

GRADO EN COMERCIO

TRABAJO FIN DE GRADO

**“NUEVAS FORMAS DE PAGO, BLOCKCHAIN Y
CRIPTOMONEDAS”**

LUCÍA MARTÍN ESTEBAN

**FACULTAD DE COMERCIO
VALLADOLID, JULIO DE 2021**



UNIVERSIDAD DE VALLADOLID
GRADO EN COMERCIO

CURSO ACADÉMICO 2020/2021

TRABAJO FIN DE GRADO

“Nuevas formas de pago, Blockchain y Criptomonedas”

Trabajo presentado por: Lucía Martín Esteban

Tutor: David Pérez Román

FACULTAD DE COMERCIO

Valladolid, julio de 2021

ÍNDICE:

1	Introducción.....	1
2	Orígenes	2
3	Tecnología que sustenta las criptomonedas: Blockchain	4
3.1	Funcionamiento de Blockchain	5
3.2	La Minería de bloques- Blockchain.....	8
3.2.1	El algoritmo PoW (Proof of Work o “Prueba de Trabajo”)	9
3.2.2	El algoritmo Proof of Stake o “Prueba de Participación”	10
3.3	Clasificación de las redes- Blockchain.....	11
4	La clave del éxito: <i>Halving</i>	14
5	Criptomonedas.....	15
5.1	Características de las criptomonedas.....	17
5.2	Ventajas y desventajas de las criptomonedas.....	19
5.2.1	Ventajas:.....	19
5.2.2	Desventajas:	20
5.3	Monederos de criptomonedas	21
5.4	¿Cómo funcionan los monederos de criptomonedas?	22
5.5	Tipos de monederos de criptomonedas.....	22
5.5.1	Monederos full wallet y lightweight wallet	22
5.5.2	Hardware wallets	23
5.5.3	Papel wallets.....	23
5.5.4	“Hot wallet” y “cold wallet”.....	24
5.5.5	Monederos HD.....	24
5.5.6	Monederos SPV.....	24
5.5.7	¿Son seguros los monederos?.....	25
5.6	Legalidad de las criptomonedas	25
6	Principales Criptomonedas	28
6.1	Bitcoin	30
6.1.1	¿Qué es el Bitcoin?	30
6.1.2	Valoración e historial de precios.....	32
6.2	Ethereum	35
6.2.1	¿Qué es el Ethereum?.....	35
6.2.2	Valoración e historial de precios.....	36
7	Perspectivas de las criptomonedas	38
7.1	Empresas.....	38
7.2	Bancos	40
7.3	Opinión general: El trilema de las criptomonedas	41
7.4	Sectores más avanzados en el uso de las criptomonedas.....	43
8	Proyección futura de las criptomonedas	45
9	Conclusiones.....	47
10	Bibliografía	49

Índice de tablas

Tabla 1: Ejemplo participación en la red	11
--	----

Índice de Ilustraciones

Ilustración 1: Cadena de bloques, Blockchain.....	4
Ilustración 2: Tipos de sistemas. Fuente: (Grange).....	7
Ilustración 3: ¿Cómo funciona Blockchain?	7
Ilustración 4:Proof of Work and Proof of Stake	9
Ilustración 5: Halving Bitcoin	14
Ilustración 6: Criptomonedas.....	15
Ilustración 7: Ciclo de emoción del mercado.....	21
Ilustración 8: Wallet Criptomonedas.....	21
Ilustración 9: Wallet Criptomonedas.....	23
Ilustración 10: Porcentaje de capitalización de criptomonedas en el mercado total en los últimos 7 años (Porcentaje de la capitalización de mercado de las principales criptomonedas , 2021)	28
Ilustración 11: Ranking 10 principales criptomonedas por su capitalización en el mercado. (Principales 100 Criptomonedas por capitalización de mercado, 2021).....	29
Ilustración 12:Porcentaje de capitalización de las criptomonedas.	29
Ilustración 13: Logotipo del Bitcoin.....	30
Ilustración 14: Variación del precio del Bitcoin	32
Ilustración 15: Variación precio Bitcoin en 2020-21	34
Ilustración 16:Logotipo Ethereum.....	35
Ilustración 17:Ejemplo contrato inteligente.....	35
Ilustración 18: Evolución precio de Ethereum.	36
Ilustración 19:Precio Ethereum Mayo-Junio-Julio 2021	37
Ilustración 20: Pagos mundiales con criptomonedas	38
Ilustración 21:Bancos o Criptomonedas.....	40

RESUMEN

Estudio del nacimiento, funcionamiento, desarrollo y evolución de las criptomonedas en el mercado mundial, en concreto el Bitcoin como criptomoneda mas importante y con más cotización en el mercado, junto a Ethereum, Así como el estudio de la plataforma que permite operar con criptomonedas, Blockchain y su aceptación por parte de las entidades centrales, las empresas y las personas.

ABSTRACT

Study of the creation, operation, development and evolution of crypto currencies in the world market, specifically Bitcoin as the most important crypto currency and with more quotation in the market, next to Ethereum, as well as the study of the platform that allows to operate with crypto currencies, Blockchain and its acceptance by central entities, companies and people

PALABRAS CLAVE:

Dinero, Moneda, Criptomoneda, Blockchain, Bitcoin, Minado, Monedero

1 Introducción

En el pasado la gente solía comercializar con artículos útiles para su vida, por ejemplo, cambiaban la carne de un animal por leña, pero igual que todo, el comercio evolucionó y se empezaron a utilizar elementos con valor asociado como el oro, la plata o piedras preciosas. En la actualidad el medio de cambio utilizado son las monedas y los billetes, el llamado dinero fiduciario.

El dinero fiduciario se basa en la confianza de las, ya que no está respaldado por nada que no sea el compromiso de pago por la entidad emisora. Es controlado por autoridades financieras, los bancos.

Durante la revolución del comercio electrónico el 1990, algunos pioneros empezaron a preguntarse de que forma podría evolucionar el dinero para poder evitar las autoridades centrales y ser digital.

Al principio muchos de los pioneros se dieron cuenta de que era muy complicado implementar una moneda y un sistema que funcionara correctamente independiente de los bancos y los gobiernos. El problema principal se basaba en que era muy complicado que dos terceros se fiaran para hacer una transacción de forma online sin ninguna entidad que asegurase la operación.

La primera criptomoneda, el Bitcoin ofreció una solución a este problema utilizando la criptografía para crear un registro descentralizado impenetrable.

El corazón que hace posible el funcionamiento recibe el nombre de Blockchain, la cadena de bloques que permite hacer transacciones persona a persona de forma segura.

A lo largo del trabajo estudiaremos a fondo el sistema Blockchain, como surgió, que funcionamiento tiene y que algoritmos son los empleados para este sistema, además analizaremos los tipos de redes que pueden existir

También estudiaremos las criptomonedas, sus características principales, las plataformas necesarias para poder operar con ellas y las leyes bajo las que se debe operar. Haré un profundo estudio sobre las dos criptomonedas mas importantes en el momento y cuál ha sido su evolución.

Por ultimo analizaremos el punto de vista de los bancos, las empresas y las personas sobre las criptomonedas, cuáles son los sectores en los que más se usan y sus perspectivas de futuro.

2 Orígenes

A lo largo de los tiempos se han inventado y utilizado muchos medios de intercambio de bienes y servicios. Cada uno de ellos ha sufrido transformaciones debido a su evolución, cambios o incluso han llegado a desaparecer. El sistema actual de intercambio de monedas y billetes surgió de la evolución de los antiguos sistemas de trueque e intercambio de metales preciosos

Sin embargo, debido a la evolución y los avances tecnológicos surge la necesidad de encontrar un medio de intercambio adaptado a los tiempos: las criptomonedas o criptodivisas.

El nacimiento de las criptomonedas¹ o criptodivisas se sitúa en los años 80. Con el objetivo de encontrar un medio para crear cambios sociales y políticos surge un nuevo movimiento llamado Cypherpunk². Su funcionamiento se basaba en proteger la privacidad de las personas frente a los gobiernos. David Chaum, precursor de la utilización de la criptografía en el medio digital y un firme defensor de la privacidad, estableció sistemas criptográficos de alta seguridad, alguno de los ejemplos son las firmas ciegas y grupales, las credenciales criptográficas y el primer modelo de dinero criptográfico seguro. (Jurado, 2021)

En la década de los 90, David Chaum crea “Digicash”, un sistema de dinero electrónico centralizado que permite realizar transacciones de manera anónima con total seguridad. (Muñoz, 2021)

A raíz del nacimiento del dinero criptográfico seguro y los avances tecnológicos, en 1997 aparece una nueva tecnología llamada “Hash cash”³ de mano de Adam Black, su función era formar parte de la validación de algoritmos de bloques, a través de la minería de las criptomonedas, de forma simplificada, un usuario usa el proceso de hash cash para crear un sello que garantice y verifique su legitimidad. Para los expertos, gracias a este software se pudo definir los principales pilares que determinan los protocolos de seguridad y de minería que inspiraron las criptomonedas. (Quintiliano, 2021)

¹Podemos definir las criptomonedas como un tipo de moneda digital, no existen de forma tangible, pero sirven como moneda de intercambio, permitiendo transacciones instantáneas a través de internet a cualquier parte del mundo.

² El movimiento llamado Cypherpunk lo conforman el conjunto de personas que promueven el activismo digital y tratan de proteger tanto la privacidad como la seguridad de los usuarios digitales usando la criptografía para asegurar el anonimato.

³ Hash Cash se creó como una solución para evitar el Spam, para ello utiliza una prueba de trabajo que permite verificar que un correo determinado no es publicidad o basura.

En 1998, un año después de la creación de Hash cash, Wei Dai diseña b-money, con la intención de crear un sistema de dinero electrónico que permitiera mantener el anonimato y que estuviera distribuido. Este sistema no se llegó nunca a implantar, pero muchos analistas consideran que fue la primera criptomoneda real, ya que el sistema que planteaba se asemeja mucho al esquema de prueba de participación, es decir, el sistema teórico de las criptomonedas actuales. (Savedra, 2019)

En 2009 un desarrollador desconocido publicó bajo el seudónimo de Satoshi Nakamoto⁴ creó la primera criptomoneda, el Bitcoin. (¿Quién es Satoshi Nakamoto?, 2021)

⁴ La identidad de Satoshi Nakamoto es una de las identidades más misteriosas en el mundo de las criptomonedas. No se conoce nada más que una secuencia de mails que propiciaron una de las invenciones tecnológicas con más importancia de la humanidad. El Bitcoin y la red Blockchain

3 Tecnología que sustenta las criptomonedas: Blockchain



Ilustración 1: Cadena de bloques, Blockchain

Para conseguir entender las criptomonedas y los Bitcoins, en primer lugar, hay que comprender la tecnología Blockchain, podemos entenderlo como un registro de datos donde cada usuario o nodo en la red ejecuta y almacena transacciones y las agrupa en forma de bloques. (Molano, 2019)

La confianza en los agentes encargados de intermediar en las operaciones financieras desapareció como consecuencia de la crisis de 2007, y fue el motivo por el cual se produjo en desarrollo tecnológico con capacidad de trasladar el control de las entidades financieras a los propios usuarios, sin necesidad de tener un intermediario que valide las operaciones. La desaparición de la intermediación hace posible que los sistemas financieros, económicos e incluso políticos sean más transparentes y democráticos. (Parrondo, 2018)

La tecnología Blockchain permite registrar transacciones de una forma segura, transparente y descentralizada, además, aunque la tecnología Blockchain dio el salto a la fama con la aparición del Bitcoin cuando experimentó una subida del mil por ciento, no solo se puede utilizar con criptomonedas, si no que su uso se extiende a muchos más horizontes. (Parrondo, 2018)

Blockchain tiene la capacidad suficiente para poder almacenar y registrar las transacciones y operaciones de usuario a usuario de forma segura, eficiente, inmutable y verificable. Por lo tanto, como he comentado anteriormente puede aplicarse a todo tipo de tareas como las auditorías o la contabilidad de productos de la cadena de suministros

La tecnología Blockchain podría ayudar a solventar muchos problemas de diferentes vertientes, en la industria de los medios digitales, podría zanjar el problema de piratería de video y música, podría conseguirse legalizar al completo la industria artística haciendo que las compras, ventas y herencias sean legítimas, desde el punto de vista social, podría utilizarse para la emisión de votos o para comprobar si la certificación de un

producto es de origen ético. En el caso de los servicios públicos podría utilizarse para realidad pagos de la salud, o para verificar los documentos de registro de la propiedad. Todo ello de forma segura, transparente permitiendo a los usuarios prescindir de los intermediarios que suelen encargarse de validar las entidades, la titularidad o la validez de las transacciones. (¿Qué es le tecnología Blockchain?, 2021)

La implantación de la tecnología Blockchain en las empresas puede desencadenar una nueva revolución para la innovación y las formas de financiación de proyectos empresariales. (¿Qué es le tecnología Blockchain?, 2021)

3.1 Funcionamiento de Blockchain

Para comprender como funciona la red del Blockchain, veamos cómo funcionan las redes tradicionales.

A lo largo siglos, las redes tradicionales han usado bases de datos para recopilar y almacenar datos de transacciones y operaciones e información, y las entidades gubernamentales las han usado para crear y alimentar registros públicos. Hasta el momento, era necesaria la existencia de un intermediario central o autoridad, como los bancos o las oficinas gubernamentales para gestionar los cambios en las transacciones e indicar quién es el poseedor y de qué es poseedor en un momento concreto. Este proceso permite legitimar las operaciones. (Pastor, 2018)

EL hecho de que los usuarios confíen en el intermediario para que verifique las transacciones correctamente, permite que los usuarios puedan intercambiar bienes entre sí aun sin conocerse. El cometido de los intermediarios es ofrecer la seguridad y protección suficiente entre los interesados y mantener un control para acceder a la información del registro oficial.

Estos registros tradicionales, aunque han sufrido una mejora con la aplicación de la tecnología digital, presentan ineficiencias en costes y tiempo, y una insuficiencia de capacidad para frenar el incremento de fraudes y crisis de desconfianza. (Parrondo, 2018)

En la red de Blockchain, se sustituye la autoridad central encargada de la legitimación de las transacciones.

