de que las criptomonedas son ya una parte importante y en crecimiento de la revolución tecnológica actual y que están presentes en multitud de esferas cotidianas, sobre todo a nivel financiero y económico.

Objetivos

Objetivo General: analizar el impacto de la blockchain y los cripto activos en la economía y las finanzas.

Objetivos Específicos:

- Conocer las bases de funcionamiento que dan utilidad a los cripto activos y a la blockchain.
- Conocer el marco regulador de los cripto activos en Europa y España.
- Analizar la influencia de bitcoin y otros cripto activos a nivel financiero y económico.
 - Analizar la viabilidad de bitcoin desde una perspectiva monetaria.

- Analizar las posibilidades de implantación Bitcoin y otros cripto activos en los sistemas financieros.
- Comprender las utilidades y limitaciones de las principales criptomonedas a nivel económico y financiero.

1. Dinero, funciones y propiedades.

1.1 Origen e historia del dinero.

El dinero es una herramienta esencial en la economía moderna, pero su origen es antiguo y complejo. La historia del dinero se remonta a miles de años atrás, cuando los seres humanos empezaron a necesitar un medio de intercambio para facilitar el comercio. Las primeras formas de intercambio fueron el trueque, de manera que los bienes y servicios se intercambiaban directamente unos por otros. Este método, aunque simple, tenía sus limitaciones, por ejemplo, como apuntaba Menger (1892), *“en esos casos, en los que la oferta y la demanda cuantitativamente no coinciden; en los cuales, una mercancía indivisible debe ser intercambiada por una variedad de productos ... que sólo se las demanda en determinadas oportunidades y que únicamente pueden ser suministradas por ciertas personas....., el intercambio de los bienes en cuestión, como regla general y por necesidad, no se realizaría”*. Además, el trueque tiene otros inconvenientes, como el hecho de no permitir el ahorro, lo que limitaba el crecimiento económico.

Ante estas dificultades, las personas empezaron a utilizar objetos que eran aceptados por todos como medio de intercambio. Estos objetos podían ser conchas, cuentas de vidrio, metales preciosos o cualquier otra cosa que tuviera valor en sí misma o que pudiera ser convertida en algo valioso, como lo serían posteriormente las monedas.

Según Whipps (2007), se cree que las primeras monedas fueron acuñadas en el Reino de Lidia en el s.VII A.C. Las monedas, fabricadas en metales como el oro, la plata y el bronce, se utilizaban para representar el valor de los bienes y

servicios en una sociedad. A medida que las monedas se fueron extendiendo por el mundo, se convirtieron en una forma más práctica y conveniente de intercambio que el trueque. Con el tiempo se crearon otras formas de dinero, como los billetes y las letras de cambio, que permitían a las personas realizar transacciones comerciales sin tener que transportar grandes cantidades de monedas.

La invención de la moneda fue un gran paso adelante en la historia del dinero, pero no fue hasta 1668 que se creó el primer banco central del mundo en emitir papel moneda, el Banco Nacional de Suecia, que se encargó de gestionar el dinero y las finanzas del país (Alfonzo, 2018).

Es especialmente destacable que, durante el siglo XIX, muchos países adoptaron el patrón oro, de manera que el valor de una moneda estaba respaldado por una cantidad determinada de oro. El patrón oro permitió a los ciudadanos cambiar sus billetes por una cantidad de oro previamente fijada por las autoridades.

El patrón oro se mantuvo vigente en muchos países hasta el inicio de la Primera Guerra Mundial, cuando Gran Bretaña decidió abandonarlo en 1914 para financiar los gastos militares. Otros países europeos, como Alemania y Francia, abandonaron el patrón oro después de la guerra debido a la devaluación de sus monedas, la inflación y las dificultades para mantener sus reservas de oro. Y sucesivamente, con un sistema monetario internacional que se volvió más complejo, los diferentes países comenzaron a abandonar el patrón oro.

Desde entonces, la mayoría de los países han adoptado sistemas monetarios basados en el dinero fiduciario, es decir, en el que el valor de una moneda no está respaldado por ningún bien tangible, sino por la confianza en la economía y el gobierno del país emisor.

1.2 Propiedades y funciones del Dinero

Mankiw (2014) define el dinero como “la cantidad de activos que pueden utilizarse fácilmente para realizar transacciones”, y añade que dicho dinero tiene tres funciones básicas, concretamente:

- 1) Medio de cambio. El dinero es un medio de cambio porque permite que las personas intercambien bienes y servicios sin necesidad de realizar un trueque, lo que simplifica en gran medida el comercio y aumenta la eficiencia del mercado.
- 2) Unidad de cuenta. Lo que significa que es una forma comúnmente aceptada de medir el valor de los bienes y servicios en una economía. El uso del dinero como unidad de cuenta facilita la comparación de precios y la realización de cálculos económicos, lo que permite a las personas tomar decisiones informadas sobre cómo gastar y ahorrar su dinero.
- 3) Depósito de valor. Esta función se refiere a la capacidad del dinero de mantener su valor a lo largo del tiempo, lo que permite que las personas lo utilicen como un medio para ahorrar, hacer frente a situaciones imprevistas y planificar su futuro financiero.

Como se ha comentado en el apartado anterior, a lo largo de la historia multitud de activos han venido cumpliendo con estas funciones. Incluso en determinados momentos y situaciones se ha utilizado objetos como alcohol o cigarrillos, que se emplearon en los campos de concentración durante la II Guerra Mundial, como se muestra en el artículo de Radford (1945). Esto nos indica que una gran cantidad de objetos o “activos” pueden ser utilizados como dinero (Weber, 2021).

Sin embargo, no todos estos activos son igual de eficientes o efectivos para actuar como dinero y cumplir sus funciones. A continuación, se recogen las propiedades que debería tener el dinero para ser realmente útil según la Reserva Federal de St. Louis (*St. Louis Fed*, s. f.).

Durabilidad: el dinero debe ser resistente al desgaste y al paso del tiempo, de manera que pueda ser usado en múltiples transacciones sin deteriorarse. Para lograr esto, los billetes y monedas están hechos de materiales resistentes y duraderos, como el papel moneda y el metal.

Portabilidad: el dinero debe ser fácilmente transportable y manejable, de manera que se pueda utilizar en cualquier lugar. El papel moneda y las monedas están diseñados para ser fácilmente transportados en bolsillos, carteras y bolsas.

Divisibilidad: el dinero debe ser divisible en unidades más pequeñas para poder adaptarse a diferentes necesidades de transacción. Por ejemplo, un billete de \$100 dólares pueden ser dividido en diez billetes de \$10 dólares, o en 100 monedas de \$1 dólar.

Uniformidad: Cada unidad de dinero debe ser igual en valor y calidad, para que sea aceptada en todas partes. De esta forma, un billete de \$20 dólares es igual en valor y calidad en cualquier parte del mundo donde se acepte el dólar estadounidense.

Escasez: El dinero debe ser relativamente escaso para tener valor, ya que, si fuera abundante, su valor se reduciría. La escasez se logra a través de la regulación de la oferta de dinero, ya sea por parte de los gobiernos o por el mercado.

Aceptabilidad: El dinero debe ser ampliamente aceptado y reconocido como medio de intercambio en la economía. Para lograr esto, es necesario que el dinero sea aceptado por los comerciantes y la población en general.

1.3 Como se crea el dinero. El papel de los bancos centrales y comerciales.

Como Mankiw (2014) explica en su manual, la “oferta monetaria” es el nombre que se da a la cantidad de dinero existente. Las formas más utilizadas para medir la oferta monetaria son la masa monetaria M2, que incluye el efectivo en

manos del público (monedas y billetes), los depósitos a la vista y los depósitos a corto plazo, y la M3, que engloba a la M2 e incluye los depósitos a plazo.

En los países que utilizan dinero fiduciario, son los bancos centrales los que controlan esta oferta monetaria a través de lo que se conoce como “política monetaria”. Si bien es cierto que la banca comercial también tiene la capacidad para incrementar la oferta monetaria, esta capacidad acaba estando condicionada por las directrices de los bancos centrales. A continuación, se explicará brevemente como los bancos centrales y la banca comercial pueden aumentar la oferta monetaria.

El mecanismo que tiene la banca comercial para generar dinero es a través de los préstamos, mediante el “sistema de reservas fraccionado”. De esta forma, cuando una persona realiza un depósito en el banco, digamos 1.000€, el banco pasa a ser acreedor del depositante por esa cantidad. Sin embargo, el banco únicamente tiene obligación de mantener una pequeña cantidad de ese depósito como reserva (coeficiente de reserva obligatorio o coeficiente de caja), pudiendo utilizar el resto para otras operaciones.

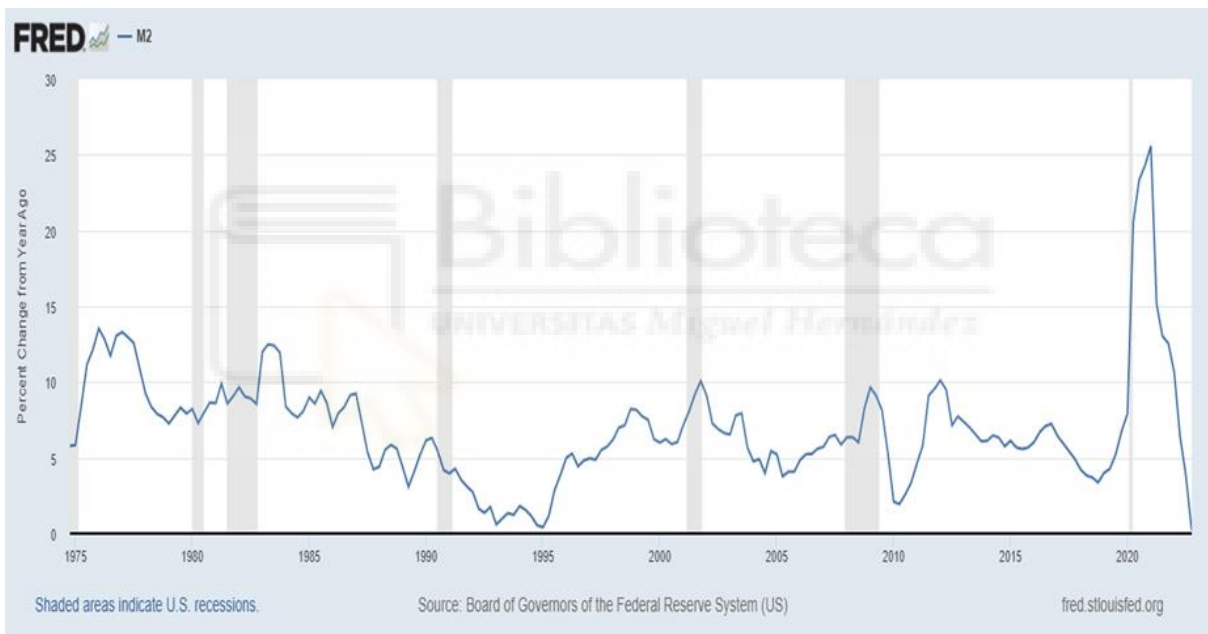
Así, si el banco decide utilizar 900€ de ese depósito para prestárselos a otra persona, el total de dinero existente acaba de aumentar de 1.000€ a 1.900€, ya que el primer depositante todavía podrá ver en el balance de su cuenta sus 1.000€, y además la persona que pidió el préstamo verá que en su cuenta aparecen 900€. Esta operación se puede repetir sucesivas veces, aunque no de forma ilimitada, ya que, como se ha comentado anteriormente, la banca comercial está condicionada por la regulación del banco central, que puede influir la capacidad de creación de dinero estableciendo el porcentaje obligatorio de reservas que debe mantener los bancos. Cuantas más reservas deba mantener el banco, menos capacidad para hacer préstamos tendrá y, por tanto, menos capacidad para generar dinero.

El otro gran instrumento de política monetaria que tienen los bancos centrales para controlar la oferta monetaria, además del coeficiente de caja, son las Operaciones de Mercado Abierto. Esto consiste en que los bancos centrales

realicen operaciones de compraventa de deuda pública de los países, de forma que, cuando un banco central compra deuda de un país está inyectando liquidez en la economía e incrementando la oferta monetaria, mientras que cuando vender títulos de deuda ocurre lo contrario.