Veamos un ejemplo aclarativo, tradicionalmente, si una persona quería transferir doscientos euros a otra persona, tenía que seguir un proceso, en primer lugar ir al banco, demostrar que es el propietario de la cuenta y ordenar que se llevara a cabo una transacción por una cantidad de doscientos euros a otra persona, el banco se encargaría de comprobar que efectivamente la persona dispone de esa cantidad de dinero para realizar la transacción y exigiría al banco de la persona receptora ingresar en la cuenta de

la otra persona doscientos euros. A cambio de los trámites el banco cobraría al emisor una comisión de transferencia (normalmente) y el dinero llegaría a su destinatario el plazo aproximado de dos días.

Con la red de Blockchain, el banco desaparecería y el proceso sería el siguiente: el emisor ordenaría que se traspasen doscientos Bitcoins a otra persona, cada nodo⁵ de la red comprobaríamos que tiene dicha cantidad de criptomonedas y que no han sido transmitidas con anterioridad. Una vez haya sido comprobado. La transacción es aprobada y registrada en la red, y de forma automática el receptor recibe los doscientos Bitcoins sin coste alguno. (Parrondo, 2018)

Por lo tanto, los usuarios dejan de depender de un organismo central intermediario, sino que son todos los nodos de la red los encargados de verificar la legitimidad de la transacción. Además, en el sistema tradicional, tanto el emisor como el destinatario de la operación son conocidos, mientras que con la tecnología Blockchain se puede mantener el anonimato de las partes. Todo se produce gracias a su construcción distribuida y a un conjunto de algoritmos e incentivos que aseguran una única verdad registrada: La minería.

El nacimiento del Blockchain se produce por la aparición de la criptomonedas, en concreto con el Bitcoin. Satoshi Nakamoto define en su libro blanco del Bitcoin las criptomonedas como:

“Definimos una moneda electrónica como una cadena de firmas digitales. Cada propietario transfiere la moneda al siguiente propietario firmando digitalmente un hash de la transacción previa y la clave pública del siguiente propietario, y añadiendo ambos al final de la moneda. El beneficiario puede verificar las firmas para verificar la cadena de propiedad”. (Nakamoto, 2008)

⁵ Entendemos por nodo cada uno de los ordenadores interconectados a la red de criptomonedas, encargados de verificar cada uno de las operaciones mediante el software que permite su funcionamiento.

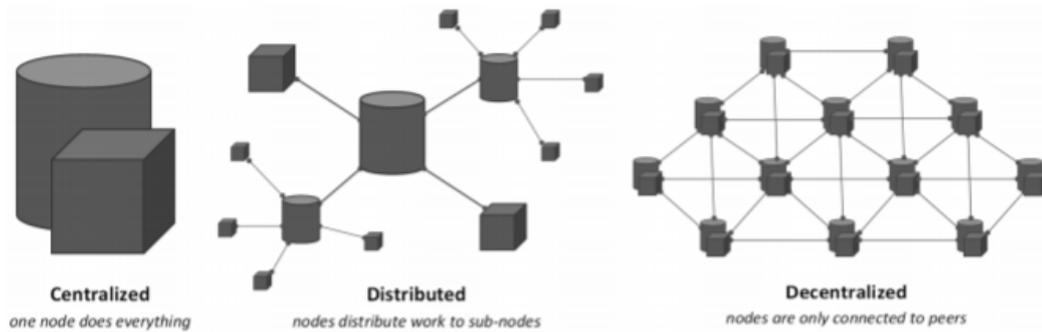


Ilustración 2: Tipos de sistemas. Fuente: (Grange)

El objetivo principal de la red Blockchain es verificar la propiedad de lo que se quiere traspasar y que no se ha traspasado con anterioridad, es decir, evitar la duplicidad de las operaciones. La forma de conocer que una moneda no se ha traspasado con anterioridad es conociendo en que se ha utilizado la moneda previamente. Para poder realizar cualquier operación con la moneda, esta registra una firma de entrada y de salida por lo que si la moneda ya tiene una firma de salida del propietario que está intentando volver a traspasarla, los nodos de la red lo descubrirán y no se validará la operación. (Parrondo, 2018)

CÓMO FUNCIONA EL BLOCKCHAIN

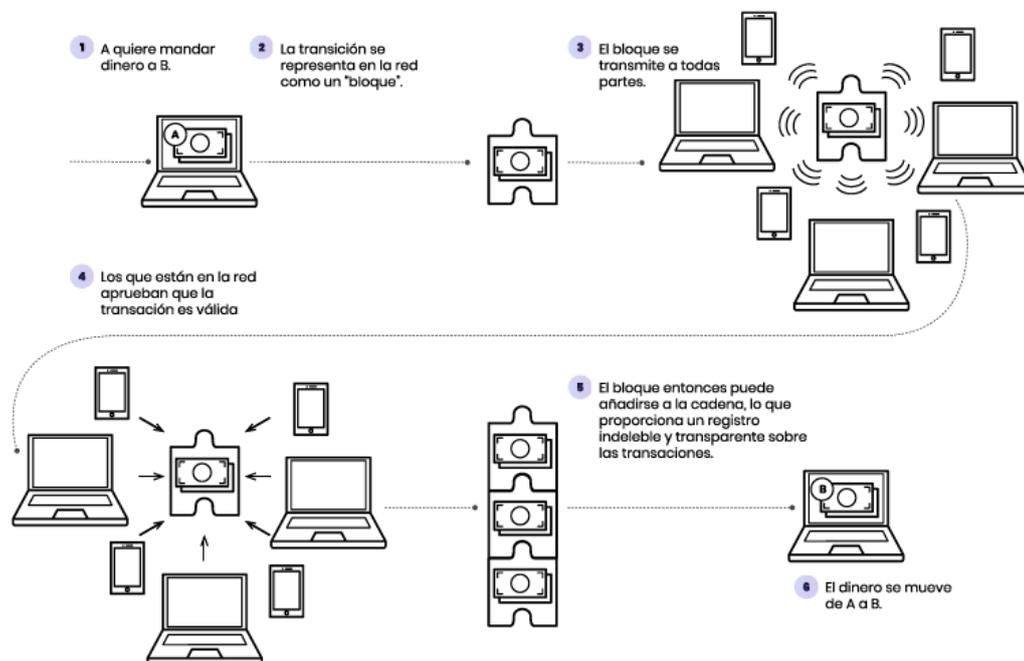


Ilustración 3: ¿Cómo funciona Blockchain?

En el Sistema de la red Blockchain, las operaciones y transacciones que se realizan son públicas, de forma que cada uno de los nodos que forman parte de la red confirma la única verdad existente, detectando, si se da el caso, el fraude o intento de engaño. Los

datos a los que los usuarios tienen acceso para comprobar la veracidad de la transacción se almacenan en una cadena de bloques codificados, almacenados no solo en el servidor de la red si no en cada nodo que participa.

Cualquier usuario puede solicitar desde su nodo una transacción que se agrega a la cadena de bloques, hasta que dicha solicitud no sea verificada y legitimada por todos los usuarios de la red, no se lleva a cabo la transacción. El proceso mediante el cual se verifican los datos de una transacción y se legitima recibe el nombre de minería. Son los mineros lo que llevan a cabo el proceso de minería, que de forma simplificada consiste en verificar que la solicitud de transacción proviene de una persona con capacidad y autorización para hacerlo, certificar que el transmisor es el propietario de lo que se va a traspasar y que no ha sido transmitido con anterioridad.

Para verificar las transacciones, los mineros deben resolver un problema matemático, y cuando se encuentra la solución válida, un nuevo bloque se mina y se añade a la cadena de Blockchain en consenso del resto de participantes. El minero que encuentra la solución válida recibe una recompensa por el bloque minado y añadido a la red.

Cuando se añaden los bloques a la red, estos son públicos para todos los participantes y se registran, como he dicho anteriormente, no solo en el servidor si no en cada uno de los nodos de la red. La información es descentralizada por lo que ningún participante podrá eliminarlo o modificarlo, es un sistema inviolable, cada usuario puede comprobar la veracidad de una operación en su propio registro.

3.2 La Minería de bloques- Blockchain

Entendemos la minería como la forma de registrar los datos de transacciones de forma encriptada en la cadena de bloques. Se lleva a cabo por los mineros mediante la resolución de un problema matemático, el minero que antes encuentre la solución válida mina el bloque, que se une a la cadena de bloque y reciben una recompensa a cambio del trabajo realizado y los medios utilizados. La recompensa de los mineros es la obtención de una cantidad determinada de las criptomonedas que estén minando, los mineros ponen a la venta, es decir en circulación esas nuevas criptomonedas y obtienen los beneficios por sus ventas. Así obtienen la recompensa económica por su trabajo y por los gastos incurridos de la resolución del problema matemático.

El proceso de minería se lleva a cabo mediante la utilización de dos métodos principales: PoW (Poof of Work) o PoS (Proof of Stake). Son tipos de algoritmos que permiten al sistema la distribución de todas las monedas que han sido ya minadas.



Ilustración 4: Proof of Work and Proof of Stake

3.2.1 El algoritmo PoW (Proof of Work o “Prueba de Trabajo”)

El algoritmo basado en la prueba de trabajo fue diseñado principalmente con el objetivo de crear un sistema seguro que permitiera a los usuarios realizar sus transacciones en la red sin riesgo de sufrir ataques maliciosos. El funcionamiento es sencillo y puede dividirse en seis etapas

La primera etapa es la de transacción, el proceso de minado de un bloque comienza cuando un usuario desea enviar dinero a otro usuario, el usuario emisor envía una solicitud de transacción al resto de usuarios y se mantiene a la espera hasta que el resto de usuarios validen y confirmen la transacción para poder llevarla a cabo.

La segunda etapa o de recopilación, las peticiones de transacción en la red se recopilan en bloques por los mineros, son los mineros lo que forman cada bloque de “solicitudes”, no se reparten, por lo que cabe la posibilidad de que varios usuarios hayan usado para crear los bloques las mismas transacciones, pero el minero que resuelva el algoritmo matemático será el que mine el bloque y “gane” la carrea, haciendo que el resto de mineros tengan que reconstruir sus bloques de solicitudes de transacción pendientes.

La tercera etapa consiste en la formación, una vez que cada nodo minero haya recopilado las transacciones que quiere agrupar en cada bloque debe formar el bloque e incluir el hash del bloque anterior.

La cuarta etapa es la prueba de trabajo, una vez formado el bloque, con el hash anterior y la recopilación de solicitudes, tiene que crear una firma válida para el bloque, se realiza mediante un complejo cálculo que requiere mucha potencia computacional y gasto de energía eléctrica, la solución es conocida como hash de salida. En este momento, cuando el minero consigue el hash de salida, quiere decir que ha conseguido la solución válida del algoritmo matemático, y se mina el bloque.

La quinta etapa cuando el bloque ha sido minado, debe ser transmitido dicho bloque con el consentimiento y firma del resto de nodos de la red para que sea validado. Una vez concluido el proceso de minado y realizado su transmisión, el minero recibe la recompensa

Sexta etapa: es la etapa de verificación, al igual que el resto de procesos que se realizan en la red Blockchain, la transmisión también debe ser validada y verificada por los nodos de la red. Verifican que tanto el bloque como el hash cumplen con los requisitos necesarios para entrar en el sistema y verifican su legitimidad. También se comprueba la realización de la prueba de trabajo, el minero que ha minado el bloque y su capacidad computacional para verificar que realmente ha sido el quien ha resuelto el algoritmo. Así como la capacidad de la persona en concreto para hacer uso de las criptomonedas recibidas. (¿Qué es PoW?, 2021)

3.2.2 El algoritmo Proof of Stake o “Prueba de Participación”

El algoritmo de prueba de participación es completamente diferente a la prueba de trabajo. Para empezar, viendo las diferencias, la principal es que, en este modelo, no son los participantes los que eligen las transacciones que validan, sino que es el propio sistema el que asigna un nodo como nodo validador de un bloque con un conjunto de transacciones ya fijadas. La asignación de un nodo como validador de un bloque se hace de forma aleatoria, pero de forma equitativa, es decir, un nodo que tenga mucho peso en la red por sus reservas y participación, tendrá muchas más probabilidades de ser asignado como validador que otro nodo con muchas menos reservas y peso en la red

Por lo tanto, cuantas más reservas tenga un nodo en la red, más posibilidades tendrá de ser asignado validador y obtener ganancias económicas

Al igual que en el algoritmo de prueba de trabajo, aunque la asignación o elección de los nodos que minan los bloques es diferente, el consenso necesario para validar las transacciones y acciones llevadas a cabo en la red es obligación de todos los usuarios. (García & Molekle, 2017)

Para explicar mejor el proceso equitativo mediante el cual se asignan los bloques a minar, analizaremos en la siguiente tabla como se repartirían los bloques teniendo en cuenta el peso en la red de cada nodo.

De forma simplificada vemos como la red que planteamos está formada por 100 inversores, existen 3 grupos diferentes con una cantidad de monedas cada uno en reserva y vemos cuál sería su porcentaje de participación:

Grupo de inversores	Inversores	Monedas en reserva	Total monedas de reserva	% participación
Grupo A	50	1000	50000	15,38%
Grupo B	30	2500	75000	23,08%
Grupo C	20	10000	200000	61,54%
TOTAL	100	325000	325000	100%

Tabla 1: Ejemplo participación en la red

El grupo A es el más numeroso en cuanto a inversores, sin embargo, tiene menos monedas en reserva que los grupos B y C, el grupo B tiene menos inversores que el Grupo A, pero tiene más monedas en reserva. Por último, el grupo C es el que menos inversores tiene y el que más monedas en reserva. Por lo tanto y cómo podemos observar, el número de inversores es indiferente, el parámetro que se tiene en cuenta para asignar los bloques es el peso que tienen en la red por la cantidad de monedas que tengan en posesión.

Una vez se ha llevado a cabo el proceso de asignación los nodos validadores realizan la tarea de validar transacciones o crear nuevos bloques con el incentivo de conseguir beneficios económicos.

Cuando el proceso de minado de un bloque ha finalizado, se vuelve a empezar y se realiza la asignación a otro nodo para asegurar la participación de todos los nodos en la red.

A diferencia del proceso de prueba de trabajo, el algoritmo de participación no requiere el gasto tan elevado de equipos informáticos y capacidad energética.