Un ejemplo de intervención de los bancos centrales fue la realizada como consecuencia de la crisis generada por el Covid-19. De hecho, el incremento del agregado M2 ha sido el más rápido y agresivo en la historia. En el Figura 2 se muestra el cambio porcentual de la M2 en Estados Unidos desde 1975.

Figura 2 Cambios porcentuales en la M2 en Estados Unidos



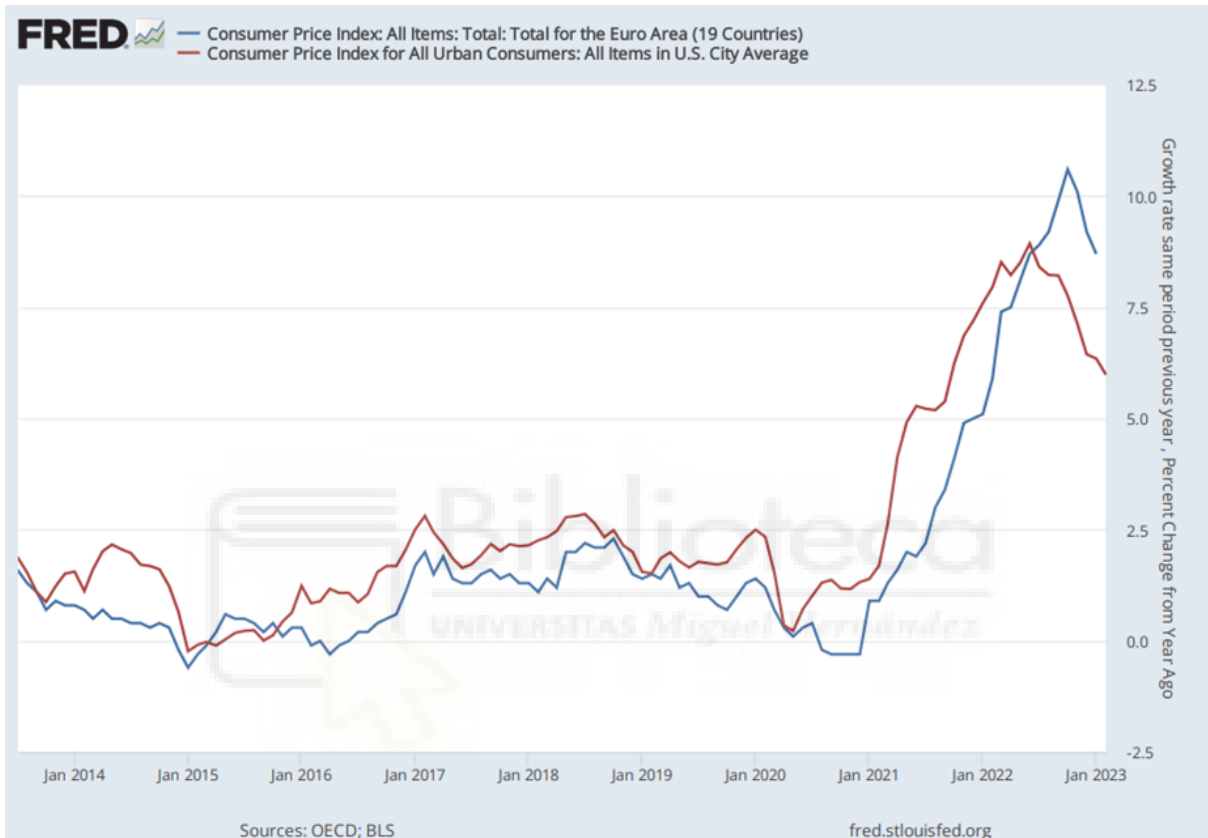
Fuente: Reserva Federal de St.Louis²

Aunque el gráfico anterior sólo muestra los cambios en la M2 en EEUU, el fuerte incremento de la masa monetaria de 2019 y 2020 se ha replicado en un gran número de países con el objetivo de inyectar dinero en la economía para hacer frente a la crítica situación durante la pandemia. Sin embargo, esta financiación “gratuita” mediante el incremento de la oferta monetaria no está exenta de peligros. Una de las consecuencias más notorias de crear tanto dinero es que éste se

² Gráfico obtenido de <https://fred.stlouisfed.org/series/M2SL>

devalúa, generando inflación en la economía. Como se puede observar en la Figura 3, en 2020 la inflación comenzó a dispararse tanto en la zona euro como en Estados Unidos, llegando hasta cotas de 10,6% y 8,9% respectivamente.

Figura 3: Datos de Inflación en EEUU y la Eurozona



Fuente: Reserva Federal de St. Louis³

De hecho, esta desbocada inflación que se aleja del objetivo de los bancos centrales, que es el 2%, es el motivo por el cual en la Figura 2 se observa una reducción muy pronunciada del crecimiento del dinero en el año 2022. Los bancos centrales están intentando controlar la inflación combinando reducciones de la oferta monetaria con incrementos de los tipos de interés a un ritmo histórico. De esta forma se puede concluir que el control de la oferta monetaria es un arma de

³ Gráfico obtenido de <https://fred.stlouisfed.org/series/CPIAUCSL>

doble filo con consecuencias económicas y financieras indeseadas si no se utiliza de forma adecuada.

En definitiva, el dinero es un elemento fundamental en la economía y las finanzas, y su correcto funcionamiento es esencial para el bienestar económico de cualquier sociedad. Sin embargo, el dinero tal y como lo conocemos no está exento de problemas y limitaciones.

Por ello, cada vez son más los que ven en las criptomonedas, como Bitcoin, una alternativa atractiva al sistema monetario actual. Pero antes de adentrarnos en el análisis de estas criptomonedas, es necesario entender la tecnología en la que se basan: la blockchain. El siguiente apartado, se centrará en explicar en qué consiste esta tecnología y cómo ha revolucionado la forma en la que se concibe la economía y las finanzas.

2. Blockchain

Aunque la tecnología blockchain existe desde 1991, no es hasta 2008 con la aparición de Bitcoin que esta tiene una utilidad real y comienza a visibilizarse. Blockchain es una tecnología de registro distribuido de información, que permite la creación de una base de datos compartida y segura, sin necesidad de una autoridad central que la supervise, es decir, descentralizada.

Se trata de una red de ordenadores llamados “nodos”, que están interconectados y trabajan en conjunto para mantener un registro de transacciones que se van añadiendo en bloques de información sucesivos, los cuales son enlazados mediante complejos algoritmos criptográficos, formando así una cadena de bloques o blockchain.

Cada nodo puede introducir información en un bloque de manera autónoma, y la información contenida en cada bloque es verificada y validada por todos los nodos de la red, lo que hace que sea prácticamente imposible manipular la

información. Además, cada bloque contiene la información de su bloque anterior, lo que impide que un bloque pueda ser modificado sin modificar también todos los bloques que lo preceden. Esto crea un sistema altamente resistente a la manipulación y la falsificación, lo que la convierte en una tecnología muy segura y confiable.

En cuanto a su funcionamiento, cada nodo de la red tiene una copia completa de la cadena de bloques, lo que permite que cada uno de ellos pueda leer, verificar y validar la información contenida en los bloques, haciendo así la información totalmente transparente para los usuarios. Cada transacción es validada por los nodos de la red, que comprueban que la información es correcta y que se cumple con las reglas establecidas en el protocolo de la cadena de bloques. De esta forma, cualquier información introducida con datos erróneos, maliciosos o con manipulaciones sería rechazada por el resto de los nodos.

La blockchain es básicamente un libro mayor de contabilidad que, en lugar de estar registrado únicamente por una entidad, como pudiera ser un banco, está registrado por todos los nodos que componen la red, eliminando así la necesidad de confiar en un único ente que salvaguarde la información. Esto permite que todos los participantes puedan verificar y consultar el registro, asegurando así la integridad de su contenido.

La seguridad es el pilar central de la blockchain. Autores como J. Wang et al. (2019), destacan la importancia de la seguridad y privacidad en la tecnología blockchain. Estos autores abordan también los desafíos de seguridad y privacidad en la tecnología blockchain y discuten posibles soluciones para abordar estos problemas.

Las distintas Blockchain se pueden clasificar en tres tipos: públicas, privadas y consorcio.

- Las blockchain públicas, como Bitcoin y Ethereum, permiten la participación de cualquier persona en la red y ofrecen transparencia y descentralización, lo que significa que no hay un ente centralizado que controle la red.

- Las blockchain privadas, en cambio, son utilizadas dentro de una organización o empresa, y sólo son accesibles por las personas autorizadas. En estas redes, la seguridad y la privacidad son las principales preocupaciones.

- Las blockchain consorcio son una mezcla de las anteriores, y son utilizadas por grupos de empresas o instituciones que trabajan juntas para crear una red compartida, pero en la que sólo los miembros autorizados pueden participar en la validación de transacciones y la gestión de la red.

2.1 Aplicaciones de la Blockchain

Como se ha mencionado previamente, la tecnología Blockchain es la base para muchas otras tecnologías y aplicaciones. Es importante pues conocer cuáles son las principales esferas a las que puede afectar este sistema de registro de información y cuáles son sus aportaciones.

2.1.1 Criptomonedas y pagos:

La creación de Bitcoin y otras criptomonedas fue el primer caso de uso de la tecnología Blockchain. Además, se han desarrollado otras criptomonedas que tienen aplicaciones más allá del ámbito financiero, como por ejemplo la tokenización de activos no financieros, haciendo que su valor sea fácilmente divisible y transmisible.

Un “token” es una unidad de cualquier criptomoneda. Por tanto, la tokenización supone asignar un número definido de tokens a un activo, como una vivienda. De esta forma, la vivienda puede ser un activo inmobiliario controlado proporcionalmente por múltiples personas, en función de la cantidad de tokens que hayan adquirido.

2.1.2 Smart Contracts

La tecnología blockchain también permite la creación y ejecución de contratos inteligentes (smart contracts), que son programas informáticos que se ejecutan automáticamente una vez que se cumplen ciertas condiciones predefinidas. Estos contratos permiten a las partes establecer acuerdos sin la necesidad de un intermediario y pueden ser utilizados en una amplia gama de transacciones financieras y comerciales.

Un ejemplo de aplicación de smart contracts es en el mercado de seguros. Una aseguradora podría utilizar un contrato inteligente para automatizar la reclamación y el pago de una póliza. El contrato estaría programado para detectar automáticamente si se ha producido un evento asegurado y, en ese caso, pagar automáticamente al asegurado.

Otro ejemplo es el uso de smart contracts en el sector inmobiliario. Los contratos inteligentes pueden ser utilizados para automatizar la compra y venta de propiedades, lo que reduce el tiempo y los costos asociados con los intermediarios tradicionales como abogados y agentes inmobiliarios.

2.1.3 Identidad Digital

Otra de las aplicaciones de la blockchain se aplica en el registro de identidades digitales, lo que podría ayudar a combatir el fraude y el robo de identidad. La blockchain permite la creación de registros inmutables y seguros de identidades digitales, lo que puede ser utilizado por gobiernos, empresas y organizaciones para verificar la identidad de los usuarios.

Por ejemplo, la plataforma Sovrin⁴ se dedica a ofrecer soluciones de identidad digital descentralizada y segura a nivel mundial utilizando blockchain. Los usuarios pueden crear su propia identidad digital en la plataforma, la cual está protegida por

⁴ <https://sovrin.org/>

criptografía y utilizarla, gracias a su red, en cualquier lugar del mundo. Además, los usuarios pueden controlar quién tiene acceso a su información personal y quién no.

Otro ejemplo similar es la plataforma Civic⁵. La empresa se especializa en proporcionar servicios de identidad para empresas y aplicaciones descentralizadas, de forma que pueden verificar su identidad en diferentes sitios web sin tener que proporcionar su información personal cada vez. La plataforma utiliza tecnología punta en criptografía y seguridad para garantizar que la información del usuario esté protegida en todo momento.

2.1.4 Propiedad intelectual y derechos de autor

La tecnología blockchain también puede ser utilizada para la protección y gestión de propiedad intelectual y derechos de autor. Los registros en la cadena de bloques pueden utilizarse para crear sellos de tiempo y firmas digitales que proporcionen una prueba inmutable de la propiedad y autenticidad de los trabajos creativos. Además, los contratos inteligentes pueden ser utilizados para automatizar el pago de regalías y garantizar que los creadores reciban una compensación justa por su trabajo.

Un ejemplo de esta aplicación es la plataforma de distribución de música basada en blockchain, Ujo Music. La plataforma permite a los músicos subir y vender su música directamente a los oyentes, eliminando intermediarios y asegurando una compensación justa a los creadores. Además, la plataforma utiliza contratos inteligentes para garantizar el pago de regalías y la protección de los derechos de autor.

Otro ejemplo de aplicación de la tecnología blockchain en propiedad intelectual y derechos de autor es la plataforma Monegraph. Esta plataforma permite a los creadores de contenido proteger y gestionar sus obras digitales de manera segura y eficiente. Monegraph registra la propiedad intelectual de las obras en la blockchain, demostrando su autoría y estableciendo licencias de uso y distribución

⁵ <https://www.civic.com/>

de forma transparente y automatizada. De esta manera, se puede evitar la piratería y el uso no autorizado de las obras, y los creadores pueden recibir compensación por su trabajo de manera más eficiente y justa.

2.1.5 Votación y elecciones

La blockchain también se está utilizando en la creación de sistemas de votación electrónica más seguros y transparentes. En su artículo Kshetri y Voas (2018) explican el funcionamiento de la Votación Electrónica por Blockchain (BEV) y muestra algunos ejemplos de ello. Al utilizar la blockchain, es posible crear un sistema de votación que no pueda ser manipulado y que garantice la transparencia y la seguridad de los votos. Esto puede mejorar significativamente la confianza en los procesos electorales.

2.1.6 Cadena de suministros

La cadena de suministro es un proceso crítico para muchas empresas, y va desde el fabricante hasta el consumidor final. Al utilizar la tecnología blockchain, las empresas pueden rastrear y verificar la procedencia de los productos en cada paso del proceso de producción y transporte. Esto permite que la cadena de suministro sea más transparente, lo que puede mejorar la confianza de los clientes y permite gestionar la responsabilidad en caso de problemas o defectos en los productos.

Además, la blockchain puede mejorar la eficiencia de la cadena de suministro al automatizar los procesos y reducir los costos. La tecnología puede permitir una mayor coordinación entre los diferentes participantes de la cadena de suministro, lo que puede ayudar a evitar errores y reducir los retrasos en el proceso.

La compañía IBM⁶, por ejemplo, ha creado todo un sistema de soluciones de Supply Chain basada en Blockchain, ofreciendo todas estas ventajas a aquellas empresas que requieran de grandes movimientos logísticos y de suministros en sus actividades.

⁶ <https://www.ibm.com/supply-chain-visibility>

3. Criptomonedas

Como se ha visto en el apartado anterior, la blockchain es una tecnología revolucionaria que permite el registro seguro e inmutable de transacciones en línea, y es precisamente esta tecnología la que ha hecho posible la creación y el funcionamiento de las criptomonedas. Estas son un tipo de moneda digital que opera de forma descentralizada y se basa en la seguridad y transparencia de la blockchain.

Las criptomonedas han tenido un rápido crecimiento, tanto a nivel de transacciones en el mercado de la especulación, como en el número de usuarios para una utilización monetaria y desarrollo tecnológico. Conocer los distintos tipos de criptomonedas existentes y sus diferentes funcionalidades es clave para el análisis objeto de este trabajo.

En este apartado se profundizará en el conocimiento de las principales criptomonedas, explorando su funcionamiento general y la forma en la que pueden influir en la economía, las finanzas y la sociedad. Se analizará así las posibilidades y limitaciones que tiene dicha tecnología al aplicarla en estos ámbitos.

3.1 Clasificación de Criptomonedas

Clasificar las criptomonedas puede ser un proceso complejo debido a la gran variedad que existen y a las diferentes características que presentan. Sin embargo, una forma común de hacerlo es por su función o propósito, lo que permitirá también analizar cuál es su utilidad. Posteriormente se profundizará en las principales criptomonedas que a continuación se presentan.

A) Criptomonedas de pago:

Las criptomonedas de pago, como su nombre indica, son aquellas diseñadas para facilitar transacciones financieras entre individuos o empresas sin la intervención de terceros como bancos o gobiernos, es decir, permiten "saltarse" al

intermediario gracias a su funcionamiento. A diferencia de las monedas fiduciarias, las criptomonedas de pago se basan en la tecnología blockchain, que garantiza la seguridad y la privacidad de las transacciones. Entre las criptomonedas de pago más populares se encuentran Bitcoin, Litecoin, Dash y Bitcoin Cash, entre otras. Estas criptomonedas se utilizan para comprar bienes y servicios en línea, y en algunos casos, también se aceptan como forma de pago en tiendas físicas (Newbery, 2021).

En general, estas criptomonedas de pago tienen una alta volatilidad en los mercados y su valor se ve afectado por varios factores, como la adopción y la regulación gubernamental. A pesar de esto, su uso sigue siendo cada vez más común en todo el mundo, especialmente en países con una infraestructura financiera deficiente o en situaciones donde la privacidad es una prioridad para los usuarios.

b) Criptomonedas de plataforma:

Las criptomonedas también se utilizan para financiar y desarrollar aplicaciones descentralizadas (dApps). Las dApps se construyen sobre las plataformas de blockchain y permiten a los desarrolladores crear aplicaciones que pueden ejecutarse sin la necesidad de un intermediario centralizado. Estas aplicaciones pueden abarcar una amplia variedad de industrias, como la banca, los seguros, el comercio electrónico y los juegos, entre otros. Para conseguir esto, además de blockchain se utilizan contratos inteligentes (smart contracts) para automatizar procesos y asegurar la integridad de los datos (Cai et al., 2018). Más adelante se profundizará en este aspecto, pues los smart contracts tienen una gran relevancia financiera.

El uso de criptomonedas en el desarrollo de dApps permite que los usuarios finales interactúen directamente con la aplicación sin tener que confiar en intermediarios o terceros. Los desarrolladores pueden crear tokens personalizados en la plataforma de blockchain para financiar sus proyectos y permitir que los usuarios accedan a los servicios de la aplicación. Los usuarios pueden comprar

estos tokens con criptomonedas y usarlos para pagar por servicios o productos dentro de la aplicación.

La creación de dApps con criptomonedas tiene varias ventajas, como señalan Cai et al. (2018) en su artículo. En primer lugar, el hecho de crear las aplicaciones de forma descentralizada y que no dependan de intermediarios permite la reducción de los costos y aumentar la transparencia. En segundo lugar, los tokens de la aplicación se pueden utilizar para financiar el desarrollo de la aplicación y permitir el acceso a los servicios de la misma. Esto, además de mejorar la accesibilidad a la aplicación, también permite a los desarrolladores crear más proyectos gracias al acceso a fondos directos de particulares que quieran colaborar. En tercer lugar, el uso de criptomonedas en la creación de dApps permite la creación de aplicaciones transfronterizas que pueden ser utilizadas por usuarios de todo el mundo sin la necesidad de conversiones de moneda.

Estas criptomonedas son, por tanto, atractivas para los desarrolladores debido a la flexibilidad y facilidad de uso que ofrecen. Las dApps pueden ser creadas utilizando un lenguaje de programación familiar, lo que reduce la barrera de entrada y acelera el proceso de desarrollo. Además, las criptomonedas de plataforma ofrecen una alta escalabilidad y seguridad, lo que las convierte en una opción popular para aplicaciones empresariales y gubernamentales.

Sin embargo, como con cualquier tecnología emergente, hay desafíos y riesgos asociados. Por ejemplo, la falta de regulación, la posibilidad de errores de codificación o las dApps creadas con intención de estafa pueden llevar a problemas de seguridad y pérdida de fondos (bitcoin.com, s.f.).

La criptomoneda por excelencia en la que se construyen un mayor número de dApps es Ethereum, a la cual se le dedicará su propio espacio más adelante en este trabajo, precisamente por la gran cantidad de aplicaciones y soluciones que se pueden crear en su red. También existen otros ejemplos, como Brave, que es un navegador web descentralizado que utiliza el token BAT, o Step App, que es una

aplicación de fitness que premia a los usuarios con su propio token como recompensa por realizar las distintas actividades físicas que ofrece.

c) Criptomonedas de privacidad

Las criptomonedas de privacidad tienen un enfoque distinto a las criptomonedas tradicionales, ya que se centran en proteger la identidad y la privacidad del usuario. A diferencia de otras criptomonedas, que utilizan un registro público de transacciones (como la blockchain de Bitcoin), las criptomonedas de privacidad utilizan técnicas de cifrado y anonimato para ocultar la información de los usuarios.

Hay que tener en cuenta que, aunque las criptomonedas son, en su base, bastante privadas y los datos personales en la blockchain están “camuflados” con códigos alfanuméricos, toda la información sobre transacciones y saldos es pública y de libre acceso. Cualquier persona podría consultar el saldo y el importe de una transferencia que realiza la persona A a la persona B, aunque sus identidades estén codificadas. Es aquí donde entra esta categoría de criptomonedas, tratando de dar un paso más allá en la privacidad de los usuarios.

Estas criptomonedas de privacidad funcionan a través de tecnologías específicas que permiten a los usuarios realizar transacciones anónimas e imposibles de rastrear, lo que las hace muy atractivas para aquellos que buscan proteger su privacidad en línea. El funcionamiento de estas criptomonedas se basa en diferentes algoritmos criptográficos, que en conjunto aseguran el anonimato del usuario.

Uno de los algoritmos más utilizados para este fin es el *Zero-Knowledge Proof*. Como muestran Sun et al. (2021) el algoritmo utilizado permite a los usuarios demostrar que poseen cierta información, pero sin tener que revelarla. Esto permite que los usuarios no tengan que mostrar información sobre su identidad o sus activos. Además, las criptomonedas de privacidad también utilizan la tecnología de mezclado de monedas, que permite a los usuarios diluir sus transacciones con las

de otros usuarios, dificultando aún más la identificación de la fuente de la transacción y, por tanto, su trazabilidad.

Por supuesto, tanto las criptomonedas de privacidad como el resto de las criptomonedas en general se enfrentan a fuertes críticas precisamente por esta excesiva “ocultación” de información. Una de las principales desventajas de las criptomonedas de privacidad es su posible uso para actividades ilícitas (Jansana, 2022). Debido a que la privacidad es una de las características principales de estas monedas digitales, los usuarios pueden realizar transacciones de forma anónima, lo que puede facilitar actividades delictivas como el lavado de dinero, el financiamiento del terrorismo o la compra de artículos ilegales como armas o sustancias estupefacientes.

Sin embargo, las criptomonedas no dejan de ser una tecnología más, y su potencial reside en el uso que se les dé. Este tipo de criptomonedas también tiene grandes aplicaciones en determinadas situaciones. Por ejemplo, pueden ser utilizadas para evitar la censura y la vigilancia gubernamental en países donde la libertad de expresión y el derecho a la privacidad son limitados o inexistentes. Al permitir que los usuarios realicen transacciones de forma anónima y sin restricciones gubernamentales, las criptomonedas de privacidad pueden ayudar a proteger los derechos y libertades de los ciudadanos, sobre todo si existen colectivos discriminados.

Está claro que el tema de la privacidad y la utilización indebida de las criptomonedas es muy controvertido y no está exento de polémica, por lo que se volverá a tratar más adelante en el caso particular de Bitcoin, pues se trata de la criptomoneda que más posibilidades tiene de ser adoptada masivamente.

d) Criptomonedas estables

Las criptomonedas estables, también conocidas como *stablecoins*, son un tipo de criptomoneda que se caracterizan por tener un valor estable, es decir, que su precio no fluctúa tanto como otras criptomonedas como Bitcoin o Ethereum.

Estas criptomonedas surgieron como una respuesta a la necesidad de estabilidad en el mercado de las criptomonedas. En su mayoría, estas monedas estables están diseñadas para mantener un valor equivalente a una moneda fiduciaria o a un activo subyacente como el oro o el petróleo.

Así pues, Ayuso y Conesa (2020) identifican 2 tipos de *stablecoins*, las colateralizadas y las que están respaldadas por algoritmos. Concretamente la estabilidad del precio de las *“stablecoins colateralizadas se debe al mantenimiento de una reserva de fondos o de activos que respalde las stablecoins en circulación”*. Las monedas estables más comunes están respaldadas con moneda fiduciaria como el euro o el dólar o con cualquier otro activo financiero o real.

En cuanto a las *stablecoins* basadas en algoritmos, estas consiguen la estabilidad mediante complejas operaciones y sistemas que permiten ajustar de forma dinámica la oferta de la moneda, creándola o destruyéndola para ajustarla a la demanda.