3.3 Clasificación de las redes- Blockchain

Para hacer una clasificación de las redes hay que atender a dos aspectos diferentes:

En primer lugar, basándonos en la capacidad de los usuarios de acceder a los registros, podemos diferenciar entre redes públicas y privadas. Las redes privadas restringen el acceso a los datos a los usuarios en general si no tienen autorización, están delimitadas, sin embargo, las redes públicas son de acceso libre para todos los usuarios participantes en la red, no tienen ningún tipo de delimitación.

En segundo lugar, basándonos en la capacidad de los usuarios de realizar transacciones y añadirlas a bloques, podemos diferenciar entre redes sin permisos o con permisos. En las redes sin permiso, los usuarios pueden agregar y generar transacciones y bloques libremente (siempre asegurando que el usuario tiene capacidad para realizar la transacción, que las criptomonedas con las que opera son realmente suyas y no las ha

traspasado con anterioridad) y los mineros reciben recompensas por minar los bloques y añadirlos a la cadena de bloques. Las redes con permisos las usan generalmente empresas privadas para uso interno, los usuarios necesitan tener permiso de los administradores de la red, este tipo de redes son centralizadas, lo que quiere decir que al igual que los bancos, están controladas por una entidad central de la que dependen todas las transacciones. Tampoco existe el sistema de recompensas porque es la propia entidad la encargada de verificar y validar las operaciones.

Dadas estas características podemos clasificar las redes de Blockchain en tres grupos:

- **Blockchain Pública**: Como hemos explicado anteriormente, en este tipo de red cualquier usuario puede realizar transacciones, crear bloques o formar parte del proceso de minado y validación de los bloques. El proveedor de confianza de estas redes públicas, es el proceso de consenso llevado a cabo a través de la minería y la encriptación de datos a través de los dos mecanismos descritos anteriormente *Work of Proof (WoP)* y *Work of Stake (Wos)*. Las Blockchain públicas son por naturaleza descentralizadas, algunos ejemplos de las criptomonedas que operan en este tipo de redes son Bitcoin, Ethereum, Litecoin, Namecoin...
- **Blockchain de consorcio**: Consiste en validar las transacciones de la cadena de bloques por la mayoría de los nodos, es decir, si la Blockchain está formada por 100 nodos, es necesario que 75 de ellos estén de acuerdo para validar y legitimar la transacción. No es necesario la validación de todos los nodos de la red. El acceso a los datos puede ser público o restringido para los usuarios, este tipo de cadenas de bloques suelen considerarse como parcialmente descentralizadas. Algunos ejemplos son: BankChain, Alianza Enterprise Ethereum, R3...
- **Blockchain privada**: La Blockchain privada es siempre centralizada, lo que significa que todas las transacciones deben ser validadas y registradas por una o varias entidades centrales de las que dependen todos los usuarios de la red. El acceso al registro de datos puede ser público o limitado, a elección de la entidad central.

Cabe destacar el caso de hyperledger, uno de los proyectos de apoyo a la creación de Blockchain privadas, lo forman un conglomerado de empresas asociadas que pretenden crear una plataforma global para el uso de Blockchain privadas, es decir, la empresa que quiera usar una Blockchain privada no deberá desarrollar la plataforma, sino que ya está creada como

un “formato” base. Empresas muy destacadas forman parte del conglomerado, algunas de ellas son Intel, IBM, Cisco...

4 La clave del éxito: Halving

Con el objetivo de explicar en qué consiste el método halving vamos a estudiar es caso de los Bitcoins. Desde su origen, solo existen 21 millones de Bitcoin, cada diez minutos desde el momento de su lanzamiento, se libera un único bloque de información. El primer bloque conocido como “*genesis block*” se estableció el 3 de enero de 2009. La cantidad de monedas de cada bloque no es fija, sino que va variando de la siguiente forma: Primero cada bloque estaba formado por 50 Bitcoins, cada aproximadamente 4 años, este número se divide por la mitad en un proceso llamado *halving*. Está previsto que en 2036 ya se habrán minado el 99% de los Bitcoins existentes, y el ultimo Bitcoin se minará en 2040.

Se puede entender el halving como el proceso por el cual se limita o regula la oferta, unido a que el número existente de Bitcoins es finito y que por lo tanto el límite no puede superarse ni puede alterarse el ritmo en que incrementa la masa de Bitcoins disponibles. Lo que hace el sistema completamente previsible, lo que resulta fundamental para un sistema monetario.

Pero, ¿No es un problema la escasez de Bitcoins? Lo cierto es que no, ya que cada Bitcoin se puede dividir hasta el octavo decimal y en un futuro aún más.

Por lo tanto, aunque la cantidad de Bitcoins contenidos en cada bloque vaya disminuyendo debido al halving, si las transacciones van en aumento, la recompensa de los mineros seguirá siendo interesante, garantizando la sostenibilidad del sistema.

“Según los expertos, una transferencia de Bitcoin es al menos tres veces más segura que una transferencia entre cuentas bancarias, así que si alguien cree que los algoritmos criptográficos empleados por Bitcoin no son lo suficientemente confiables, tampoco deberá confiar en las tarjetas de crédito, ni en cualquier tipo de transferencia bancaria electrónica” (Bitcoin. La moneda del futuro)



Ilustración 5: Halving Bitcoin

5 Criptomonedas

La primera criptomoneda reconocida fue el Bitcoin, con su aparición comenzó a desarrollarse la expansión de muchas otras criptomonedas. Desde su aparición todas fueron consideradas monedas, aunque realmente no entraban dentro de la definición de moneda.



Ilustración 6: Criptomonedas

La definición de moneda contempla que son unidades de cuenta, con una reserva de valor y se usan como medio de cambio. Ya que el ecosistema de nuevas monedas fue creado a partir de la aparición del Bitcoin, que sí que cumplió con la definición de monedas, se consideró que el resto también lo eran.

Podemos definir **la criptomoneda** como un tipo de moneda basada en la criptografía⁶. Al igual que las monedas en general, su fin es ser un medio de pago, pero mucho más seguro al utilizar algoritmos de encriptación para registrar todos sus movimientos. Se usa la criptografía para regular la cantidad de monedas que están en circulación y validar y verificar el proceso de pago de forma segura para ambas partes. En resumen, las criptomonedas son un tipo de moneda virtual que se utiliza como medio de pago y se caracteriza por ser un sistema descentralizado. Las operaciones se realizan mediante un cifrado digital que brinda la seguridad del usuario y sin necesidad de la existencia de intermediarios.

Al hablar de criptomonedas y *Tokens*, debemos tener en cuenta que son diferentes, la criptomoneda o moneda digital son lo mismo y según su definición son únicamente monedas, entendidas como un medio de cambio, mientras que los Tokens tienen una

⁶La criptografía basa su uso es la utilización de códigos cifrados mediante algoritmos que brindan seguridad a los usuarios que la usan. Los códigos son realmente información que se ha modificado para que el resto de usuarios no pueda leer dicha información, es ilegible si no se resuelve el algoritmo.

utilidad más amplia y su concepto no se liga únicamente a la moneda, sino que tiene muchas más acepciones como ficha o cheque de regalo. Tradicionalmente al hablar de *Token* nos referimos a las fichas que se usan como forma de pago en los eventos privados.

Aunque los conceptos son diferentes muchas veces se confunden los Bitcoins con los Tokens o los Tokens con criptomonedas. A medida que ha ido avanzando la tecnología, estos conceptos se han simplificado mucho más para permitirnos hacer una diferenciación clara; las criptomonedas que incluyen los Bitcoins y los Altcoins tienen la función de medio de pago, mientras que los Tokens o criptovalores incorporan funciones adicionales al medio de pago.

La palabra Altcoin proviene de la combinación de las palabras alternativa y coin, como bien puede entenderse, es una moneda digital alternativa al Bitcoin, es decir el conjunto de criptomonedas que no son Bitcoins (Marco Sanjuán, s.f.), Estudiaremos con profundidad los Altcoin más adelante.

Los Tokens son un tipo de activo, puede o no ser una moneda, que al realizar transacciones se registra en una cadena de bloques de una determinada plataforma, alguna de las plataformas más conocidas y en auge son Ethereum o Wave. La característica principal de los Tokens es que pueden representar cualquier tipo de activo que sea fungible y negociable, como participaciones en proyectos empresariales o medios de pago. (Díaz, 2018)

Un caso bastante conocido de las plataformas de Tokens **es Energy Efficiency Coins (EEcoin)** hace referencia a un Token mediante el cual un usuario puede ser partícipe de un ecosistema de Blockchain orientado al uso de las energías renovables. Los usuarios pueden votar y proponer nuevos proyectos al resto de miembros de la red. Los propietarios de los Tokens pueden comercializar con ellos, sin embargo, aunque pueda parecer que forman parte de la empresa, no tienen los mismos derechos que los accionistas.

En el libro blanco de EEcoin dice:

“EECoin is not a security, future, or share, it is not a guarantee of ownership in a company or any underlying assets, or a claim against any consumer rights as guaranteed by EnLedger. The goal of this structure is to offer the public a way to participate in an energy-efficient Blockchain network and to provide capital to renewable energy projects, increasing price competition for renewable energy assets and thereby enabling society to directly provide a market incentive for production of renewable forms of energy as opposed to nonrenewable one” (Libro Blanco EEcoins)

En el párrafo explica que la plataforma EEcoins no está pensada como un negocio que de seguridad, un futuro o una acción, sino que el objetivo es ofrecer al público una forma de participar en una red de eficiencia energética para proporcionar capital a futuros proyectos, y crear un incentivo de mercado para la producción de formas de energía renovables.

La función más habitual de los Tokens es, al igual que en el ejemplo anterior, recaudar fondos para proyectos específicos, hay casos en que los propietarios de los Token reciben como recompensa beneficios del proyecto o participaciones. Crear Tokens es muy sencillo, y es esa sencillez la que ha potenciado su uso entre las empresas para la creación de campañas de fidelización o recaudación de fondos a través de una oferta inicial de monedas o *Initial Coin Offering* (ICO), lo estudiaremos más adelante.

5.1 Características de las criptomonedas

La Dirección General de Operaciones, Mercados y Sistemas de Pago del Banco de España considera las monedas virtuales como *“un conjunto heterogéneo de instrumentos de pago innovadores que, por definición, carecen de un soporte físico que los respalde”*.

Las criptomonedas se caracterizan por tener un conjunto de rasgos comunes que son la clave de su fama y justifican su operatividad y su calor económico:

- **Descentralización:** Es la característica diferencial de las criptomonedas y el motivo de su creación, al hablar de descentralización hacemos referencia al hecho de que las monedas digitales no se encuentran controladas ni reguladas por ninguna autoridad. Por esta razón el mercado determina el valor de las criptomonedas, sin la interferencia de ningún banco, país o gobierno. Además, el término descentralización hace referencia a que las operaciones con criptomonedas se realizan únicamente mediante internet, favoreciendo aún más el no control de una autoridad.
- **Operatividad:** El hecho de que las criptomonedas no operen en ningún mercado en concreto, sino que es común a todos los mercados, hace posible que puedan realizarse operaciones las 24h del día, durante 365 días al año. Este rasgo de las criptomonedas es diferencial, ya que para el uso de las mismas únicamente es necesario un oferente y un demandante, evitando los gastos producidos por terceros en las transacciones.
- **Confidencialidad:** Al realizar una transacción con una criptomoneda, es necesario que tengan dos códigos, uno de entrada y otro de salida, que solamente conocen las partes de la operación. Esto hace posible que no sea necesario revelar tu identidad al hacer una transacción. Este aspecto tiene

ventajas e inconvenientes, ya que permite mantener la privacidad, pero también hace posible la participación confidencial en actividades ilícitas.

- **Volatilidad:** Como hemos mencionado anteriormente, el valor de las criptomonedas varía según los flujos de mercado, sin que ninguna autoridad interceda, de forma que puede sufrir de forma repentina alteraciones en su valor. Esta característica favorece el trading⁷ en el mercado de criptomonedas, es decir, la negociación o especulación de las mismas.
- **Aceptación:** El valor de las monedas depende del mercado y de los propios usuarios de la red, varía según la aceptación de su valor, es decir, el valor que están dispuestos los usuarios a pagar por una moneda.
- **Transparencia:** Hace referencia a la capacidad que tienen todos los individuos de la red de Blockchain a acceder a un registro propio. En los registros de cada nodo aparecen todas las transacciones que se realizan en la red.
- **Limitadas:** debido a la forma de producción de criptomonedas, no existe un número ilimitado a diferencia de las monedas o billetes tradicionales. La producción de criptomonedas es muy diferente ya que se crean a través del proceso explicado anteriormente, la minería.
- **Inmediatez:** las operaciones realizadas con criptomonedas se efectúan con mucha rapidez, un factor muy importante para las transacciones realizadas desde países diferentes, por ejemplo, ya que pueden realizar y recibir las transacciones prácticamente de forma inmediata, sin necesidad de esperar un plazo para darlas por finalizadas.
- **Desregulación:** Actualmente, no existe una regularización de las criptomonedas, aunque cada vez está más cerca la creación de un reglamento comunitario.

“Un marco legal específico es necesario a nivel europeo para hacer normas hechas a medida de los criptoactivos que todavía no están dentro de ninguna otra legislación ya vigente. Este marco deberá impulsar la innovación y la justa competencia además de proveer altos estándares de protección para los consumidores y garantizar la integridad del mercado. Con él, los servicios relacionados con

⁷ El trading o especulación bursátil se lleva a cabo cuando los inversores intercambian sus activos financieros con el objetivo de conseguir un beneficio económico.

criptoactivos deberían tener más fácil crecer y operar de forma transfronteriza dentro de la Unión” (Belinchón, 2020)

- **Accesibilidad:** Un distintivo clave de las criptomonedas es que cualquier persona puede acceder a la red y adquirirlas, crear una cartera de criptomonedas o wallet⁸ y comenzar a realizar transacciones enviando y recibiendo criptomonedas. Las criptomonedas pueden conseguirse por dos vías, la primera de ellas es mediante un monedero, al verificar un bloque, el minero recibe nuevas monedas con las que puede operar, la recompensa de las monedas se debe al complejo trabajo que conlleva descifrar los algoritmos matemáticos y a los medios necesarios y energía computacional para poder llevarlos a cabo, todo ello hace que sea un medio muy poco accesible. Sin embargo la segunda forma tiene un funcionamiento más sencillo y accesible, ya que únicamente consiste en adquirir las criptomonedas a empresas u otras personas a través de las casas de cambio⁹.