Las criptomonedas estables presentan una serie de ventajas importantes que las diferencian de las criptomonedas tradicionales. En primer lugar, la estabilidad de su valor las hace más atractivas como herramienta para el almacenamiento de valor y para realizar transacciones comerciales en comparación con las criptomonedas volátiles. Además, al tener una paridad con una moneda fiduciaria, como el dólar estadounidense o el euro, pueden ser utilizadas para transacciones internacionales sin la necesidad de tener una cuenta bancaria en el país de destino (Pascual, 2019)

Las criptomonedas estables también se están convirtiendo en una herramienta popular para realizar inversiones en el mercado criptográfico, ya que permiten a los operadores mover sus activos de una criptomoneda volátil a una criptomoneda estable para evitar las fluctuaciones del mercado. Esto puede proporcionar cierta estabilidad y protección contra la volatilidad, especialmente en momentos de incertidumbre económica o política.

El hecho de que una criptomoneda sea estable puede suponer, a priori, la solución a uno de los mayores problemas de las criptomonedas tradicionales. Lo que convertiría a estas criptomonedas en ideales para ser utilizadas como moneda alternativa y escapar o complementar a los sistemas financieros tradicionales. De hecho, las principales stablecoins consiguen mantener su paridad con el activo de referencia de una forma bastante eficaz. En el trabajo realizado por Sempere Tortosa (2022) se incluye un estudio de la paridad de las principales stablecoins que existen, concluyendo que, en general, éstas han mantenido su estabilidad de forma correcta.

Sin embargo, no se ha de olvidar que las mayores stablecoins son centralizadas, a diferencia de otros cripto-activos. Esto supone que las monedas estables están sujetas a la confianza de que el emisor de la moneda va a cumplir con su parte y mantendrá esa paridad necesaria. Se pierde así una de las propiedades que dan el atractivo a las criptomonedas, la descentralización y la no dependencia de terceros.

La quiebra del Silicon Valley Bank (SVB) en marzo de 2023 proporciona un ejemplo de cómo estas stablecoins pueden fallar. Este es el caso de USDC, una stablecoin emitida por Circle, y la segunda moneda estable más importante por capitalización de mercado. Con la caída del SVB, el emisor Circle comunicó que tenía exposición al banco, estando aproximadamente el 9% de los dólares con los que se respalda USDC en esta institución. Esto causó una venta masiva de la moneda en favor de otros activos financieros, lo que supuso que su valor se desplomara por debajo de los \$0.88 dólares, perdiendo así la paridad 1:1 con el dólar. Este efecto se contagió a otras monedas como Tether o DAI, la primera y cuarta stablecoins por capitalización de mercado, respectivamente.

Esto es una clara muestra de que, aunque las criptomonedas puedan representar un cambio en la utilización del dinero y las finanzas, no están exentas de riesgos e imperfecciones. De hecho, en el caso particular de las stablecoins, las imperfecciones vienen derivadas en su mayoría de los problemas que ya

presentaba el sistema financiero tradicional, como es la necesidad de un tercero de confianza que garantice un correcto funcionamiento de sus activos.

e) Criptomonedas de Utilidad

Las criptomonedas de utilidad, también conocidas como tokens de utilidad, son aquellas que se crean para ser utilizadas dentro de una plataforma o sistema específico. Estos tokens están diseñados para cumplir una función específica dentro de la plataforma, como el pago de tarifas de transacción, la adquisición de servicios o productos, el acceso a determinadas funcionalidades y otras funciones similares.

Los tokens suelen emitirse en grandes cantidades para asegurarse de que la plataforma tenga suficiente cantidad para cubrir todas las necesidades de los usuarios.

Entre las principales ventajas de las criptomonedas de utilidad destacan su capacidad para incentivar la adopción de la plataforma, ya que los usuarios necesitan adquirir tokens para poder utilizar sus servicios o productos. Además, su valor se basa en la utilidad que proporcionan dentro de la plataforma, lo que significa que pueden ser menos volátiles que otras criptomonedas. También suelen tener tarifas de transacción más bajas que otras criptomonedas, lo que las hace más atractivas para su uso en transacciones diarias.

Sin embargo, también tienen algunas limitaciones. Una de las principales es que su valor está estrechamente ligado al éxito de la plataforma para la que fueron creados, lo que significa que, si la plataforma no tiene éxito, el valor de los tokens de utilidad puede disminuir significativamente o incluso desaparecer. Además, su liquidez puede ser limitada en comparación con otras criptomonedas, lo que dificulta su compra o venta en algunos casos (Fornell, 2019)

En cuanto a los ejemplos de criptomonedas de utilidad, se pueden mencionar algunos como el token de utilidad de Binance (BNB), utilizado para pagar tarifas en la plataforma de intercambio de criptomonedas Binance, o el token de utilidad de

Augur (REP), utilizado para apostar en eventos en la plataforma de predicción Augur.

Es fácil confundir las criptomonedas de utilidad con las de plataforma, anteriormente descritas, pero existen diferencias fundamentales. La principal diferencia radica en su función y objetivo. Las criptomonedas de plataforma, como Ethereum, están diseñadas para proporcionar una plataforma de desarrollo para crear aplicaciones descentralizadas y contratos inteligentes. En cambio, las criptomonedas de utilidad, como Binance Coin (BNB), se utilizan para realizar transacciones dentro de una plataforma específica, como un exchange o una aplicación descentralizada.

Para comprenderlo de forma sencilla, podemos entender las criptomonedas de plataforma como la “tecnología” que permite el desarrollo de distintas aplicaciones descentralizadas y contratos inteligentes, mientras que los tokens de utilidad son las monedas específicas que se utilizan dentro de esas aplicaciones y permiten realizar pagos y transacciones dentro de un ecosistema específico. Además, las criptomonedas de utilidad a menudo ofrecen beneficios adicionales a los usuarios, como descuentos en las tarifas de transacción y acceso a servicios exclusivos en la plataforma.

4. Regulación de las Criptomonedas

La regulación de las criptomonedas es un tema que ha generado un gran debate a nivel global en los últimos años. A pesar de que estas monedas digitales se han vuelto cada vez más populares y utilizadas en distintas partes del mundo, aún existe una gran incertidumbre en cuanto a su estatus legal y la forma en que deben ser reguladas por los distintos gobiernos.

Por un lado, hay países que han adoptado una postura más favorable hacia las criptomonedas, permitiendo su uso y comercio con ciertas regulaciones, mientras que otros han optado por prohibir su utilización. Por otro lado, existen

países aún se encuentran en una fase de incertidumbre y están trabajando en la creación de marcos legales claros.

Entre las principales preocupaciones de los gobiernos y reguladores en relación con las criptomonedas se encuentra la lucha contra el fraude y sus problemas de estos activos como inversión, debido a su complejidad y falta de regulación. (CNMV y Banco de España, 2021)

Otro factor que influye en la regulación de las criptomonedas es el desconocimiento de la tecnología detrás de ellas por parte de los reguladores y legisladores. Esto ha llevado a la creación de normas a menudo inadecuadas o ineficientes, y a la necesidad de una mayor educación y comprensión sobre las criptomonedas y su potencial impacto económico y social.

No cabe duda de que, tanto la tecnología Blockchain en general como las criptomonedas en particular están cada vez más presentes en la sociedad y la economía globales. Esto requiere que los legisladores de todo el mundo pasen a la acción y proporcionen un marco jurídico que asegure una utilización correcta y ética de las criptomonedas al mismo tiempo que permitan desarrollar su tecnología sin asfixiar el potencial que tienen.

En esta parte del trabajo se va a analizar los enfoques que han adoptado los distintos países y sus gobiernos a la hora de regular las criptomonedas y las consecuencias que dichas regulaciones pueden tener en la adopción de esta tecnología.

4.1 Marco Europeo

Para poder analizar las regulaciones existentes en los países de la Unión Europea es necesario primero conocer las normas de carácter supranacional a la que estos países deben acogerse para desarrollar sus propias legislaciones.

MiFID 2

La primera gran legislación en la que se ven englobadas las criptomonedas es la directiva MiFID 2⁷ junto con el reglamento MiFIR⁸. La directiva MIFID 2, o la Directiva de Mercados de Instrumentos Financieros II, es una regulación que fue adoptada en 2018 y es la norma aplicable para los mercados financieros tradicionales. Su objetivo principal es proteger a los inversores y garantizar la integridad y transparencia de los mercados financieros en la UE. La regulación establece una serie de requisitos que los proveedores de servicios de inversión deben cumplir, como la necesidad de mantener registros detallados de transacciones, la divulgación de información completa y precisa a los clientes, y la evaluación continua de la aptitud y conveniencia de los productos ofrecidos a los clientes. En resumen, MIFID 2 tiene como objetivo mejorar la transparencia y la protección del inversor en los mercados financieros de la UE.

La principal forma en que las criptomonedas están sujetas a MIFID 2 es a través de los proveedores de servicios relacionados con cryptoactivos, como los exchanges. La directiva establece que cualquier entidad que proporcione servicios de inversión en la Unión Europea debe cumplir con ciertos requisitos de licencia, capitalización, supervisión y cumplimiento.

Además, los exchanges de criptomonedas que operan en la UE deben cumplir con los requisitos de MIFID 2 si ofrecen servicios de inversión en criptomonedas, como la compraventa de criptomonedas o la gestión de carteras de criptomonedas. Esto incluye el registro como una entidad de servicios de inversión, cumplir con los requisitos de capital mínimo, establecer políticas y procedimientos de cumplimiento, y someterse a la supervisión de la Autoridad Europea de Valores y Mercados (ESMA).

⁷ Council Directive 2014/65/EC of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU [2014] OJ L173/349.

⁸ Council Regulation (EC) 600/2014 on markets in financial instruments and amending Regulation OJ L648/2012.

Otra forma en que las criptomonedas están sujetas a MIFID 2 es a través de la regulación de los proveedores de servicios de pago, que también se aplican a los exchanges de criptomonedas. La directiva establece que cualquier proveedor de servicios de pago que opere en la UE debe cumplir con ciertos requisitos de licencia, seguridad, protección de datos y transparencia. Esto incluye la necesidad de someterse a la supervisión del regulador financiero de cada país.

MiCA

En el año 2019 *Facebook* anunció el lanzamiento de su stablecoin *Libra*, lo que supondría el primer lanzamiento de criptomoneda de una gran corporación en el mundo. Debido al impacto que esto podría suponer en la estabilidad financiera, la Unión Europea decidió a elaborar una regulación unificada, el Reglamento MiCA, que englobará a los países miembros. Hasta este momento ha existido una falta de regulación clara y coherente que ha llevado a la implementación de diferentes regulaciones en diferentes países, dificultando la seguridad jurídica y la adopción.

Según el comunicado de la Comisión Europea (2020), la regulación MICA, o el Marco Regulatorio de Mercados de Criptoactivos, es una propuesta de la que busca establecer un marco regulatorio claro y completo para el mercado de criptoactivos en la Unión Europea. El objetivo principal de MICA es garantizar la protección del consumidor y la integridad del mercado, al mismo tiempo que se fomenta la innovación y el crecimiento del sector de criptoactivos. El reglamento MiCA busca también proporcionar una definición clara de los criptoactivos, tratando de enmarcar a todos aquellos que se quedaban fuera de la MiFID 2.

Así pues, una de las características clave de MiCA es que establece una regulación para todas las criptomonedas, incluyendo tanto los criptoactivos que funcionan como medios de pago como aquellos que no lo hacen. Esto es importante porque muchos países ya tienen regulaciones para las criptomonedas que funcionan como medios de pago, como Bitcoin, pero no para otras criptomonedas. MiCA busca asegurarse de que todos estos activos estén regulados de manera coherente y uniforme en toda Europa.

Otra característica importante de MiCA es que establece requisitos claros para las empresas que operan en el mercado de las criptodivisas. Por ejemplo, MiCA establece requisitos para la información que las empresas de criptomonedas deben proporcionar a los inversores, así como para la protección de los fondos de los inversores. También establece normas para las empresas que ofrecen servicios de custodia de criptomonedas, como la necesidad de mantener los fondos de los clientes en cuentas segregadas.

MiCA también establece requisitos para las empresas que ofrecen servicios de intercambio de criptoactivos en cuanto a la identificación del cliente y la prevención del lavado de dinero.

Además, las empresas que ofrecen servicios de intercambio de criptomonedas deben cumplir con los requisitos de capital establecidos por MiCA, garantizando que las empresas tengan suficientes fondos para operar y proteger a los inversores en caso de problemas financieros.

MiCA también establece requisitos para las empresas que ofrecen servicios de asesoramiento en criptomonedas. Estas empresas deben cumplir con los requisitos de registro y divulgación establecidos por MiCA. Esto garantiza que los inversores reciban asesoramiento de empresas que cumplen con las normas europeas.

Además, MiCA establece un marco para la supervisión y el cumplimiento de las normas. Las autoridades de supervisión de los Estados miembros de la UE deben asegurar el cumplimiento de las normas establecidas por MiCA. Además, se establece un mecanismo de cooperación entre las autoridades de supervisión de diferentes países de la UE para garantizar una aplicación coherente de las normas. Se trata básicamente de asegurar la coordinación entre los estados miembros y la propia Unión Europea para los flujos de información.

Es importante tener en cuenta que MICA aún no ha sido adoptada oficialmente y está sujeta a cambios y revisiones. Se espera que la regulación se

implemente de manera gradual en los próximos años, lo que permitirá a las empresas adaptarse a los nuevos requisitos y procesos hasta su completa entrada en vigor en 2024.

Limitaciones de MiCA

Aunque la implementación de MiCA es un paso importante para la regulación de las criptomonedas en Europa existen ciertos aspectos con margen de mejora dentro de la norma.

Como señala Gabilondo García (2021) en su trabajo, el Reglamento MiCA falla en uno de sus principales objetivos, definir correctamente los distintos criptoactivos. Los conceptos tratados en la norma quedan definidos de una forma excesivamente amplia y poco precisa, lo que supone un serio problema a la hora de que los distintos estados puedan legislar en base a MiCA. Esto generará una preocupante disparidad conceptual y de aplicación normativa en los distintos países en función de cuál sea su interpretación del reglamento. Es una situación similar a la ya existente y que el Reglamento MiCA no consigue resolver.

Por su parte, Van der Linden y Shirazi (2023) muestran algunas otras limitaciones de la norma, destacando como importante ciertos requisitos excesivamente estrictos que se proponen. La rigidez de alguno de los aspectos regulados en el MiCA podría suponer un desincentivo y severas limitaciones a ciertos proyectos criptográficos, sobre todo los de carácter descentralizado, ya que estos no están situados en un lugar geográfico concreto, lo que supone un vacío total en la aplicación o no de la norma.

Otro de los aspectos más controvertidos es la alta demanda de información que será requerida a las empresas de criptomonedas, sobre todo en cuanto a sus usuarios. No se ha de olvidar que una de las principales razones de ser de las criptomonedas es su descentralización y su privacidad, lo que choca frontalmente con los requerimientos de información y control que se espera obtener con esta norma.

Todos estos aspectos regulatorios podrían desincentivar en gran medida la adopción de las criptomonedas por parte de los usuarios y la adopción de proyectos futuros por parte de compañías o de pequeños emprendedores. Como se verá a continuación, los distintos países han decidido adoptar una gran variedad de enfoques en sus regulaciones, donde algunos apuestan fuertemente por una nueva tecnología y donde otros ven en esta un cambio que puede ser peligroso y que se debe limitar y controlar.

4.2 Enfoques en la regulación de los criptoactivos

La propuesta de reglamento MiCA, anteriormente comentado, deja entrever el gran número de variables a tener en cuenta para regular de forma mínimamente eficiente un conjunto de tecnologías tan novedosas. Los países deben atender aspectos que afectan tanto a particulares, como son las ganancias y pérdidas patrimoniales o las transacciones y cambios de valor, como aspectos que regulan a las propias empresas dedicadas al sector, que además variarán en función de la actividad.

Lo que es cierto es que las criptomonedas deben gran parte de su auge a la especulación en los mercados, por lo que uno de los primeros focos de atención en cuanto a la regulación suele ser la política impositiva respecto a las ganancias que generen las inversiones en criptomonedas. Aunque la inversión especulativa puede no ser el aspecto más interesante o relevante del potencial de las criptomonedas, la presión impositiva a la que se someten sí tiene una gran importancia a la hora de incentivar la adopción de los usuarios o la inversión en nuevos proyectos tecnológicos.

En general, los países han optado por gravar los beneficios derivados de las criptomonedas de acuerdo con sus regulaciones ya existentes para otros tipos de inversiones, es decir, incluyéndose en sus respectivos impuestos sobre rendimientos del capital.

Sin embargo, esta es una visión bastante limitada, ya que no todas las criptomonedas tienen las mismas características o naturaleza. Se trata de un problema similar al que se apreciaba con el reglamento MiCA, al no tener claro como clasificar estos activos se hace muy difícil regularlos y se meten todos en el mismo saco.

Una analogía similar la podemos encontrar cuando surgieron los primeros coches a motor en las carreteras. Anteriormente solo circulaban caballos y carruajes por las vías públicas, pero cuando los coches comenzaron a utilizarse no existía un reglamento que regulara este tipo de vehículos. La primera solución de los legisladores fue incluir cierta normativa para los coches a motor en la misma norma que regulaba los caballos y carruajes. Esto obviamente no funcionó muy bien, ya que la naturaleza de los coches a motor era distinta y no se le puede aplicar una misma legislación (Kendus, 2017).

Ahora bien, como se ha mencionado, regular los beneficios generados por las criptomonedas no es el único reto al que se enfrentan los países. Existe un sinfín de casuísticas derivadas de la utilización de la tecnología Blockchain y las criptomonedas que requieren atención. Ante esta situación los distintos gobiernos de todo el mundo han optado por enfoques muy distintos a la hora de regular las criptomonedas. A continuación, se mostrarán algunos casos concretos de regulaciones y posturas adoptadas por los países para tratar esta situación.

4.2.1 Caso de España

En el trabajo realizado por Pascual Cerdá (2022) se realiza un análisis del marco jurídico de las criptomonedas en distintos ámbitos, centrándose en el territorio nacional. En el texto se expone que la legislación española **no dispone** de una regulación específica para las criptomonedas, y que toda la normativa existente está basada en documentos sin rango normativo.

Ha sido la Hacienda española la que ha ido dando forma al marco de las criptomonedas mediante resoluciones y consultas vinculantes, tratando de

adaptarlas a la normativa ya existente. Sin embargo, la autora señala que las directrices proporcionadas son, en muchos casos, insuficientes o contradictorias.

En España, desde una perspectiva legal, la naturaleza jurídica de las criptomonedas se presenta heterogénea e incierta, combinando características de varios activos, complicando así su clasificación. Esto se traduce en una gran dificultad para establecer normativa legal y tributaria.

Sin embargo, el hecho de que no exista una regulación expresa no exime a los contribuyentes de sus obligaciones tributarias. Los intercambios de criptomonedas son tratados, a efectos fiscales, como cualquier otro activo, por lo que se deben declarar y tributar en el IRPF en caso de personas físicas y en el Impuesto de Sociedades en caso de personas jurídicas. Del mismo modo, si se alcanzan ciertos umbrales, también serán objeto del Impuesto sobre el Patrimonio.

Sin embargo, debido a la incertidumbre generada por la falta de regulación y definición claras, se dificulta mucho la tarea de declarar unos activos tan nuevos. La naturaleza descentralizada y global de las criptomonedas hace que la recopilación de la información tributaria sea muy compleja. Esto pone en aprietos a los usuarios que reciben requerimientos por parte de Hacienda, y del mismo modo dificulta la tarea de control que la Dirección General de Tributos (DGT) realiza sobre las obligaciones impositivas.

En 2022 la hacienda española introdujo un modelo informativo, el 720, en el que se obligaba a declarar las criptomonedas que se tuvieran en el extranjero si superaban un valor de 50.000€. Sin embargo, la propia jurisprudencia europea declaró dicho modelo “contrario a derecho” debido a las desproporcionadas sanciones que se imponían. Ahora la Hacienda española prepara el nuevo modelo 721, con las mismas obligaciones, pero con sanciones modificadas.

Sin embargo, el propio concepto de tener criptomonedas “en el extranjero” es totalmente ambiguo. La naturaleza descentralizada de estos activos hace que no se pueda identificar su situación geográfica. Las criptomonedas no son más que

apuntes contables registrados en la Blockchain, pero los saldos no se encuentran en ningún lugar, sino en la propia “red Blockchain”.

Este no es más que otro ejemplo de la complejidad a la que se enfrentan los reguladores ante esta nueva situación, lo que está generando un clima de inseguridad jurídica que trae consigo consecuencias negativas. Por una parte, los legisladores se enfrentan al reto de crear una normativa sobre una tecnología que desconocen, lo cual puede ser altamente ineficaz. Por otra parte, esta inseguridad jurídica está frenando la adopción de una tecnología con un gran potencial. Incluso si un contribuyente quisiera cumplir con todas sus obligaciones, se encontraría en una situación de desconocimiento, ya que ni siquiera la propia normativa aclara los procedimientos a seguir.

5. Viabilidad de las criptomonedas en la economía y las finanzas.

La trayectoria que han llevado las criptomonedas desde su nacimiento en 2008 ha sido estelar. Decenas de miles de criptomonedas se han creado en este tiempo y muchas de ellas ya han dejado de existir. Esto pone de manifiesto la etapa tan incipiente en la que se encuentra esta tecnología. Mientras que algunas criptomonedas tienen objetivos muy concretos y realizan bien su función, otras están destinadas a ser proyectos que fracasarán al no aportar ningún valor a la sociedad o la economía.

Sin embargo, en el corto tiempo de existencia de esta tecnología ya se han identificado criptomonedas que pueden aportar un gran valor añadido al mundo en el que vivimos. Expertos en diferentes campos como la economía, la ingeniería, la banca o la política son capaces de reconocer el potencial de algunos de estos activos.

En este apartado se va a realizar un análisis de las principales criptomonedas existentes, de su funcionamiento y utilidades y de cuáles son las posibilidades de

implantación que tienen en sus respectivos campos de acción como la economía, las finanzas y la sociedad.

5.1 Bitcoin

En 2008 se creó Bitcoin, la primera criptomoneda del mundo, cuando Nakamoto (2008) escribió su White Paper. Desde entonces se ha convertido en la criptomoneda más conocida y popular en la actualidad, y se utiliza como medio de intercambio (funciona bastante bien para realizar transacciones entre dos personas o entidades de forma casi instantánea y a coste reducido) y almacenamiento de valor digital descentralizado. Los defensores más firmes de Bitcoin consideran que está destinado a ser el “Oro 2.0”, es decir, una reserva de valor que permita almacenar la riqueza sin depender de los gobiernos y que además sea inconfiscable.

Nakamoto propone un sistema de pagos que no dependa de un intermediario financiero, puesto que para él esto supone ineficiencias monetarias y costes asociados. Esto lleva a la principal característica de Bitcoin, la descentralización, lo que significa que no está controlada por ningún gobierno, entidad financiera o corporación. En lugar de ello, las transacciones de Bitcoin son verificadas por una red descentralizada de nodos que utilizan la tecnología Blockchain.

Bitcoin se ha convertido en una opción atractiva para muchas personas debido a su seguridad, privacidad y su capacidad de ser utilizada en cualquier parte del mundo. Aunque también tiene sus críticos y escépticos.

En este apartado se analizará cual es el funcionamiento de Bitcoin, cuáles son los distintos usos reales que se le pueden dar, y cuáles son las posibilidades de ser implantado en el sistema monetario y financiero actual, teniendo en cuenta sus repercusiones.

5.1.1 Funcionamiento de Bitcoin

Bitcoin es una criptomoneda que se basa, como el resto de criptomonedas, en la tecnología Blockchain, la cual permite la realización de transacciones seguras y transparentes en una red descentralizada. El objetivo principal de Satoshi Nakamoto al crear Bitcoin fue proporcionar una forma segura y descentralizada de realizar transacciones financieras sin la necesidad de intermediarios. Nakamoto también buscaba resolver el inconveniente del **doblo gasto**, el cual ha sido un problema común en la historia de las transacciones digitales.

El doble gasto es la situación que se da cuando un usuario intenta gastar una misma unidad monetaria en más de una transacción o en la misma transacción. Sería como intentar pagar algo que cuesta 10€ utilizando dos veces el mismo billete de 5€. En el dinero físico es fácil controlar que un billete no es el mismo que otro, pero en transacciones digitales este control se complica. En las transacciones digitales tradicionales suelen ser los bancos los que garantizan que los apuntes contables que se realizan son correctos, y los usuarios confían en ello.