5.2 Ventajas y desventajas de las criptomonedas.

Una vez definidas las características principales de las criptomonedas, cabe destacar las ventajas y desventajas frente al sistema tradicional de cambio de monedas y billetes.

5.2.1 Ventajas:

Una de las principales ventajas de las criptomonedas es que su **coste de transacción** habitualmente es muy bajo, a diferencia de las transferencias bancarias tradicionales que incluyen una comisión por la realización de operaciones financieras. La disminución o eliminación de los costes de transacción se traduce en que los vendedores, por ejemplo, no tienen que incluir este gasto en los precios de sus productos y servicios y pueden permitirse bajar sus precios.

Además, las transacciones se producen con mucha más **rapidez** con criptomonedas, ya que son más rápidas que los procesos de pago mediante cheques o transacciones bancarias. Todas las transacciones realizadas en la red Blockchain se

⁸ Una wallet o monedero de criptomonedas es una cuenta que el usuario abre en una plataforma para poder almacenar sus criptomonedas, pero también para operar con ellas.

⁹ Podrían definirse de forma similar a las oficinas de cambios de divisas, su función es actuar como intermediarios entre los usuarios.

registran de forma permanente en los registros de todos los usuarios y los usuarios no tienen que preocuparse, a diferencia de los sistemas tradicionales, de los cobros revertidos que pueden ocasionar las transacciones.

Las criptomonedas tienen **acceso libre y abierto** a todas las personas. El Banco mundial estimó tras la realización de un estudio en los países menos desarrollados que el sesenta y cuatro por ciento de las personas no tienen acceso a servicios financiero básicos. Además, debido a las devaluaciones de las monedas, en algunos países las personas sufren una paralización financiera. Las criptomonedas ofrecen una solución alternativa a estos problemas por su fácil acceso desde cualquier parte del mundo.

Las criptomonedas blindan la **privacidad** de las personas para hacer transacciones. Uno de los puntos más destacables de las criptomonedas es su acceso público y con código abierto, que garantiza la seguridad de los usuarios para corroborar y verificar las transacciones. En los registros se detalla toda la información de las transacciones y lo vincula con un usuario mediante una dirección, pero no revela su identidad real, por lo tanto, mientras que el usuario no comparta su dirección, nadie podrá vincularle con las transacciones.

La única forma de acceder al dinero es mediante una clave privada, una contraseña criptográfica conocida únicamente por su poseedor, lo que significa, que ninguna entidad, ya sea un banco, corporación o gobierno puede manipular tus fondos.

La información de tus contraseñas nunca será conocida por los vendedores, a diferencia de las tarjetas bancarias, en las que al realizar un pago tienes que dar a conocer información con la que pueden robarte.

5.2.2 Desventajas:

La Volatilidad del precio de las criptomoneda es una de sus principales desventajas, de la misma forma que una persona puede ganar mucho dinero cuando el precio de las criptomonedas sube, también puede perderlo muy rápidamente cuando bajan.



Ilustración 7: Ciclo de emoción del mercado

Aunque se describa las criptomonedas como una forma segura de realizar operaciones financieras existe la posibilidad de **sufrir hackeos** en las terceras partes que trabajan con las criptomonedas, en los Exchange¹⁰ y monederos que veremos en apartados posteriores.

Además, el hecho de que las criptomonedas permitan realizar transacciones de forma anónima y privada, favorece su uso para la compra de actividades, servicios y productos mediante **transacciones ilegales**, como el terrorismo, la compra de drogas, o pagos en negro.

5.3 Monederos de criptomonedas



Ilustración 8: Wallet Criptomonedas

Como hemos comentado anteriormente, las criptomonedas pertenecen a una red de pagos descentralizada, lo que significa que no existen intermediarios, como bancos o empresas que influyan y por ende que realicen las transacciones de apertura de carteras.

¹⁰ Un Exchange de criptomonedas, es una plataforma cuya función básica es el permitir a los poseedores de criptomonedas intercambiarlas por otras o por dinero fiduciario (Crypto Economy, 2019)

Los usuarios pueden crearse tantas cuentas como quieran, estas cuentas son direcciones y cada una se asocia a una contraseña o clave privada que certifica quién es el propietario de dicha dirección y cuáles son las reservas que posee.

Para poder controlar los fondos y las cuentas es necesario que el usuario vincule su cuenta con un monedero de criptomonedas o “wallet”. Podemos definir los monederos de criptomonedas como softwares especiales que permiten al usuario mantener el control de sus cuentas y sus reservas de criptomonedas. Los monederos permiten no solo almacenar las monedas sino también realizar operaciones con ellas, ya sea de enviar o recibir criptomonedas de forma segura y sencilla. Hay muchas variantes de monederos, pero lo que todos tienen en común es la capacidad que ofrecen al usuario para el uso y disfrute de las criptomonedas.

5.4 ¿Cómo funcionan los monederos de criptomonedas?

Su funcionamiento podríamos decir que es similar al pago mediante PayPal, ya que utilizas tu correo electrónico como identificador único de usuario dentro del sistema. De esta forma puedes usarlo para realizar pagos, pero también para recibirlos.

En el caso de las criptomonedas se utiliza una dirección única e irrepetible para identificarte junto con una clave encriptada y privada que se genera automáticamente al iniciar la wallet.

Lo que almacenan realmente los monederos son los códigos privados necesarios para autorizar a realizar transacciones con las direcciones de criptomonedas asociadas.

Por lo tanto, un monedero o wallet de criptomonedas, es realmente una zona en la que se pueden almacenar claves privadas y que además realiza la función de una interfaz con capacidad para realizar transacciones sobre una Blockchain de la criptomoneda que usemos. Sus funciones nos permiten almacenar, enviar y recibir criptomonedas.

5.5 Tipos de monederos de criptomonedas

Existen una gran variedad de monederos, cada uno con sus propios beneficios y desventajas, cada usuario debe elegir cuáles de ellos utilizar adaptándolo a sus necesidades:

5.5.1 Monederos full wallet y lightweight wallet

Los monederos full wallet o monederos completos son lo que se descargan la totalidad de la cadena de bloques de las criptomonedas. Supone descargar la Blockchain completa y precisa de mucha capacidad de almacenamiento para ello (La Blockchain de

Bitcoin ocupa a rededor de los 250 GB). Uno de los principales full wallet y el primero que se creó es “Bitcoin Core”, y todos están relacionados con su desarrollo

Por otro lado, los lightweight wallet o monederos ligeros, almacenan la cadena de bloque parcialmente pero no la cadena en su conjunto. Al no descargar la cadena de bloques al completo como los full wallets ocupa mucho menos y necesita menos potencia computacional para poder funcionar, sin embargo, se recomienda para pequeñas cantidades de criptomonedas ya que no garantizan la seguridad y anonimato del usuario.

5.5.2 Hardware wallets



Ilustración 9: Wallet Criptomonedas

Los hardware wallets destacan por la seguridad que ofrecen al usuario para almacenar criptomonedas. Son dispositivos físicos que al igual que el resto de monederos, se usan para almacenar los códigos privados que permiten interactuar con las criptomonedas. Su creación tiene como fin garantizar la seguridad y privacidad de los fondos y proteger al usuario frente a robos y hackeos.

Son dispositivos fáciles de usar y transportar, los hay de diferentes formas, pero en general son dispositivos pequeños. Existen muchas marcas diferentes que ofrecen dispositivos para este tipo de servicio, pero las más destacables en el mundo de la seguridad cibernética y que son líderes en desarrollo son: Trezor, Ledger y Keepkey.

5.5.3 Papel wallets

Este tipo de monederos, únicamente almacena las claves privadas, pero no ofrece ningún tipo de acceso a la red de Bitcoin. Básicamente, los monederos de papel almacenan las claves en un papel, que o bien puedes guardar en un archivo o imprimirlo y guardarlo en un lugar seguro.

Es una forma un poco rudimentaria de almacenar claves, pero se considera muy segura ya que está libre de ciberataques y de fallos propios de hardware. (Bit2me, 2021)

5.5.4 “Hot wallet” y “cold wallet”

Los Monederos calientes o Monederos fríos no hacen referencia a tipos de Monederos sino a la forma de usarlos.

El monedero caliente o hot wallet es el de uso habitual por el usuario, tiene acceso rápido mediante el móvil o el ordenador y en ellos no se suele llevar la suficiente cantidad de dinero para que si sufres un ciberataque o un robo comprometa tu situación económica.

Ejemplo: Si una persona lleva en el monedero de su Smartphone 300 euros en criptomonedas, y de forma inconsciente descarga una aplicación que copia los datos de almacenamiento de todo el dispositivo, una persona malintencionada podría robar esos datos para robar las criptomonedas en cuestión de segundos sin que el usuario tenga consciencia de lo que está pasando. Normalmente, si ocurre esto, el usuario habrá tenido mala suerte pero su futuro no se verá comprometido porque la cantidad de dinero disponible en ese monedero no era demasiado elevada. (Recopilatorio de las mejores wallets de criptomonedas multiplataformas, 2021)

Por otro lado, el monedero frío o *cold wallet* se utiliza en la situación opuesta que le *hot wallet*, en él almacenas cantidades de dinero grande o ahorros, este tipo de monederos ofrecen una seguridad absoluta hacia los robos o ataques de cyber-seguridad, por esta razón su tecnología se desarrolla con softwares o hardware sin posibilidad de virus y sin conexión a internet.

5.5.5 Monederos HD

Los monederos Hd se utilizan para crear claves públicas, privadas y direcciones de criptomonedas, para explicarlo de forma sencilla, hd permite que a partir de un numero de diferentes dígitos y caracteres (un código) se formen muchos más ligados a él. Como si fuera un árbol, de un código salen muchas ramas y en cada una de ellas hay una clave pública, otra privada y una dirección de criptomoneda, de forma que un usuario puede sacar todas sus direcciones y claves de un mismo código y acceder a ellas en cualquier momento. (¿Qué son las HD Wallets?, 2021)

5.5.6 Monederos SPV

Monederos Simple Payment Verification, este tipo de monederos son una mezcla entre los monederos completos y los ligeros, ya que ocupan poco espacio, pero tienen la capacidad de verificar mediante la criptografía los datos recibidos para evitar sufrir un ataque al servidor.

Los monederos SPV tiene los atributos justos para permitir validar las transacciones sin depender de un tercero de confianza, como en el caso de los monederos ligeros que sería el servidor.

5.5.7 ¿Son seguros los monederos?

Es imprescindible mantener las criptomonedas de forma segura y para ello es necesario conocer para qué ocasiones se utilizan cada uno de las diferentes modalidades de monederos. La forma que tienen los usuarios de operar con sus criptomonedas es mediante las claves privadas, si estas se pierden, se corrompen o llegan a otro usuario, se perderá el control de las criptomonedas, por eso es imprescindible almacenar las claves privadas en un monedero de confianza.

En general los monederos considerados más seguros son los de papel porque dependen únicamente del usuario y del lugar donde guarde el papel impreso con los códigos, ahora bien, es un método mucho más rudimentario y lento que un monedero online, cada usuario debe elegir el tipo de monedero que se adecue a sus necesidades.

5.6 Legalidad de las criptomonedas

En el mundo existen 194 países, de los cuales, menos de media docena de ellos prohíben expresamente la compra, operación o tenencia de criptomonedas a sus ciudadanos y empresas.

En Bolivia y Argelia, por ejemplo, están prohibidos los Bitcoins y Altcoins por sus leyes nacionales. Sin embargo, en gran parte de los países del mundo no podemos definir a las criptomonedas como legales o ilegales, ya que sencillamente no tienen una regulación establecida o su legislación no contienen reglas específicas sobre ellas. Además, el hecho de que sean descentralizadas ha generado un halo de suspicacia injustificada en muchos casos.

A pesar de la ambigüedad legal de las criptomonedas en muchos territorios, lo cierto es que desde los inicios del Bitcoin en 2009, se han producido pequeños intentos legislativos de regular las criptomonedas.

El principal problema que tienen los estados es la complejidad para dar una definición clara sobre las monedas virtuales. Al ser de reciente creación los estados tienen mucha dificultad para incluirlas en las categorías jurídicas tradicionales, por esta razón existe un gran debate acerca de la naturaleza jurídica de las criptomonedas.

La Directiva UE 2018/843 (2018/843, s.f.) por la que se modifica la Directiva 2015/849 relativa a la prevención de la utilización de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, y por la que se modifican las Directivas 2009/138/CE y 2013/36/UE establece una definición de monedas virtuales como:

“representación digital de valor no emitida ni garantizada por un banco central ni por una autoridad pública, no necesariamente asociada a una moneda establecida legalmente, que no posee el estatuto jurídico de moneda o dinero, pero aceptada por personas físicas o jurídicas como medio de cambio y que puede transferirse, almacenarse y negociarse por medios electrónicos”.

Aunque gracias a esta definición ha sido posible dejar más claro los principales aspectos de las criptomonedas, no existe homogeneidad en la naturaleza de las monedas virtuales. Desde el punto de vista económico, aunque las criptomonedas se identifican con la definición de moneda, no se ajustan a las características del dinero fiduciario (JIMÉNEZ, 2021)

Tampoco puede considerarse las criptomonedas como dinero (definido en el artículo 2.2 de la Directiva 2009/110/CE del Parlamento Europeo y del Consejo de 16 de septiembre de 2009 sobre el acceso a la actividad de las entidades de dinero electrónico y su ejercicio) definido como el mecanismo de transferencia digital de una moneda.

El dinero electrónico tiene una relación directa con la definición de dinero tradicional, por lo que sí que está cubierto por una base legal y los fondos comprendidos en la misma unidad monetaria. A diferencia de las criptomonedas, que no cumplen dichos requisitos.

Desde el punto de vista legal, las criptomonedas tienen propiedades de activo y también de medio de pago, lo que hace complejo también su determinación y su aplicación de marco legal. (JIMÉNEZ, 2021)

En otros países como Estados Unidos, sí existe una regulación propia para las criptomonedas, pero en España todavía no existe.