Este problema ha sido una barrera para la creación de monedas digitales, ya que se necesita encontrar una forma de prevenir este tipo de fraude. Los sistemas tradicionales de pagos digitales, como las tarjetas de crédito, confían en intermediarios centralizados para prevenir el doble gasto. Sin embargo, en un sistema descentralizado como Bitcoin, donde no hay intermediarios, es necesario encontrar una solución diferente.

Con Bitcoin, el problema del doble gasto se soluciona con la Blockchain, donde todas las transacciones se registran en bloques y luego se enlazan unos con otros en una cadena. Como la información de la cadena es verificable por todos los usuarios

Para que una transacción sea validada y confirmada en la blockchain, necesita ser aprobada por la mayoría de los nodos en la red. Una vez que se confirma una transacción, se registra en la blockchain y se considera irreversible.

Este consenso entre la mayoría de usuarios es lo que da su seguridad a la red. En lugar de delegar la verificación en un intermediario de confianza, se verifica por mayoría de participantes, asegurando así que nadie esté abusando de ese doble gasto. De este modo, si se quisiera introducir un dato erróneo en la red, este solo podría registrarse si el 51% de los usuarios lo validaran, lo cual es prácticamente imposible, y cada vez más difícil conforme aumenta el número de participantes de la red de Bitcoin.

Además, la tecnología blockchain en Bitcoin también permite la creación de nuevas monedas (nuevos bitcoin) mediante un proceso llamado minería. Los mineros son usuarios de la red que utilizan su poder de procesamiento para resolver complejos rompecabezas matemáticos y validar transacciones en la blockchain. A cambio de su trabajo, los mineros reciben una recompensa en forma de nuevas monedas de Bitcoin. Es precisamente este incentivo el que garantiza que las transacciones serán correctas, ya que el proceso para resolver el problema matemático consume muchos recursos, y un validador no se arriesgaría a que su transacción fuese errónea.

5.1.2 Bitcoin: Divisa o Reserva de valor

Matos (2008) señala que, tanto Bitcoin como las criptomonedas en general, pueden funcionar como una divisa o como una *commodity*, y destaca la necesidad de preguntarse cuál de estas formas será la considerada por reguladores y gobiernos. Esto nos lleva de nuevo a la controversia con las normativas sobre criptomonedas, ya que es difícil determinar cuál es su naturaleza.

Para el propósito de este TFG, se revisará el Bitcoin como posible divisa, su capacidad para funcionar como dinero, y para ello se pasa a analizar las funciones. Concretamente:

Función 1: Medio de cambio

Esta fue la principal función para la que Bitcoin fue creado, ser un medio de pago descentralizado. La primera transacción para adquirir bienes realizada con

Bitcoin se produjo el 22 de mayo de 2010, cuando se adquirieron dos pizzas familiares por un total de 10.000 bitcoin, lo que por aquel entonces equivalía a unos \$41 (Leal, 2023). A día 13 de mayo de 2023, con un Bitcoin cotizando a \$26.800 el valor de esos 10.000 bitcoin ascendería a unos 268 millones de dólares.

Cada vez son más los comercios que permiten los pagos con Bitcoin u otras criptomonedas en sus establecimientos, sobre todo en tiendas online, debido a la naturaleza digital de esta moneda. Microsoft o Starbucks ya aceptan el pago de sus servicios con Bitcoin, y plataformas de pago como Paypal y Mastercard permiten a sus clientes pagar en cualquier lugar del mundo con Bitcoin y otras criptomonedas. Además, gracias a estas plataformas, la cantidad de Bitcoin que se utiliza en cada transacción se ajusta al precio que la criptomoneda tiene en el mercado en ese momento y se adapta al precio del producto adquirido. De esta forma se solucione en gran medida el problema de la volatilidad de precios.

Sin embargo, el hecho de utilizar plataformas de pago intermediarias para pagar con Bitcoin supone un choque frontal con la filosofía con la que se creó, ya que al tener que utilizar un intermediario de pago se pierde la descentralización con la que fue creado Bitcoin. A pesar de esto, es indudable que la aceptación y utilización por parte de grandes empresas está ayudando a que la adopción de Bitcoin se acelere día a día.

Función 2: Unidad de Cuenta

El dinero cumple la función de unidad de cuenta cuando es aceptado comúnmente para medir el valor de bienes y servicios de una economía. Aquí se presenta un gran problema para Bitcoin, ya que su utilización no responde a la economía de un solo país con su propia moneda, sino que se trata de una tecnología global. Bajo esta premisa, se hace prácticamente imposible que el mundo entero utilice una única moneda para medir el valor de sus bienes. Para ello la adopción de Bitcoin debería ser totalmente masiva y a una escala global.

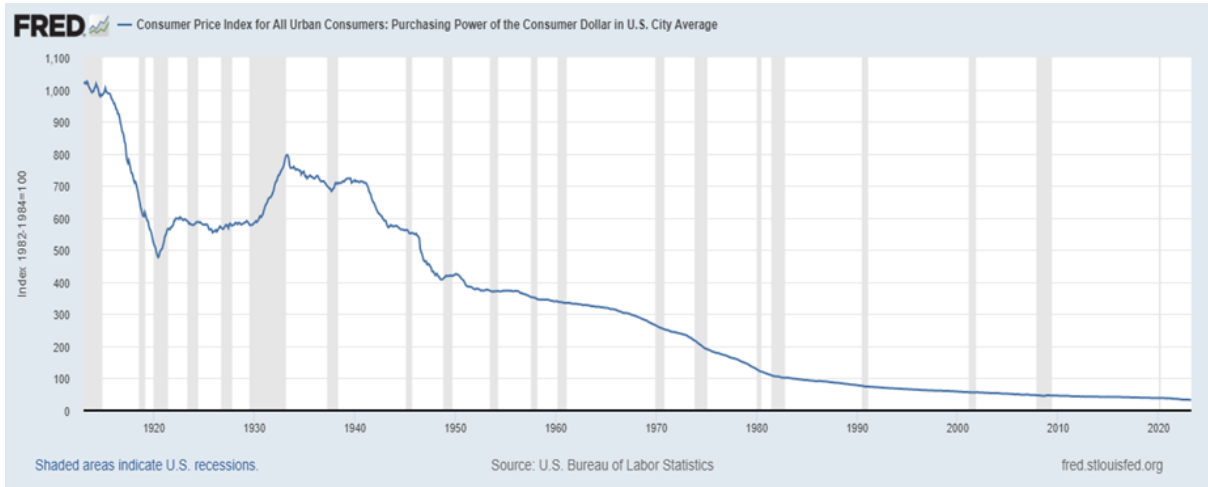
Sin embargo, sí es factible que bitcoin pueda llegar a ser una unidad de cuenta alternativa y complementaria a las monedas de cada país, unificando de alguna forma los tipos de cambio de las distintas divisas de un modo similar al que lo hacen el dólar o el euro, siendo monedas de referencia internacional. Dado que Bitcoin no está ligado a ningún gobierno o país, podría llegar a convertirse en un estándar global que no estuviera sometido a los intereses de los distintos gobiernos, generando una confianza intrínseca para todos los países que lo quisieran utilizar. Aun así, a día de hoy Bitcoin no actúa como una unidad de cuenta eficiente, sobre todo debido a su volatilidad de precio y a una necesidad de mayor adopción.

Función 3: Reserva de Valor

Si existe un activo por excelencia considerado reserva de valor es el oro. Cualquier persona o gobierno que ha querido mantener su capacidad adquisitiva a lo largo del tiempo, sobre todo en situaciones de dificultad económica, ha recurrido al oro en un intento de reducir las fluctuaciones y la incertidumbre de la economía global.

Otro de los activos considerados reserva de valor es el dólar estadounidense, la moneda fiduciaria más extendida actualmente, pero ¿funciona realmente esta divisa como reserva de valor? En el Figura 4 se muestra la capacidad de compra del dólar estadounidense tomando como base (100) una cesta de la compra en 1984. Se puede observar cómo el poder adquisitivo del dólar se ha reducido casi un 97% en los últimos cien años, lo que significa que la cantidad de artículos que se podía comprar con un dólar en 1913 era muy superior a la que se puede adquirir en 2023.

Figura 4: Poder adquisitivo del dólar estadounidense.



Fuente: Reserva federal de St. Louis⁹

El mal rendimiento del dólar como reserva de valor puede deberse a la ausencia de una característica que sí tiene el oro y que comparte con Bitcoin: la escasez. El hecho de que exista una cantidad máxima y limitada de oro en el mundo es uno de los factores clave para que este no haya perdido su poder adquisitivo a lo largo de la historia.

Bitcoin, debido a su programación interna, también tiene una cantidad limitada de monedas existentes. La cantidad máxima de bitcoins que existirá será de 21 millones. Además Bitcoin está diseñado para que la cantidad de monedas que se pueda crear se reduzca a la mitad cada cuatro años, en un proceso denominado "*halving*". De esta forma, bitcoin se presenta también como una moneda deflacionaria.

Esta escasez y deflacionabilidad, combinada con la seguridad que ofrece la tecnología blockchain, ha llevado a muchos a creer que Bitcoin es un buen activo de reserva de valor. Además, Bitcoin es resistente a la censura y no está sujeto a la política monetaria de ningún gobierno.

⁹ Gráfico obtenido de <https://fred.stlouisfed.org/series/CUUR0000SA0R>

Sin embargo, también hay limitaciones en cuanto a la capacidad de Bitcoin para funcionar como reserva de valor. Aunque la cantidad total de bitcoins es limitada, la oferta de otros criptoactivos es infinita, lo que significa que la competencia es constante y la oferta total de activos digitales puede ser muy grande.

Además, un gran inconveniente es el precio de Bitcoin, que ha demostrado ser muy volátil, lo que significa que la gente puede tener dificultades para confiar en ella como un medio de almacenamiento de valor confiable.

Otra limitación es que Bitcoin todavía se considera una tecnología relativamente nueva y puede haber dudas sobre su sostenibilidad a largo plazo. Mientras que el oro viene funcionando como reserva de valor durante miles de años, la vida de bitcoin apenas alcanza los quince años, por lo que todavía tiene un largo camino antes de demostrar su eficacia.

Propiedades del dinero en Bitcoin

La primera propiedad del dinero que se trató en este texto fue la durabilidad, como capacidad para resistir el desgaste y el paso del tiempo. En el caso de Bitcoin, su durabilidad se basa en su tecnología subyacente, la blockchain, que proporciona un registro inmutable de todas las transacciones que se han realizado en la red.

Otra de las propiedades del dinero es la portabilidad. Como dinero digital, bitcoin es altamente transportable. Cualquier usuario puede acceder a sus bitcoins desde su teléfono móvil o almacenarlo de una forma segura en las denominadas "wallet". Estos aparatos con aspecto de memoria USB no son más que unos dispositivos físicos que permiten al usuario acceder a sus fondos de criptomonedas desde cualquier lugar del mundo con conexión a internet.

En cuanto a la divisibilidad y uniformidad de Bitcoin, cada unidad de esta moneda es divisible en 100 millones de partes de igual valor, como si de céntimos de un euro se tratara. Cada una de estas partes más pequeñas se llama "satoshi", en honor al creador de Bitcoin, Satoshi Nakamoto. De esta forma, cada bitcoin se

puede dividir en 100.000.000 satoshis. Esta gran divisibilidad permite, como en otras divisas, realizar transacciones de cuantías grandes y pequeñas.

Otra propiedad a tener en cuenta es la escasez. Como ya se ha mencionado, Bitcoin tiene una limitación de producción de 21 millones de bitcoin, y nunca existirá más de esa cantidad. De hecho, en este aspecto concreto bitcoin supera con creces al dinero fiduciario actual, cuya oferta es totalmente dependiente de la política monetaria de los distintos países.

Finalmente, en cuanto a la aceptabilidad, este es el gran punto débil de Bitcoin por el momento. No cabe duda de que, para poder usar un activo como dinero, este debe ser ampliamente aceptado por la gente. Aunque Bitcoin ha incrementado el número de usuarios desde su creación, su utilización ha estado por el momento ampliamente ligado a la especulación. Ya se ha visto como el número de empresas que aceptan o utilizan Bitcoin también está en aumento, y esto hará que los usuarios vayan percibiendo esta moneda digital como un posible medio de pago efectivo (nos encontramos ante la pescadilla que se muerde la cola).