La unidad de inteligencia financiera estadounidense considera las monedas virtuales como monedas, aunque estas no cumplan con todos los requisitos y atributos, por lo que le aplican la misma regulación. El regulador financiero estadounidense considera las

criptomonedas como el regulador del mercado de futuro e instrumento financiero, como un contrato de inversión. Otorga a las criptomonedas la consideración de “commodity.”¹¹

Muchos organismos se han posicionado por la regulación de la Directiva 2018/843; la Autoridad Bancaria Europea, el Banco Central Europeo o la Autoridad Europea de Valores y Mercados entre otros.

En España, como hemos comentado anteriormente, no existe una regulación aplicable a las criptomonedas aunque sí que podemos encontrar documentos sin rango normativo como consultas de la Dirección General de Tributos (DGT), avisos de la Comisión Nacional del Mercado de Valores (CNMV) y del Banco de España (BdE) o alguna resolución judicial como la sentencia de AP de Asturias de 6 de febrero de 2015 (Méndez, 2018)

La 5ª Directiva (UE) 2018/843 estableció como plazo máximo el pasado 10 de enero de 2020 para que los Estados Miembros adaptaran sus disposiciones legales, reglamentarias y administrativas para dar cumplimiento a lo establecido en la directiva. Cumpliendo con esta obligación, el pasado 13 de octubre de 2020 el Consejo de Ministros de España aprobó el proyecto de ley denominado “Ley de Medidas de Prevención de Lucha contra la Elusión Fiscal”. Con esta ley se pretende establecer controles estrictos sobre el uso de las criptomonedas con el objeto de evitar el fraude fiscal. Así, cualquier ciudadano español que opere con criptomonedas deberá comunicarlo de igual forma que si lo realizara con pagos en efectivo, es decir, cualquier tipo de pago que se realice con criptomonedas deberá ser declarado de la misma forma que lo es el pago con divisas. (Méndez, 2018)

En definitiva, las criptomonedas suponen una evolución y se mantendrán en el tiempo, por eso es necesario que se creen unas normas estrictas que las regule, para proteger tanto a la economía como las personas. Desde mi punto de vista creo que es muy necesario que los estados pongan punto y final a la falta de control sobre las criptomonedas, y deben regularse todos los aspectos que supongan un riesgo, por esta razón me parece que la regulación de las criptomonedas a través de la Ley de Medidas de Prevención de Lucha contra la Elusión Fiscal es un buen comienzo

¹¹ En Estados Unidos se utiliza esta calificación para hablar de las criptomonedas, su significado traducido es materia prima, pero realmente hace referencia a un bien destinado a su uso comercial producido por el ser humano.

6 Principales Criptomonedas

Tras la aparición de la primera criptomoneda, el Bitcoin, surgieron muchas nuevas criptomonedas. Actualmente existe una gran oferta de diferentes criptomonedas, aunque su número varía diariamente. Actualmente, el Bitcoin es la criptomoneda con más presencia en el mercado y con la cotización más alta.

A día de hoy, 28 de junio de 2021 existen más de 6000 criptodivisas diferentes, en el ranking, el primer puesto lo cubre Bitcoin, seguido de Ethereum, Tether y Binance Coin. La capitalización total del mercado de criptomonedas se sitúa en \$1,382,74,390,745 y el volumen en las últimas 24 horas \$75,953,334,566 (cryptocurrency, 2021)

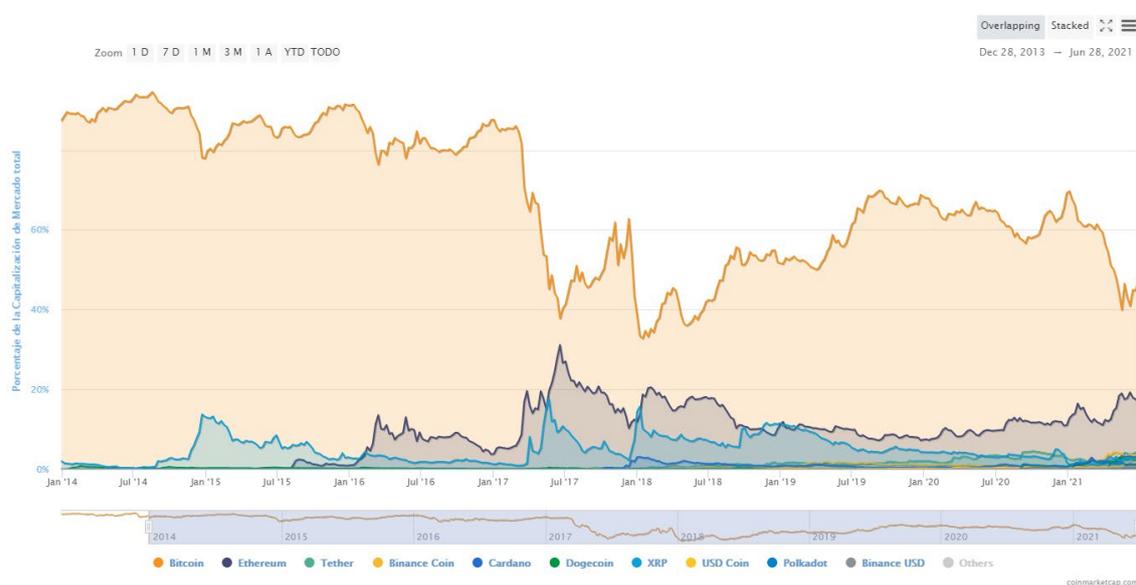


Ilustración 10: Porcentaje de capitalización de criptomonedas en el mercado total en los últimos 7 años (Porcentaje de la capitalización de mercado de las principales criptomonedas , 2021)

La grafica representa el porcentaje de capitalización de las criptomonedas principales en los últimos 7 años. Como podemos observar, el Bitcoin es la criptomoneda con más fuerza de mercado y ostentaba prácticamente todo el dominio del mercado hasta 2017, en el momento en que otras criptomonedas como Ethereum y XRP empezaron a aumentar su porcentaje de capitalización en el mercado. En 2017 el Bitcoin sufrió una bajada de casi un 50 por ciento de capitalización pasando de un 86% en febrero a un 34% en junio, mientras que, la segunda moneda más fuerte en ese momento y que continúa siéndolo aumentaba de un 4% a un 32%, la criptomoneda Ethereum.

El mínimo histórico registrado en porcentaje de capitalización de Bitcoin se produjo el 15 de enero de 2018, disminuyendo su porcentaje hasta un 32,81%. Esta bajada fue motivada por un endurecimiento en la política monetaria emitida por el Sistema de Reserva

Federal de los Estados Unidos, se tradujo en un incremento de las tasas de interés y afectó a prácticamente todos los activos financieros.

Tras la Bajada, Bitcoin recuperó su dominio de mercado hasta la actualidad, que sigue siendo la criptomoneda posicionada en número uno del ranking mundial.

#	Nombre	Precio	24h %	7d %	Cap. de Mercado	Volumen (24h)	Acciones en circulación	Últimos 7 días
1	Bitcoin BTC Comprar	\$34,452.70	-3.65%	-5.32%	\$646,784,954,233	\$34,271,829,971 993,206 BTC	18,743,993 BTC	
2	Ethereum ETH Comprar	\$2,083.30	-12.69%	-4.74%	\$243,307,276,421	\$23,154,128,219 11,084,323 ETH	116,475,839 ETH	
3	Tether USDT Comprar	\$1.00	-0.07%	-0.04%	\$62,546,048,856	\$55,617,822,581 55,607,235,102 USDT	62,534,142,511 USDT	
4	Binance Coin BNB Comprar	\$292.13	-5.22%	-4.13%	\$44,968,540,047	\$1,663,352,512 5,675,368 BNB	153,432,897 BNB	
5	Cardano ADA	\$1.34	-5.34%	-2.50%	\$42,720,074,238	\$2,393,740,297 1,790,053,381 ADA	31,946,328,269 ADA	
6	Dogecoin DOGE Comprar	\$0.2574	-5.43%	-15.41%	\$33,559,362,612	\$2,208,726,323 8,570,140,545 DOGE	130,214,617,895 DOGE	
7	XRP XRP	\$0.6428	-5.42%	-4.90%	\$29,759,375,470	\$2,249,535,515 3,495,660,882 XRP	46,244,517,593 XRP	
8	USD Coin USDC	\$1.00	-0.07%	-0.06%	\$25,954,479,334	\$2,031,187,493 2,030,734,810 USDC	25,948,694,963 USDC	
9	Polkadot DOT Comprar	\$15.28	-6.16%	-13.74%	\$14,637,839,933	\$952,904,621 62,213,104 DOT	955,673,251 DOT	
10	Uniswap UNI	\$17.68	-9.31%	-0.97%	\$10,215,099,456	\$283,636,715 15,972,110 UNI	575,231,223 UNI	

Ilustración 11: Ranking 10 principales criptomonedas por su capitalización en el mercado. (Principales 100 Criptomonedas por capitalización de mercado, 2021)

Podemos comprobar en la tabla de datos que las principales criptomonedas son Bitcoin, Ethereum, Tether y Binance Coin.

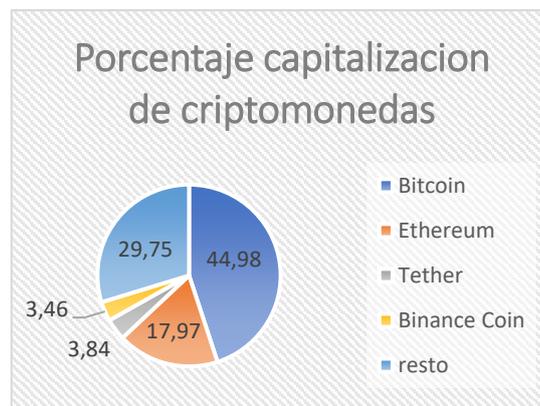


Ilustración 12: Porcentaje de capitalización de las criptomonedas.

A mitad del ejercicio de 2021, Bitcoin, Ethereum, Tether y Binance Coin representan el 70,25% del total de capitalización del mercado.

6.1 Bitcoin

6.1.1 ¿Qué es el Bitcoin?



Ilustración 13: Logotipo del Bitcoin

El Bitcoin es una moneda digital creada por un programador anónimo bajo el seudónimo de Satoshi Nakamoto, fue creada en 2008 mediante la utilización de un algoritmo matemático.

Las pruebas que se tienen sobre quién fue el creador del Bitcoin se sustentan en una serie de correos electrónicos: “Bitcoin: un sistema de efectivo electrónico usuario-a-usuario”. donde se propone la idea de crear un tipo de dinero criptográfico con control en cuanto a la generación de nuevas monedas y las transacciones que se realizan con él. Desde el momento de su creación el número de usuarios que se han añadido a esta comunidad ha aumentado exponencialmente, tanto los usuarios que realizan operaciones con ellos, como los desarrolladores que trabajan en su protocolo.

El protocolo de Bitcoin es público y cualquier usuario con conocimientos puede revisarlo, o bien crear su propia versión de software. Aunque los programadores realicen cambios en sus versiones, todas deben crearse bajo las mismas reglas, sino el sistema no será compatible con Bitcoin, por lo que tanto a los usuarios como a los programadores les interesa llegar a un consenso para que Bitcoin funcione correctamente.

Según el Banco Central Europeo: (¿Qué es el Bitcoin?, 2021)

“El Bitcoin se considera una criptomoneda. Las criptomonedas son esencialmente una unidad de valor digital que puede intercambiarse electrónicamente y que no existe en forma física. En lugar de una única autoridad u organización, una red de ordenadores crea y rastrea los Bitcoins utilizando fórmulas matemáticas complejas.”

Por lo tanto, no considera que las criptomonedas, o en este caso el Bitcoin deban ser aceptados como una moneda por varias razones, en primer lugar, no está respaldado por ninguna autoridad:

“No lo emite una autoridad pública central. Si usted tiene, por ejemplo, un billete de 10€, el BCE le garantiza su derecho a pagar con él en cualquier lugar de la zona del euro. Pero nadie le asegura su derecho a usar el Bitcoin, ni trabaja para mantener su valor estable.”

En segundo lugar, no lo considera un medio de pago, ya que generalmente no es aceptado en la mayoría de los establecimientos.

En tercer lugar, defiende que los usuarios no están protegidos, ya que se exponen a sufrir robos por piratas informáticos y no existe protección legal que lo respalde.

Por último, afirma que la volatilidad de las criptomonedas es muy elevada:

“Una moneda es un depósito de valor fiable, es decir, los ciudadanos deben tener la certeza de que con el dinero que tienen hoy podrán comprar aproximadamente las mismas cosas mañana o dentro de un año. El Bitcoin no es estable. Su valor se ha disparado y ha descendido vertiginosamente en pocos días.”

Por tanto,

“El Bitcoin es un activo especulativo. Dicho de otro modo, es una apuesta para obtener un beneficio, pero con el riesgo de perder lo invertido.”

Sin embargo, aunque el Banco Central Europeo no considere las criptomonedas monedas reales, muchos expertos defienden que sí se trata de un tipo de moneda:

Según Murad Mahmudov (Soriano, 2019):

“Bitcoin es algo que puede ser descrito con más de 100 definiciones y mucha gente debate acerca de ella, pero para mí, Bitcoin es principalmente, una nueva forma de dinero, una nueva forma de pensar sobre el dinero, sobre almacenarlo, transferirlo, organizarlo y entenderlo, y todo tipo de efectos financieros de segundo orden que surgen de aquí”.

Podemos concluir que la finalidad del Bitcoin es ser tanto una moneda digital como una red de pagos distribuida, sin una entidad central que lo controle ni intermediarios. A pesar de que el Bitcoin no tiene una autoridad central, es controlado por cada uno de los usuarios participantes. La emisión del Bitcoin está regulada por las leyes matemáticas sobre las que se sustenta el algoritmo criptográfico de Bitcoin configurado como un sistema de persona a persona mediante una red de ordenadores. El control de los Bitcoin no recae

sobre los gobiernos, entidades financieras o bancos centrales, sino en los usuarios (¿qué es Bitcoin?, 2020).