Además, como se vio en el apartado de regulación, la postura que tomen los distintos gobiernos respecto a las criptomonedas puede frenar o incentivar en gran medida la utilización de Bitcoin. No muchas personas se aventuran a adoptar una tecnología cuando el gobierno de su país no otorga seguridad jurídica o incluso prohíbe su utilización.

Reflexión

Así pues, tras haber analizado las distintas funciones y propiedades del dinero desde el punto de vista de Bitcoin podemos extraer las siguientes conclusiones:

Bitcoin funciona correctamente como medio de cambio, ya que este es su diseño y objetivo principal, permitiendo adquirir bienes y servicios. Además, no necesita de intermediarios financieros, lo que hace que pueda ser utilizado en

cualquier lugar del mundo con conexión a internet, sin las limitaciones de realizar cambios de divisa.

Aunque Bitcoin puede actuar sin problema como unidad de cuenta, su volatilidad de precios hace que por el momento no sea muy práctico medir y expresar el valor de los bienes en bitcoin.

En cuanto a su función como reserva de valor, Bitcoin presenta características que superan al dinero fiduciario actual, como la oferta limitada, el hecho de ser un activo deflacionario y la imposibilidad de los gobiernos para establecer la oferta monetaria. Sin embargo, la volatilidad del precio de bitcoin vuelve a opacar sus características positivas. Se hace imposible utilizar un activo como reserva de valor si el precio de dicho activo en el mercado puede reducirse en pocos meses un 50% o incrementarse en un 200%, por poner un ejemplo.

Bitcoin cumple con creces las propiedades del dinero de durabilidad, portabilidad, divisibilidad, uniformidad y escasez.

El gran lastre para que Bitcoin pudiera utilizarse como un medio de pago generalizado o como una reserva de valor es su aceptabilidad. La adopción masiva de bitcoin ayudaría a reducir algunos de sus grandes problemas como la volatilidad de precios, lo que a su vez generaría una mayor confianza y por tanto una mayor adopción. Se crea así un ciclo que también funciona de forma negativa, a mayor volatilidad mayor desconfianza y menor aceptación. Este es el gran problema por derivado de que Bitcoin funcione de forma descentralizada y sin una autoridad intermediaria. El hecho de no depender de gobiernos o grandes corporaciones de confianza es a la vez su fortaleza y su debilidad.

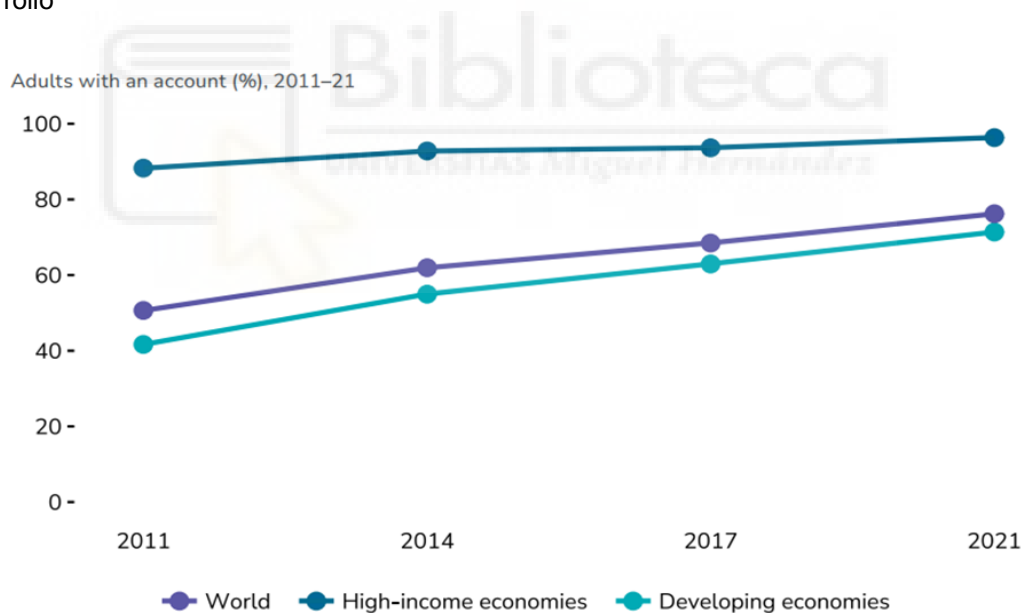
5.1.3 Otras implicaciones de la adopción de Bitcoin

Según el informe "*The Global Findex*" del Banco Mundial (2021), casi el 30% de los adultos de los países en desarrollo no poseen una cuenta bancaria (Figura 5), destacando con cifras aún más bajas los países de Latinoamérica y asiáticos. Antes de la COVID-19 estas cifras eran mucho más preocupantes, pero debido al

aislamiento de la pandemia muchas personas se vieron obligadas a usar servicios bancarios digitales, aun cuando sigue habiendo una gran numero de lugares donde el acceso a servicios financieros es muy complicado o está altamente restringido.

El Bitcoin podría jugar un papel relevante en este aspecto al brindar servicios financieros a personas que no tienen acceso a sistemas bancarios tradicionales, ya que las personas pueden almacenar y transferir valor de forma segura y económica utilizando solo un teléfono inteligente y conexión a Internet (sin necesidad de una institución financiera intermediaria). En esta línea Kim & Ryu (2022), llegan a la conclusión de que las personas sin bancarizar encuentran un activo valioso en las criptomonedas para realizar pagos y transferencias, aun cuando la adopción de estas sea parcial.

Figura 5: Porcentaje de adultos bancarizados en economías de altos ingresos y economías en desarrollo



Fuente: Recuperado de los datos de Global Findex Database (Banco Mundial, 2021)

Otro ejemplo de utilidad de Bitcoin lo encontramos en países que sufren hiperinflación. En esta situación los ciudadanos ven mermar sus ahorros de una forma acelerada. Datos de abril de 2023 indican que países como Venezuela o Argentina tienen inflaciones superiores al 100% (Datosmacro.com, 2023). En estos

casos podría ser tentador para la población adquirir activos refugio como el oro o incluso dólares estadounidenses para mantener su riqueza. Sin embargo, en países con unos sistemas financieros deficientes se hace difícil acceder a estos activos reales. La descentralización de bitcoin y su formato digital podría facilitar el acceso a un activo que permita mantener los ahorros de los ciudadanos, incluso transportarlos fácilmente a otros países para resguardarlos.

Del mismo modo, la característica de la privacidad de Bitcoin y otras criptomonedas puede ayudar a superar brechas de desigualdad por razón de género, raza, religión, orientación sexual o cualquier otro motivo de discriminación. La filosofía con la que Bitcoin fue creada es el acceso universal de un medio de pago que ninguna persona o institución pueda censurar. Algunas compañías de criptomonedas como la mexicana Bitso son muy conscientes de ello, y llevan tiempo promoviendo proyectos, junto con otras empresas como Mastercard, para la educación financiera y utilización de criptomonedas, sobre todo para superar obstáculos de desbancarización y desigualdad de género en Latinoamérica.

5.2 Ethereum

Ethereum es una criptomoneda y plataforma blockchain creada en 2015 por el desarrollador Vitalik Buterin, que permite a los desarrolladores construir y desplegar las ya mencionadas dApps en su blockchain. A diferencia de Bitcoin, la utilidad de Ethereum no es tanto actuar como una divisa o reserva de valor, sino democratizar y descentralizar el poder económico y tecnológico, brindando a individuos y organizaciones una plataforma transparente y sin intermediarios para llevar a cabo transacciones y acuerdos seguros (visión de Buterin).

Una de las características más destacadas de Ethereum es su capacidad para ejecutar contratos inteligentes. Esto ha permitido a Ethereum ser pionero e impulsar las finanzas descentralizadas (DeFi), un sector en auge que abarca una variedad de aplicaciones y servicios financieros construidos sobre su plataforma.

Otra área en la que Ethereum ha dejado una marca significativa es en el campo de los tokens no fungibles (NFTs). Estos tokens únicos e indivisibles permiten la representación de activos digitales como obras de arte, coleccionables y bienes virtuales. Sin embargo, esta rama de utilidad tiene, de momento, menores implicaciones financieras.

En cuanto a su funcionamiento, Ethereum no deja de ser una criptomoneda que utiliza su propia Blockchain, por lo que la forma de registrar la información es similar a la de Bitcoin o la de cualquier otra criptomoneda. Sin embargo, mientras que en Bitcoin la información contenida suelen ser transacciones monetarias, en Ethereum se puede transmitir información altamente programable en su propio código de programación (Solidity). Esto es lo que permite a la creación de una infinidad de aplicaciones y proyectos descentralizados.

A continuación, se presentarán algunas de las aplicaciones de Ethereum más importantes y que pueden tener una mayor utilidad en los sistemas financieros actuales.

5.2.1 Protocolos DeFi en Ethereum y utilidades.

En el ecosistema de Ethereum, las plataformas de préstamos descentralizados han ganado un gran impulso y se han convertido en una de las aplicaciones financieras más populares. Las plataformas DeFi de préstamos basadas en contratos inteligentes en Ethereum han transformado la forma en que las personas obtienen y otorgan préstamos al eliminar intermediarios y permitir transacciones directas entre los participantes. Estas plataformas utilizan los contratos inteligentes para automatizar y asegurar todo el proceso de financiero. Algunas de las aplicaciones más conocidas son “MakerDAO” o “Aave”, con las que se obtienen préstamos en forma de diversas criptomonedas con las que después se puede operar.

En estas plataformas, los usuarios depositan sus activos digitales en un contrato inteligente designado como garantía para el préstamo. Estos activos se mantienen en custodia y se utilizan como respaldo en caso de incumplimiento de

las condiciones. A continuación, el contrato inteligente evalúa el valor de la garantía depositada y establece un límite de préstamo, es decir, la cantidad máxima que el usuario puede pedir prestado en relación con el valor de su garantía.

El préstamo se otorga automáticamente por el contrato inteligente sin necesidad de aprobación manual ni verificación crediticia, ya que la garantía respalda la transacción.

Los propios contratos inteligentes realizan el seguimiento de los pagos de principal, intereses y demás obligaciones contractuales. Si un prestatario incumple con los pagos o el valor de la garantía cae por debajo de un umbral específico debido a la volatilidad del mercado, el contrato inteligente puede activar automáticamente la liquidación de la garantía. En este caso, la garantía se vende o subasta para recuperar los fondos prestados.

Es indudable que esto supone un gran cambio en el sistema financiero tradicional. Los bancos son intermediarios que ofrecen servicios financieros a distintos entes, y uno de sus negocios más rentables es la concesión de préstamos. Con los nuevos sistemas de finanzas descentralizadas la posición de los bancos puede verse amenazada al verse desplazado el volumen de negocio hacia otras alternativas financieras.

En la Figura 6, se puede ver como en la actualidad existen más de 14 mil millones de dólares bloqueados en servicios DeFi de préstamos, sin embargo, esta cifra llegó a su máximo en la primera mitad de 2022, alcanzando los 51 mil millones de dólares.

Figura 6: Dólares bloqueados en protocolos DeFi de préstamos



Fuente: DefiLlama¹⁰

Pero los préstamos no es el único servicio ofrecido por las finanzas descentralizadas. Existen plataformas de aseguradoras, intercambio de divisas, fondos de inversión o custodia de valores, entre otros. Todos ellos son servicios que ha venido ofreciendo el sistema financiero tradicional y que en la actualidad están en pleno proceso de cambio.

Si bien es cierto que un intermediario financiero con renombre puede dar seguridad a los servicios que ofrece, el uso de contratos inteligentes trata de evitar que los usuarios tengan que “confiar” en una institución que supervise las operaciones, ya que estas están codificadas mediante algoritmos matemáticos, que son inmutables, y por tanto, no requieren confianza.

Por supuesto, los contratos inteligentes no están exentos de riesgos. Se ha de tener en cuenta que todos estos protocolos, al igual que las criptomonedas, son una tecnología incipiente. Hasta la fecha se han producido multitud de fallos de seguridad, como hackeos, errores en los códigos de los contratos o estafas creadas expresamente bajo estos protocolos para quedarse con los fondos de los usuarios.

¹⁰ Gráfico obtenido de <https://defillama.com/categories>

Del mismo modo que las finanzas tradicionales llevan siglos perfeccionándose a base de catástrofes y correcciones, Ethereum y los protocolos Defi necesitarán su propio periodo de maduración para llegar a consolidarse como una opción financiera que no despierte dudas en los usuarios. Igual que en el auge las “punto com”, la mayoría de los proyectos fracasarán, pero unos pocos podrían quedarse como líderes en el sector y revolucionar las finanzas, como Internet revolucionó la vida de las personas en su día.