6.1.2 Valoración e historial de precios

El nacimiento del Bitcoin marcó un antes y un después en el desarrollo económico y tecnológico financiero, debido a su operatividad y el buen funcionamiento del algoritmo tecnológico se produjeron muchos cambios en la economía.

Los Bitcoin se valoran regidos por la ley de la oferta y la demanda, esto significa que si la demanda sube, el precio también subirá y viceversa. La confianza de los usuarios y el número de transacciones realizadas también afecta a su valoración, además del precio que los usuarios están dispuestos a pagar. Su funcionamiento es similar al resto de activos financieros.

El valor de los Bitcoins varía continuamente y al ser un sistema descentralizado sin respaldo del gobierno, no existe un precio oficial. En la gráfica expuesta a continuación podemos observar la variación del precio del Bitcoin a lo largo de los años, desde 2014 hasta la actualidad, 2021.



Ilustración 14: Variación del precio del Bitcoin

Cuando el Bitcoin nació, la cotización de la moneda era prácticamente nula, debido al desconocimiento generalizado sobre las criptomonedas y en este caso sobre el Bitcoin. Desde su lanzamiento en 2009 hasta la actualidad, el Bitcoin ha sufrido un gran desarrollo y su capitalización se ha incrementado exponencialmente.

El valor mínimo histórico del Bitcoin se produjo en septiembre de 2010, el precio por moneda si situaba en 0,04 euros. En el año 2011 el valor del Bitcoin alcanzó la cifra de 1 euro y al final de año la moneda ya valía 30 euros. En 2013 el valor del Bitcoin llegó hasta los 1000 Euros, pero como podemos observar en la gráfica, su valor sufrió una caída debido a un hackeo de la mayor casa de cambios del momento, en el que se perdieron 850 mil Bitcoins y su precio comenzó una caída progresiva hasta situarse por debajo de los 400 euros. (Matteo A. D., 2019)

EN 2013 se produjo el cierre forzado de una de las webs más grandes que comercializaban con criptomonedas, "Silk Road".

"Su principal operador, Ross Ulbricht, fue sentenciado a cadena perpetua por cargos asociados con la comercialización de drogas ilícitas, piratería informática y conspiración." (Matteo A. d., 2015)

Este acontecimiento supuso que muchas personas tomaran una decisión sobre si estaban a favor del uso de criptomonedas o no.

En 2014 muchas empresas con un potencial fuerte decidieron dar un paso hacia el desarrollo y adoptar como forma de pago los Bitcoin, alguna de las empresas fueron Microsoft, Dell o Newegg.

En 2017 China reconoció oficialmente el Bitcoin como medio de pago, a esta decisión se unieron otros países de la Unión Europea como Alemania y Francia. Además, en este mismo año el Bitcoin se incorporó por primera vez a la bolsa de Estados Unidos. Estos acontecimientos motivaron un incremento en el valor del Bitcoin alcanzando el diciembre de 2017 el precio por moneda de 16.727,68 Euros.

Tras alcanzar su máximo hasta el momento el diciembre de 2017, la cotización del Bitcoin empezó a disminuir hasta la cifra de 3.114,04 euros por moneda un año después. Hasta marzo de 2019, la cotización se ha mantenido medianamente estable, posicionando el valor de la moneda en torno a los 3.500 euros.

En el mes de abril de 2019 su valor empezó a incrementarse considerablemente llegando a valer 11.426 Euros en junio de 2019. En 2020 el valor del Bitcoin sufrió fluctuaciones entre los 5.000 y 10.000 euros.

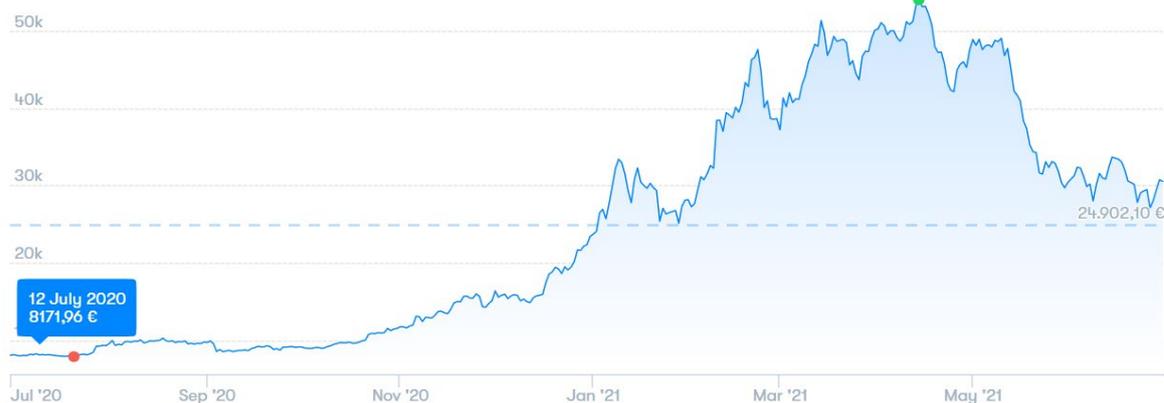


Ilustración 15: Variación precio Bitcoin en 2020-21

En septiembre de 2020, el valor del Bitcoin empezó a incrementar su valor hasta llegar a la cifra el 14 de abril de 53.981,84 euros, máximo histórico registrado hasta la actualidad. A día de hoy 30 de junio de 2021, el valor del Bitcoin se sitúa en 30.550,84 euros (Jansana, 2021)

Esta subida del precio del Bitcoin en el último año se debe a varios factores; en primer lugar, cada vez es mayor la percepción del Bitcoin como una reserva de valor:

“Bitcoin es una moneda deflacionaria por diseño. Se rige por un protocolo en el que se establece su funcionamiento y también su política monetaria: el límite de 21 millones de monedas que podrán existir no puede cambiarse o manipularse de ninguna forma para producir inflación inesperada, y la creación de nuevas monedas está programada para producirse a un ritmo muy lento (un 2.5% anual en este momento) y para cesar completamente en el futuro, hacia el año 2140, lo que hace de Bitcoin un activo cada vez más escaso.” (Ossa, 2021)

En Segundo lugar, muchas instituciones internacionales han visto el Bitcoin como un instrumento contra la inflación y las incertidumbres geopolíticas. Al ser el Bitcoin una moneda internacional, no se ve afectada directamente por las políticas monetarias de cada país.

En tercer lugar, la popularidad de los Bitcoins es cada vez mayor, e incrementa a gran velocidad, igual que su uso, propiciando un afán de compra entre los inversores.

6.2 Ethereum

6.2.1 ¿Qué es el Ethereum?



Ilustración 16: Logotipo Ethereum

Ethereum es un tipo de criptomoneda más compleja que los Bitcoins. Vitalik Buterin creó a finales de 2013 un tipo de criptomoneda descentralizada y colaborativa, que se dio a conocer a mediados de 2015.

Ethereum surgió de una innovación en los Bitcoins, pero tiene varias diferencias. En primer lugar, al igual que los Bitcoins, permite operar con dinero digital sin la necesidad de un intermediario como los bancos o los gobiernos, pero Ethereum es programable, lo que significa que no limita su uso a pagos y transacciones de dinero, sino que permite comercializar servicios financieros, juegos, aplicaciones... (¿Qué es Ethereum?, 2021)

Ethereum funciona de la misma forma que otras criptomonedas, todas las operaciones y transacciones realizadas se registran en un libro digital público, transparente e inviolable. El libro digital se denomina Blockchain y se lleva a cabo a través de la minaría de bloques.

La Blockchain de Ethereum es similar a la del Bitcoin, pero tiene diferencias, su software permite no solo gestionar transacciones sino también automatizar ciertos resultados. El software se conoce como contratos inteligentes.



Ilustración 17: Ejemplo contrato inteligente.

Un contrato tradicional describe las cláusulas y requisitos que deben cumplir ambas partes del acuerdo, un contrato inteligente se asegura de que dichas cláusulas sean cumplidas. Ejecutan de manera automática las condiciones fijadas en el contrato, eliminando el posible error humano y los retrasos que puedan ocasionarse. (Antonopoulos, 2018)

La idea sobre la que se crearon los contratos inteligentes puede aplicarse a muchas otras configuraciones, por lo que su potencial de uso es prácticamente ilimitado.

Otra de las aplicaciones que forman parte de Ethereum son las DApps. Estos son descentralizadas y son similares a los contratos inteligentes, pero tienen diferencias destacables. Igual que los contratos inteligentes, los DApps conectan mediante una interfaz a un usuario con un servicio de un proveedor, pero, mientras que los contratos inteligentes necesitan tener un mínimo de usuarios registrados, las DApps no. Además, las DApps permiten comercializar con todo tipo de activos objetos o servicios.

6.2.2 Valoración e historial de precios

Actualmente, el Ethereum es la segunda moneda con mayor cotización en el mercado después del Bitcoin. Ethereum tiene una capitalización de mercado de 228.939.729.247,95 Euros y su precio se sitúa el 4 de Julio de 2021 en 1975,43 euros. El total de acciones en circulación llega hasta los 1126.553.848. (El precio de Ethereum, 2021)

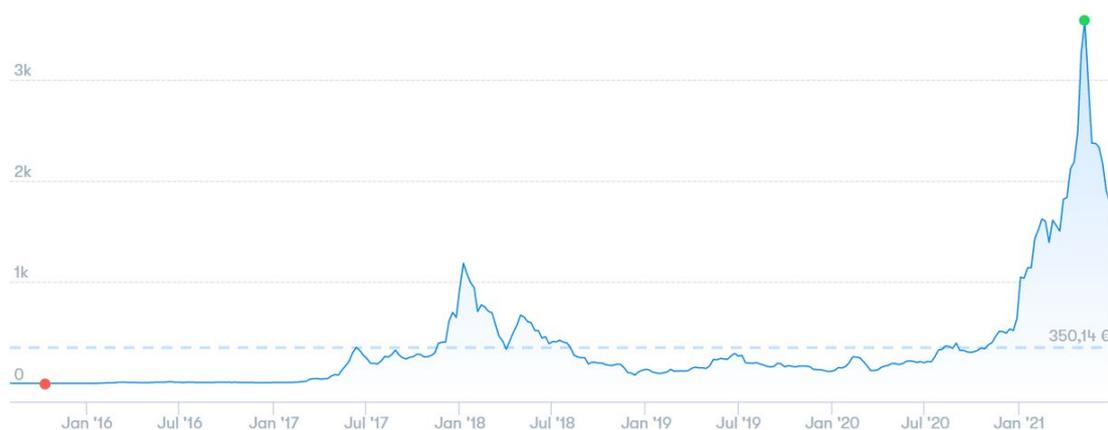


Ilustración 18: Evolución precio de Ethereum.

Como todas las criptomonedas Ethereum tiene un precio que fluctúa constantemente, se pueden realizar operaciones con la criptomoneda en cualquier

momento del día y a cualquier hora, ya que el mercado de las criptomonedas está abierto de forma continua.

Como podemos observar en el gráfico, el precio de Ethereum ha sufrido cambios sustanciales. El precio mínimo histórico registrado de Ethereum se dio en octubre de 2015, cuando su precio se situaba en 0,55 euros, este precio se mantuvo más o menos constante hasta junio de 2017, cuando su precio sufrió una importante subida llegando hasta los 350 euros. En enero de 2018 se produce una disminución de capitalización del Bitcoin, mientras que el resto de criptomonedas experimentaron una subida.

En 2018 año Ethereum alcanza el precio de 1187,08, esta tendencia de crecimiento disminuye rápidamente y Ethereum vuelve a sus valores habituales hasta que a finales de 2020 empieza a experimentar una gran subida que culmina en mayo de 2021, donde Ethereum alcanza su máximo histórico posicionando su precio en 3580,90 euros. Desde esta fecha, su valor ha sufrido una repentina bajada, a descendió hasta 1900 euros, 1600 euros menos. (ETHEUR Gráfico de criptodivisas, 2021)

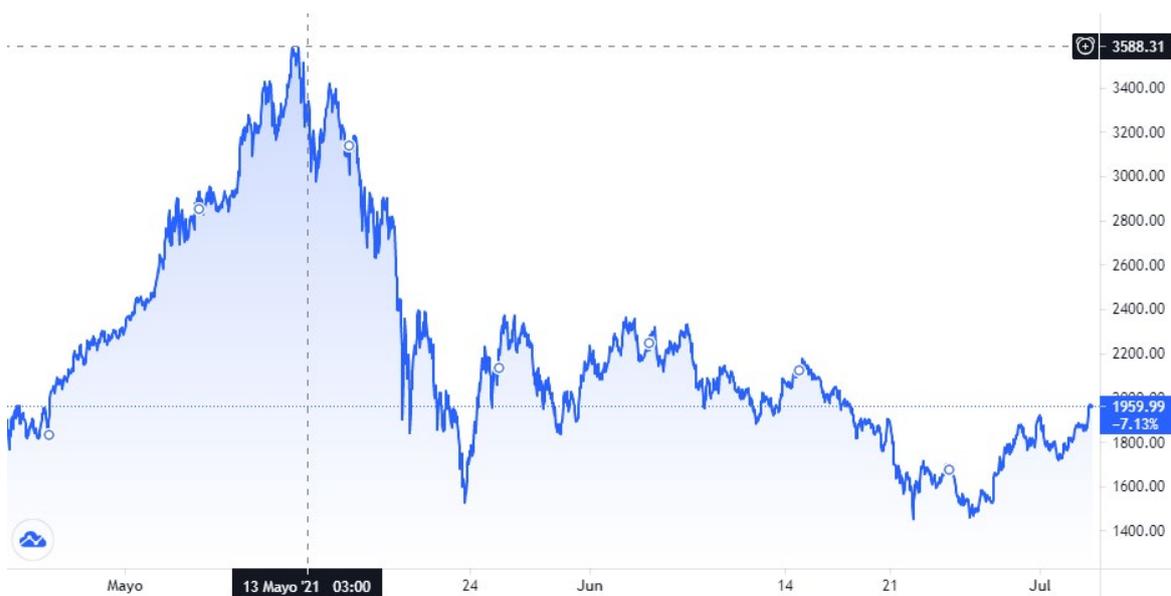


Ilustración 19: Precio Ethereum Mayo-Junio-Julio 2021

7 Perspectivas de las criptomonedas

7.1 Empresas



Ilustración 20: Pagos mundiales con criptomonedas

Tras la revalorización de las criptomonedas en 2017, cuando el Bitcoin aumentó su valor un 1550 por ciento, muchas empresas empezaron a formar opiniones sobre las criptomonedas y su inversión dentro de las empresas. Aunque el Bitcoin es la criptomoneda más conocida existe una gran variedad de criptomonedas virtuales.