Conclusiones

La Blockchain, gracias a sus características de privacidad, seguridad y descentralización, permite la construcción de un gran número de tecnologías subyacentes con una gran variedad de utilidades en distintos campos.

Dentro del ámbito de las finanzas, las aplicaciones más importantes de la Blockchain son la creación de criptomonedas y de *Smart Contracts* o contratos inteligentes. Sin embargo, las aplicaciones que puede tener para mejorar los procesos de las cadenas de suministro o para verificar la propiedad o identidad de los usuarios son cada vez más reconocidas y empleadas por empresas y por el público en general.

Sin embargo, el aspecto regulatorio de las criptomonedas es uno de los obstáculos más grandes a salvar para que esta tecnología se pueda adoptar y para que proyectos con valor agregado vean la luz en el futuro.

En España no existe una regulación específica para las criptomonedas, y toda la normativa existente viene dada por disposiciones y consultas vinculantes. Existe por tanto una inseguridad jurídica notoria que confunde a los usuarios y empresas del sector y que frena la adopción de esta tecnología.

Se espera que para 2024 entre completamente en vigor el reglamento MiCA, que regulará expresamente las criptomonedas en la Unión Europea, con el objetivo de garantizar la protección del consumidor, a la vez que se fomenta la innovación y

el crecimiento del sector de criptoactivos. Sin embargo, el reglamento MiCA parece que no resuelve de forma eficaz todas las incógnitas que surgen con las criptomonedas, proporcionando un marco normativo poco definido y con unas restricciones que pueden restringir la innovación.

Es indiscutible que, desde la aparición de Bitcoin en 2009, las criptomonedas han seguido un camino creciente en adopción y altamente volátil en precio. Si inicialmente la utilización que se le dio a los criptoactivos fue meramente especulativa, con el tiempo, el número de usuarios y empresas que ven el potencial de la tecnología también ha crecido.

Bitcoin nace con el objetivo de funcionar como un medio de pago descentralizado y seguro a nivel global. En este aspecto, Bitcoin cumple bien con su labor de ser un medio de cambio, sin embargo, tiene problemas al funcionar como unidad de cuenta o reserva de valor, sobre todo debido a la extrema volatilidad del precio de mercado.

Bitcoin posee propiedades propias del dinero como son la durabilidad, la portabilidad, la divisibilidad, la uniformidad y la escasez. Sin embargo, la aceptabilidad de Bitcoin como dinero a nivel global todavía es limitada, de nuevo, debido en gran medida a su volatilidad. Así pues, Bitcoin todavía tiene un largo camino que recorrer hasta alcanzar la madurez suficiente para poder utilizarse como dinero o reserva de valor.

Por otro lado, Bitcoin puede contribuir a mejorar la inclusión financiera y a mantener el ahorro de los usuarios, sobre todo en países con una escasa estructura financiera o que sufran ciertas dificultades económicas que afecten a la riqueza de su población.

En cuanto a Ethereum, esta criptomoneda se presenta como un entorno atractivo para desarrollar aplicaciones descentralizadas gracias a la posibilidad de construir contratos inteligentes en su Blockchain. Esta capacidad se está explotando, sobre todo, en el campo de las finanzas (Defi).

Estos servicios financieros descentralizados buscan realizar las mismas funciones que tradicionalmente realizaban los bancos, pero sin tener que pasar por estos intermediarios. Los servicios DeFi más populares son los servicios de préstamos directos entre usuarios, los seguros o el intercambio de divisas.

A pesar de todas las aplicaciones y beneficios que puedan ofrecer las criptomonedas, existen todavía muchos desafíos a superar. Todavía se trata de una tecnología emergente que está configurando su funcionamiento a base de ensayo y error. El nivel de incertidumbre existente todavía es muy elevado, tanto por la volatilidad de estos activos como por el desconocimiento existente respecto a su funcionamiento. Esta falta de comprensión se extiende por igual a usuarios finales como a los reguladores que deben proporcionar un marco jurídico apropiado.

En su análisis, Blanco Encinosa (2021) considera que estas dificultades se superarán, concluyendo que las criptomonedas *“como el dinero fiduciario, consolidarán y perfeccionarán sus funciones. Muchos más negocios las asumirán, aceptarán y adaptarán sus sistemas de información para recepcionarlas y pagar con ellas sus compras.”*

Además, añade que *“madurarán las tecnologías y la cultura popular las admitirá, como hizo en el pasado con las semillas de cacao, la plata, el oro, el papel moneda, los cheques, las letras de cambio y las tarjetas plásticas. Los gobiernos poco a poco aprenderán a lidiar con ellas y establecerán mejores procesos regulatorios para evitar que sean empleadas para lavar dinero o en delitos informáticos”.*

Esta conclusión sigue la lógica de la adopción temprana de cualquier tecnología emergente. Sin embargo, para llegar a una utilización efectiva y global de las criptomonedas será necesario un mayor periodo de tiempo y, sobre todo, un mayor nivel de información y formación para todas las personas a las que implicará.

Bibliografía

- Alfonzo, Y. (24 de junio de 2018). Breve historia del Banco central en la sociedad occidental. *que es economía*. Recuperado 25 Mayo, 2023 <https://www.queeseconomia.site/banco-central-historia/>
- Ayuso, J., & Conesa, C. (2020). Una introducción al debate actual sobre la moneda digital de banco central (CBDC). Documentos Ocasionales . *Documentos ocasionales - Banco de España, 2005*. <https://www.bde.es/f/webbde/SES/Secciones/Publicaciones/PublicacionesSeriadas/DocumentosOcasionales/20/Fich/do2005.pdf>
- Banco Mundial. (2021). *The Global Findex 2021: Interactive Executive Summary Visualization*. World Bank. Recuperado 17 Mayo, 2023 <https://www.worldbank.org/en/publication/globalfindex/interactive-executive-summary-visualization>
- bitcoin.com. (s. f.). *Common DApp risks and how to avoid them*. Recuperado 25 de mayo, 2023, de <https://www.bitcoin.com/get-started/common-dapp-risks-and-how-to-avoid-them/>
- Blanco Encinosa, L. J. (2021). Criptomonedas. Breve análisis desde la perspectiva económica y financiera. *Cofin Habana, 15(2), e16*. http://scielo.sld.cu/scielo.php?script=sci_abstract&pid=S2073-60612021000200016&lng=es&nrm=iso&tlng=es
- Cai, W., Wang, Z., Ernst, J. B., Hong, Z., Feng, C., & Leung, V. C. M. (2018). *Decentralized Applications: The Blockchain-Empowered Software System*.

IEEE Access, 6, 53019-53033.

<https://doi.org/10.1109/ACCESS.2018.2870644>

CNMV y Banco de España, (2021) Comunicado conjunto de la CNMV y del Banco de España sobre el riesgo de las criptomonedas como inversión. Recuperado 11 Mayo, 2023 <https://www.cnmv.es/Portal/verDoc.axd?t=%7Be14ce903-5161-4316-a480-eb1916b85084%7D>

Comisión Europea (2020) *COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS on a Digital Finance Strategy for the EU*. Recuperado 17 Abril, 2023. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0591>

Crypto.com. (2023, enero). *Crypto Market Sizing Report 2022*. Recuperado 22 de Mayo 2023. https://content-hub-static.crypto.com/wp-content/uploads/2023/01/Cryptodotcom_Crypto_Market_Sizing_Jan2023-1.pdf

Datosmacro.com. (2023). *IPC según los datos de cada país 2023*. Recuperado 18 de Mayo 2023. | *Datosmacro.com*. <https://datosmacro.expansion.com/ipc-paises>

Fornell, J. (2019, julio). *¿Qué es un Utility Token?*. *Bit2Me Academy*. Recuperado 25 de Mayo 2023. <https://academy.bit2me.com/que-es-utility-token/>

Jansana, N. (2022, agosto). *Los fondos del bitcoin vinculados al blanqueo y actividades ilegales se duplican*. *Bolsamania.com*. Recuperado 25 de Mayo 2023. <https://www.bolsamania.com/noticias/criptodivisas/los-fondos-del->

bitcoin-vinculados-al-blanqueo-y-actividades-ilegales-se-duplica--
10241465.html

Kendus, K. D. K. (2017, agosto). *History Unlocked – August 2017, Early Auto Laws – CTHS*. Recuperado 25 de Mayo 2023. <https://concordhist.org/history-unlocked-august-2017-early-auto-laws/>

Kim, D., & Ryu, D. (2022). *Search-Theoretic Approach to Cryptocurrency Adoption and Financial Inclusion*. SSRN. <http://dx.doi.org/10.2139/ssrn.4119560>

Kshetri, N., & Voas, J. (2018). Blockchain-Enabled E-Voting. *IEEE Software*, 35(4), 95-99. <https://doi.org/10.1109/MS.2018.2801546>

Leal, A. (2023, mayo 21). *Bitcoin Pizza Day: La compra que cambió la historia de las criptomonedas*. CriptoNoticias - Noticias de Bitcoin, Ethereum y criptomonedas. Recuperado 26 de Mayo 2023. <https://www.criptonoticias.com/criptopedia/bitcoin-pizza-day-compra-cambio-historia-criptomonedas/>

Matos, I. Z. (2008). *ANÁLISIS DE LAS CRIPTOMONEDAS EN LA ECONOMIA ACTUAL*. [Trabajo Fin de Grado. Universidad Pontificia Comillas]. <https://repositorio.comillas.edu/jspui/bitstream/11531/25169/1/TFG-Zarraluqui%20Matos%2C%20Aigo.pdf>

Weber, Max. (2021). *Economía y sociedad*. Fondo de Cultura Económica.

Menger, K. (1892). On the Origin of Money. *The Economic Journal*, 2(6), 239. <https://doi.org/10.2307/2956146>

Newbery, E. (2021, septiembre 15). *8 Digital Payment Cryptos That Are Faster Than Bitcoin*. Recuperado 25 Mayo, 2023 <https://www.fool.com/the->

ascent/cryptocurrency/articles/8-digital-payment-cryptos-that-are-faster-than-bitcoin/

Pascual Cerdá, E. (2022). *Criptomonedas. Análisis de sus implicaciones tributarias en España*. [Trabajo Fin de Grado. Universidad Autónoma de Barcelona] https://ddd.uab.cat/pub/tfg/2022/264026/TFG_EstefaniaPascualCerde.pdf

Pascual, J. L. P. (2019, abril). *¿Qué es una Stablecoin?* Recuperado 25 de Mayo, 2023. Bit2Me Academy. <https://academy.bit2me.com/que-es-stablecoin/>

Radford, R. A. (1945). The Economic Organisation of a P.O.W. Camp. *Economica*, 12(48), 189-201. <https://doi.org/10.2307/2550133>

St. Louis Fed. (Anfitrión). (s. f.). *Functions of Money—The Economic Lowdown Podcast Series (Nº 9)*. Recuperado 11 de marzo de 2023, de <https://www.stlouisfed.org/education/economic-lowdown-podcast-series/episode-9-functions-of-money>

Sun, X., Yu, F. R., Zhang, P., Sun, Z., Xie, W., & Peng, X. (2021). A Survey on Zero-Knowledge Proof in Blockchain. *IEEE Network*, 35(4), 198-205. <https://doi.org/10.1109/MNET.011.2000473>

Gabilondo Garcia, Maria. (2021). *REGULACIÓN DE LOS CRIPTOACTIVOS Análisis del régimen jurídico propuesto en la UE para los activos digitales, y del régimen aplicable actualmente a los DLT Tokens*. [Trabajo Fin de Grado. Universidad Pontificia Comillas]. <https://repositorio.comillas.edu/xmlui/bitstream/handle/11531/48232/TFG%20-%20Gabilondo%20Garcia,%20Maria.pdf?sequence=-1>

Van der Linden, T., & Shirazi, T. (2023). Markets in crypto-assets regulation: Does it provide legal certainty and increase adoption of crypto-assets? *Financial Innovation*, 9(1), 22. <https://doi.org/10.1186/s40854-022-00432-8>

Whipps, H. (2007, noviembre 16). *The Profound History of Coins*. Livescience.Com. Recuperado 14 de Marzo, 2023. <https://www.livescience.com/2058-profound-history-coins.html>