Cada vez es más habitual el uso de las criptomonedas como medio de pago en algunos países como en China o en Estados Unidos, donde está permitido pagar incluso en las farmacias con criptomonedas. Aunque en España todavía no esté muy generalizado el uso de criptomonedas como forma de pago, es el quinto país con más cajeros de Bitcoins instalados, cuenta con 148 ubicaciones dentro del territorio nacional. (Cajeros automáticos de Bitcoin por país, 2021)

El uso de criptomonedas en las empresas puede reportar múltiples beneficios:

1. Permite agilizar las transacciones:

El uso de criptomonedas como forma de pago y de cobro resolvería muchos de los problemas que se plantean a las empresas a la hora de realizar transacciones, por un lado, permite que las transacciones sean instantáneas aunque se realicen desde países y horarios diferentes. Por otro lado, las transacciones realizadas por ejemplo con Bitcoin en la red Blockchain garantizan a las partes que la transacción es segura y no existe la posibilidad de revocar el pago.

2. Permite reducir los errores en las transacciones:

Las transacciones realizadas con criptomonedas en Blockchain son muy seguras y se almacenan los datos en registros públicos que permiten a los usuarios verificar todos los datos de las transacciones y detectar errores, además Bitcoin detecta los errores tipográficos y evita errores de envío de dinero a direcciones incorrectas.

3. Permite evitar costes de comisiones:

Uno de los grandes beneficios de operar con criptomonedas en la red Blockchain es que es un tipo de sistema descentralizado, independiente de organismos con autoridad, lo que hace posible que la realización de las transacciones se lleve a cabo sin comisiones de transacción o con unas comisiones muy reducidas en comparación con los sistemas tradicionales. De esta forma las empresas pueden ofrecer sus productos, servicios o activos financieros a un precio más reducido y competitivo.

4. Aumenta las posibilidades de captar nuevos clientes:
Cada vez es mayor el interés de las personas por los Bitcoins, esto puede ayudar a las empresas a mejorar su imagen frente a los competidores adaptando como forma de pago los Bitcoins u otras criptomonedas, dando una imagen renovada e innovadora de la empresa.
5. Permite crear incentivos a los trabajadores:
Muchas empresas se han unido recientemente al cambio de pagar a sus trabajadores con criptomonedas, esto puede ser un incentivo para muchas de las personas que estén interesados en invertir en ella a largo plazo para permanecer en la empresa.

Como podemos observar son muchos los beneficios que las criptomonedas pueden aportar a las empresas, sin embargo, la mayoría de ellas tienen reticencias con su uso debido a su gran volatilidad. Algunas de las empresas que aceptan como forma de pago las criptomonedas o en este caso el Bitcoin, ya que es el más generalizado, explican que no corren ningún tipo de riesgo porque no almacenan las criptomonedas, según reciben pagos con ellas, las vuelven a poner en circulación en el mercado. Usan las criptomonedas como una forma de pago alternativa para reducir el riesgo de sufrir fraudes o para agilizar las operaciones, pero no utilizan las criptomonedas como forma de inversión. (Bitcoin para empresas ¿Qué ventajas aportan las criptomonedas?, 2018)

Algunas de las empresas que ha incluido como forma de pago las criptomonedas son “Starbucks”, “Norwegia” (una compañía aérea) o “Destinia” (página web de reservas de hoteles, vuelos...)

Además de incluir las criptomonedas como nueva forma de pago en las empresas, otras han optado por crear sus propias monedas virtuales para evitar algunas regulaciones dictadas por entidades centrales de productos tradicionales como por ejemplo las acciones.

A cambio de las monedas que compran los inversores obtienen una participación en los beneficios, pero no tienen poder de decisión en las empresas a diferencia de las acciones. (García, 2018)

7.2 Bancos



Ilustración 21: Bancos o Criptomonedas

Las criptomonedas y la tecnología bajo la que se sustentan, Blockchain, pueden ser el camino al progreso del sistema financiero tradicional, sin embargo, todavía existen muchas dudas acerca de los riesgos que entrañan.

La criptomoneda más conocida es el Bitcoin, los creadores de dicha criptomoneda y del sistema que hace posible su funcionamiento fijaron la cantidad máxima de 21 millones de Bitcoin, lo que provoca una baja liquidez en la negociación y que los usuarios especuladores se aprovechen de esta situación. En el último año el valor del Bitcoin ha variado desde los 7998,48 euros a 53981,84 euros.

El Banco de España y la Comisión Nacional del Mercado de Valores han emitido un comunicado advirtiendo a los usuarios de los peligros que se asumen al invertir en criptodivisas. Explican en el comunicado que la subida del precio de criptomonedas como Bitcoin o Ethereum han ido acompañadas de publicidad agresiva para atraer a los inversores: (Sanchez, 2021)

“Se trata de instrumentos complejos, que pueden no ser adecuados para pequeños ahorradores, y cuyo precio conlleva un alto componente especulativo que puede suponer incluso la pérdida total de la inversión”

Ambas entidades, el Banco de España y la Comisión Nacional del Mercado de valores reconocen que las criptomonedas y el Blockchain pueden ayudar a modernizar el sistema financiero español, pero todavía hace falta que tengan una regulación propia sobre la que se puedan respaldar.

“Actualmente, se está negociando a nivel europeo un reglamento (conocido como MiCA) que pretende fijar normas para la emisión de cryptoactivos y los proveedores de estos servicios. El hecho de que no sean consideradas medios de pago, que carecen del respaldo de un banco central u otras autoridades públicas y que no están protegidos por

el Fondo de Garantía de Depósitos, la convierten en una inversión de alto riesgo. Además, existen productos derivados apalancados vinculados a criptomonedas que permiten invertir indirectamente en estos, lo que incrementa aún más su complejidad y la posibilidad de sufrir pérdidas superiores a la inversión inicial, por lo que requieren de un gran conocimiento y experiencia”.

Aunque algunos bancos expresan su opinión negativa hacia la inversión en criptomonedas, otros están aprovechando la oportunidad e incluyendo los servicios con criptomonedas. Alguno de los bancos que han adoptado las criptomonedas son las siguientes:

-A finales del 2020, el banco BBVA comunico que estaban empezando a realizarse las pruebas necesarias para lanzar su nuevo servicio que:

“permitirá gestionar transacciones en Bitcoins y tener depósitos con esta criptomoneda”. (BBVA lanza en Suiza su primer servicio comercial para la compra-venta y custodia de bitcoins, 2020).

-En mayo de 2021, la plataforma española “criptan”, de MasterCard lanzó una nueva tarjeta “CriptanCard” que permite pagar con criptomonedas en cualquier negocio físico u online del mundo que acepte MasterCard. (Criptan lanza, junto a Mastercard, una tarjeta para pagar con criptomonedas en cualquier establecimiento físico y online, 2021)

-PayPal es otra de las grandes entidades que se unen al uso de las criptomonedas incluyendo dentro de sus servicios pagar con criptomonedas, en concreto con Bitcoin, Litecoin, Ethereum o Bitcoin Cash.

En conclusión, podemos afirmar que, aunque algunos bancos son reacios a la adopción de las criptomonedas, otros están a favor, lo que significa que se está desarrollando una nueva mentalidad tomando conciencia de las ventajas que puede aportar el uso de criptomonedas a la actividad financiera.

7.3 Opinión general: El trilema de las criptomonedas

El mundo del Blockchain y de las criptomonedas ha sufrido muchos cambios a lo largo de su existencia, pero a pesar de las evoluciones todavía siguen existiendo tres dilemas que hacen que las personas no confíen en las criptomonedas y, por lo tanto, no muestren predisposición a su uso diario. La creación del Blockchain y de las criptomonedas ha hecho posible un sistema que podría desbancar al sistema financiero existente.

Para que el sistema de Blockchain pueda aceptarse como base de datos tiene que cumplir con tres premisas esenciales, ser un sistema descentralizado, seguro y escalado. Pero normalmente no se cumplen la totalidad de las premisas

“La estabilidad de los precios es uno de los pilares más importantes de una moneda y el Bitcoin nunca lo ha conseguido”

La criptomoneda más importante es el Bitcoin y cumple con dos de las tres premisas, es seguro y también descentralizado, pero no estabilizado.

El Bitcoin tiene una media de entre cinco y quince transacciones por segundo, un valor muy bajo comparado con las transacciones por segundo realizadas con el sistema tradicional de pago para ser una solución validada de pago mundial.

Muchas de las otras criptomonedas diferentes del Bitcoin también tienen problemas en cuanto a su seguridad, aunque la mayoría de ellas sí que son descentralizadas.

Para el Bitcoin, el último año ha sido muy destacable por sus fuertes fluctuaciones, su tendencia al alza en ventas y la subida del precio incluso por encima de la renta variable, e incluso alcanzar su máximo histórico registrado. Esta tendencia ha provocado que la imagen del Bitcoin quede dañada, ha evolucionado la perspectiva de las personas que antes pensaban que los Bitcoin eran una reserva de valor y ahora lo ven como un activo de riesgo. (Ruchti, 2021)

“El Bitcoin tiende a comportarse de la forma más parecida a un activo de riesgo que a un refugio seguro”

Aunque la fluctuación de la criptomoneda en el último año ha sido extrema y la más destacable en su historia, no es la primera vez que ocurre. Una de las características más importantes del dinero es su estabilidad de precios, sin embargo, el Bitcoin nunca ha conseguido un precio estable. Es habitual que las criptomonedas sufran cada aproximadamente 4 años un pico y después una fuerte bajada.

La rentabilidad de las criptomonedas y en concreto la del Bitcoin es muy elevada, sin embargo esta rentabilidad va muy ligada a un riesgo muy alto. La volatilidad del Bitcoin está estrechamente ligado con la demanda y cómo las criptomonedas no se unen a ningún valor real, la demanda evoluciona en la misma medida que el sentimiento de mercado. El sentimiento de mercado hace referencia a la confianza de los usuarios en el mercado.

Por lo tanto, las noticias o declaraciones sobre la evolución y el desarrollo de las criptomonedas hacen que sus tendencias cambien muy rápidamente. Por ejemplo si una persona referente en el mundo de las criptomonedas publica su opinión respecto a una

acción o generalidad, los inversores se verán afectados por esta evolución y actuarán en consecuencia cambiando la tendencia del mercado. (Lopez, 2020)

En 2015 se hizo viral la idea:

“El Blockchain podría cambiar cada faceta de cómo opera las compañías, tenemos que comprar criptos ahora mismo”

Provocando una subida del precio del Bitcoin multiplicándolo por veinte, sin embargo, más tarde se publicó:

“Dónde están todos los casos de uso revolucionario prometidos, tal vez el Blockchain no es el futuro”

El precio bajó alrededor de 20.000 dólares.

“La volatilidad del Bitcoin está impulsada casi por completo por la demanda”

Esta volatilidad tan elevada hace que entender el Bitcoin como una reserva fiable de dinero sea imposible.

7.4 Sectores más avanzados en el uso de las criptomonedas

Cada vez son más sectores lo que se están uniendo a la tendencia de incorporar las criptomonedas a su funcionamiento. Existen opiniones muy variadas a cerca de la adopción de las criptomonedas a la vida diaria, pero en los últimos años están saliendo a la luz nuevas herramientas accesibles y fáciles de utilizar que agilizan mucho los trámites que se llevan a cabo desde dentro de las empresas.

Las criptomonedas tienen la capacidad de potenciar el crecimiento social y económico en todo el mundo. Incluso en los países menos desarrollados, ya que el acceso es libre para todo el mundo.

Las criptomonedas pueden resultar muy útiles dentro de las empresas, en la actualidad ya está implantada toda una industria construida a partir de las criptomonedas, y cada una de las operaciones son supervisadas por instituciones en todo el mundo.

La industria de las criptomonedas se encuentra en crecimiento y puede actuar como un incentivo para crecer financieramente. Los sectores cada vez usan más las criptomonedas y el aumento de las aplicaciones y programas que se ponen a disposición de las personas hacen que cada vez haya más usuarios interesados.

El hecho de que más de un tercio de la población mundial tenga dificultades para tener servicios financieros a su disposición hacen de las criptomonedas un medio mucho más accesible y seguras para todo el mundo.

Como he comentado anteriormente, existen muchas aplicaciones y programas que facilitan el uso de las criptomonedas y hacen posible que un público más amplio pueda acceder a ellos.

Sumado a estos beneficios, las criptomonedas funcionan en un sistema descentralizado, sin dependencia de ninguna autoridad, y se puede ejercer en cualquier parte del mundo, independientemente de las barreras geográficas y horarias se puede operar sin restricciones.

El uso de tecnologías novedosas como Blockchain harán posible una nueva revolución financiera que provocará un aumento del uso de las criptomonedas, permitiendo a las personas mantenerse más conectados y habilitados financieramente.

Además, el sistema Blockchain y el pago de criptomonedas no suele tener comisiones por la realización de transacciones, este ahorro puede hacer posible una disminución del precio de los productos o servicios ofertados haciendo la empresa más competitiva.

El uso de las criptomonedas en los sectores tiene muchos beneficios y su uso no se limita únicamente a las compra y venta del activo.

El sector financiero está en proceso de cambio, hace poco tiempo los bancos eran reacios al uso de las criptomonedas, sin embargo, debido a la seguridad y la rapidez de las transacciones cada vez son más las instituciones bancarias que las incluyen en sus procesos.

En el caso de la industria de los casinos pasa algo similar, poco a poco han ido adaptándose a los cambios e introduciendo como forma de pago tanto en los casinos físicos como en las plataformas de juego las criptomonedas. Muchos de ellos han creado su propia criptomoneda.

En la industria musical el uso de las criptomonedas está haciendo posible eliminar a los intermediarios antes necesarios para vender su música. Utilizando las criptomonedas pueden vender directamente su música a los compradores de una forma segura y eficaz, destaca XRP, una criptomoneda dirigida a los creadores de contenido.

Estas tres industrias son las más destacables en cuando a uso de las criptomonedas, pero cada vez se unen más al cambio, como la industria del fútbol, el sector turístico o el inmobiliario. (Ramirez P. , 2021)

8 Proyección futura de las criptomonedas

Los cambios en los sistemas monetarios ha sucedido a lo largo del tiempo y surge la duda de si las criptomonedas serán realmente el dinero del futuro, ¿podrían realmente las criptomonedas sustituir al dinero físico?

A lo largo del tiempo, cada vez que ha habido un cambio en el tipo de dinero utilizado ha sido causado por un defecto que soluciona la siguiente generación de dinero, en este momento las criptomonedas ofrecen una solución válida para evitar la impresión ilimitada de dinero y su falsificación.

Desde el inicio de las criptomonedas muchos expertos han defendido que el futuro de las criptomonedas estaba limitado y pasaría rápidamente. A día de hoy, existen más de 6000 criptomonedas diferentes, lideradas por el Bitcoin. Su éxito ha hecho que aparezcan todo tipo de opiniones acerca de su uso, en un principio la mayoría eran negativas, pero en la actualidad cada vez hay más entidades y personas que deciden lanzarse al uso de criptomonedas.

En el mundo económico existen tendencias que sugieren que en un futuro la economía será criptográfica, la criptografía ofrece grandes beneficios y tiene el potencial de cambiar la forma de ahorro de las familias. Sin embargo, la desconfianza creciente de las personas supondrá un gran obstáculo que deberá superarse para lograr la evolución.

Cada vez existirán más programas, aplicaciones y servicios disponibles para las personas que facilitan el acceso y la manipulación de las criptomonedas provocando un aumento de los usuarios que invierten en este tipo de activos y, por ende, un aumento en la cotización de las criptomonedas, multiplicando por cinco su valor en el último año. (Figuera, 2021)

Además, existe un interés creciente por los gobiernos por crear una regulación específica para las criptomonedas, propiciando un aumento de la confianza de los usuarios. Podemos afirmar que el grado de aceptación de las criptomonedas es cada vez mayor.

La sociedad está cambiando y el desarrollo tecnológico creciente. Lo lógico es que el dinero también evolucione y ofrezca soluciones frente a la era digital.

El uso de las criptomonedas y el Blockchain no se limita únicamente a la compra y venta de ellas, también existen muchas de ellas que se utilizan como medio de pago de productos. También pueden usarse para conseguir inversión.

Aunque el uso de las criptomonedas en el futuro y de la red Blockchain puede aportar muchos beneficios, también tiene algunos retos que deben superarse en cuanto a su funcionamiento.

Algunos de los grandes retos son, disminuir el elevado gasto de energía que supone que el sistema funcione de forma correcta, también aumentar la velocidad de las transacciones y mejorar los sistemas de seguridad.

“Durante 10 años, las criptomonedas han recorrido un viaje increíble. Es muy difícil saber qué nos depara el futuro durante los próximos 10 años. Es casi seguro que prevalecerán en los sectores en los que sean útiles y aporten un valor añadido real. Cuando las tareas se realizan de forma económica, rápida, automática, sin la posibilidad de alterar nada y crear un sistema que no pueda ser atacado por piratas informáticos, entonces no habrá razón para que sigamos utilizando tecnologías falibles como las que usamos hoy.”

(Ramirez P. , 2021)

9 Conclusiones

Una vez analizado el mundo del Blockchain y las criptomonedas voy a exponer las conclusiones que he sacado de todo lo estudiado.

Vivimos en un mundo cada vez más desarrollado en el que las nuevas tecnologías cada vez son más potentes y permiten realizar más procesos. Una de las nuevas tecnologías que han surgido en los últimos años es la tecnología Blockchain, un sistema revolucionario aún en desarrollo que tiene la intención de ser el medio que facilite a las personas, almacenar, verificar y gestionar información.

La propuesta de Blockchain es llevar a cabo todo tipo de procesos mediante el uso de los ordenadores y la red online de forma segura, inescrutable, descentralizada y anónima.

Blockchain consigue protegerse gracias a su propia estructura, una cadena de bloques que contiene información, cada bloque puede tener información diferente, el ejemplo más conocido es el de Bitcoin, pero existen muchos otros.

Cada bloque contiene la información relativa a las transmisiones de criptomonedas, como quién es su emisor, cuánto dinero se envía, cuándo, desde dónde, a quién... pero también está compuesto del Hash, esto es un código aleatorio, cada bloque tiene dos hashes, uno de entrada y otro de salida que vincula el bloque con el anterior y con el posterior. De forma que crea una cadena.

La seguridad que ofrece Blockchain se debe que cada usuario tiene una copia de base de datos por lo que si necesita comprobar alguna información puede acudir a ella para verificarlo, además para que una transacción sea validada es necesario que todos los usuarios de la red verifiquen que la información es correcta.

Los usuarios pueden unirse a la red Blockchain para poder operar en ella o bien para crear nuevos bloques, los llamados mineros, a medida que se van realizando las transacciones es necesario que esta información quede registrada en la cadena de bloques, para ello los usuarios mineros tienen que resolver un problema matemático, el primero que lo resuelva será el encargado de minar el bloque. Para resolverlo hace falta una gran potencia computacional y al resolverlo obtienen una recompensa

En los inicios, el Blockchain pasó inadvertido hasta que el 2009 con la aparición del Bitcoin empezó a utilizarse, pero las utilidades de Blockchain pueden ser muy variadas, no se limitan únicamente para comprar y vender criptomonedas, sino que se pueden incorporar aplicaciones para hacer contratos, votar en elecciones, guardar registros médicos y bancarios. y muchas más utilidades que están aún por explotarse.

Blockchain es mucho más que una base de datos, es una herramienta con potencial de almacenar información fuera del sistema convencional, de forma descentralizada y anónima.

Gracias a la utilización de la criptografía los usuarios pueden mantener su anonimato, ya que las transacciones que realizan se enlazan con una dirección, de forma que se pueden rastrear todas las operaciones, pero no conocer la identidad del usuario.

La utilización de las criptomonedas en diferentes ámbitos puede aportar enormes beneficios, en las empresas, usar las criptomonedas como medio de pago hace que los pagos sean más rápidos y seguros, además, las pueden conseguir financiación creando sus propias criptomonedas a cambio de participaciones en la empresa. Las personas que decidan invertir en la empresa recibirá un porcentaje de las ganancias, pero a diferencia de las acciones no tienen poder de decisión sobre el futuro de la empresa.

El mundo del Blockchain y de las criptomonedas ha sufrido muchos cambios a lo largo de su existencia, pero a pesar de las evoluciones todavía siguen existiendo problemas que hacen que las personas no confíen en las Criptomonedas y por lo tanto no muestren predisposición a su uso diario.

“Cuando las tareas se realizan de forma económica, rápida, automática, sin la posibilidad de alterar nada y crear un sistema que no pueda ser atacado por piratas informáticos, entonces no habrá razón para que sigamos utilizando tecnologías falibles como las que usamos hoy” (Ramirez P. , 2021)

10 Bibliografía

2018/843, L. D. (s.f.). Obtenido de <https://bit.ly/3hAqcR0>

Antonopoulos, A. M. (12 de 11 de 2018). *ethereumbook*. Recuperado el 03 de 07 de 2021, de <https://bit.ly/3xAikEB>

BANCO CENTRAL EUROPEO. (12 de 05 de 2021). Recuperado el 29 de 06 de 2021, de <https://bit.ly/3k7oGr2>

BBVA. (09 de 12 de 2020). Recuperado el 03 de 07 de 2021, de <https://bbva.info/3r1FAIY>

Belinchón, F. (11 de Noviembre de 2020). Europa se prepara para regular las criptomonedas. *El País*.

Bit 2 me. (2021). Recuperado el 20 de 05 de 2021, de <https://bit.ly/3xDEmq6>

Bit2me. (2021). Recuperado el 2 de 06 de 2021, de <https://bit.ly/3AVNKHp>

Bit2me. (2021). Recuperado el 21 de 05 de 2021, de <https://bit.ly/3hwKsTm>

Bit2me, A. (2021). Recuperado el 20 de 05 de 2021, de <https://bit.ly/2UAWjH4>

Bitcoin. La moneda del futuro . (s.f.).

Bitcoin.org. (2020). Recuperado el 29 de 06 de 2021, de <https://bit.ly/3wyLtyw>

BTCdirect. (04 de 07 de 2021). Recuperado el 04 de 07 de 2021, de <https://bit.ly/36wQhdo>

Cajeros automáticos de Bitcoin por país. (03 de 07 de 2021). Obtenido de <https://bit.ly/3rgahKV>

coinmarketcap. (28 de 06 de 2021). Recuperado el 28 de 06 de 2021, de <https://bit.ly/3r5yhjq>

coinmarketcap. (28 de 06 de 2021). Recuperado el 28 de 06 de 2021, de <https://bit.ly/36st382>

Con Aval Sí. (05 de 004 de 2018). Recuperado el 03 de 07 de 2021, de <https://bit.ly/3xAEdDK>

Crypto Economy. (25 de Junio de 2019). Obtenido de <https://bit.ly/3yKgr8o>

Diario Bitcoin. (2021). Recuperado el 02 de 07 de 2021, de <https://bit.ly/3r4QSwm>

Díaz, G. (26 de 08 de 2018). *Criptonoticias*. Recuperado el 26 de 06 de 2021, de <https://bit.ly/2T74sCM>

Figuera, J. L. (4 de 07 de 2021). *Criptotendencia*. Recuperado el 05 de 07 de 2021, de <https://bit.ly/3xAiETP>

- García & Molekle. (2017). Dispenza.
- García, B. (18 de 01 de 2018). *blogthinkbig.com*. Recuperado el 03 de 07 de 2021, de <https://bit.ly/2T3id5h>
- Grange, E. (s.f.). Mesh World P2P Simulation Hypotesis.
- IBM. (2021). (IBM, Productor) Recuperado el 09 de 06 de 2021, de <https://ibm.co/3xvqga2>
- IG.com. (2021). Recuperado el 02 de 07 de 2021, de <https://bit.ly/3hveeYO>
- investing. (28 de 06 de 2021). Recuperado el 28 de 06 de 2021, de <https://bit.ly/2VzAhF9>
- Jansana, N. (17 de 07 de 2021). *bolsamania*. Recuperado el 30 de 06 de 2021, de <https://bit.ly/3xBwVPV>
- JIMÉNEZ, C. G. (2021). *El bitcoin y su tributación*. Recuperado el 01 de 07 de 2021, de <https://bit.ly/3ARExjw>
- Jurado, C. L. (17 de mayo de 2021). Breve Historia de las Criptomonedas. *CCM*, 2. Recuperado el 12 de 06 de 2021, de <https://bit.ly/3ALq08S>
- Libro Blanco EEcoins*. (s.f.).
- Lopez, F. C. (14 de 10 de 2020). *BBVA Next Technologies*. Recuperado el 04 de 07 de 2021, de <https://bit.ly/3r4S1UH>
- Marco Sanjuán, F. J. (s.f.). *Altcoin (criptomoneda)*. (Economipedia, Editor) Recuperado el 07 de 06 de 2021, de <https://bit.ly/3k4BxKF>
- Mastercard. (18 de 05 de 2021). Recuperado el 03 de 07 de 2021, de <https://mstr.cd/3AOoanX>
- Matteo, A. d. (30 de 05 de 2015). *diario bitcoin*. Recuperado el 30 de 06 de 2021, de <https://bit.ly/2VoF9wE>
- Matteo, A. D. (06 de 1 de 2019). *diariobitcoin*. Recuperado el 30 de 06 de 2021, de <https://bit.ly/3hE8wUF>
- Méndez, U. (2018). Monedas virtuales: aproximación jurídico-tributaria y control tributario. En *Actualidad Jurídica Uria Méndez* (págs. 72-81).
- Molano, N. A. (22 de 05 de 2019). *bbva*. Recuperado el 10 de 06 de 2021, de <https://bbva.info/2TY6Wne>
- Muñoz, M. (25 de 04 de 2021). *Bitnovo*. Recuperado el 12 de 06 de 2021, de <https://bit.ly/3xzh70l>

- Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. En *white book*. Recuperado el 13 de 06 de 2021, de <https://bit.ly/3kg1ruO>
- Ossa, J. F. (21 de 01 de 2021). *Grupo Colombia*. Recuperado el 30 de 06 de 2021, de <https://bit.ly/3hwKV84>
- Parrondo, L. (2018). Tecnología Blockchain, La nueva era para la empresa. *Revista de Contabilidad y Dirección*, 27, 11-31. Obtenido de <https://bit.ly/3xBGxdw>
- Pastor, J. (23 de 09 de 2018). *Xacata*. Obtenido de <https://bit.ly/3wFsSBa>
- Quintiliano, R. (21 de 04 de 2021). *bitnovo*. Recuperado el 12 de 06 de 2021, de <https://bit.ly/3xyHIKY>
- Ramirez, P. (26 de 04 de 2021). *Economía 3*. Recuperado el 05 de 07 de 2021, de <https://bit.ly/36w6Ztm>
- Ramirez, P. (14 de 04 de 2021). *Economía 3*. Recuperado el 04 de 07 de 2021, de <https://bit.ly/3e4A4QE>
- Ruchti, A. (28 de 06 de 2021). *El Español*. Recuperado el 04 de 07 de 2021, de <https://bit.ly/3kg3sqS>
- Sanchez, A. (09 de 02 de 2021). *El País*. Recuperado el 03 de 07 de 2021, de <https://bit.ly/3APxAPU>
- Savedra, A. (12 de 11 de 2019). *criptodinero*. Recuperado el 12 de 06 de 2021, de <https://bit.ly/3xCoCU5>
- Soriano, J. (27 de 09 de 2019). Co-Founder de Criptan. (P. Segarra, Entrevistador) *demineria.com*. Recuperado el 29 de 06 de 2021, de <https://bit.ly/3e8thoW>
- Tradingview*. (04 de 07 de 2021). Recuperado el 04 de 07 de 2021, de <https://bit.ly/36vOrta>