DOBLE GRADO EN DERECHO Y ADMINISTRACIÓN Y DIRECCIÓN DE EMPRESAS

FACULTAD DE CIENCIAS ECONÓMICAS Y EMPRESARIALES

TRABAJO FIN DE GRADO

CURSO ACADÉMICO (2019-2020)

TÍTULO:

LAS CRIPTOMONEDAS

AUTOR:

MIGUEL ÁNGEL ROMERO CUBERO

TUTOR:

JESÚS MARÍA SÁNCHEZ MONTERO

DEPARTAMENTO:

DEPARTAMENTO DE ECONOMÍA APLICADA I

ÁREA DEL CONOCIMIENTO:

MÉTODOS CUANTITATIVOS PARA LA ECONOMÍA Y LA EMPRESA

RESUMEN:

Estudio de la irrupción, funcionamiento y evolución de las criptomonedas en el mercado de divisas mundial, en concreto del Bitcoin como primera y principal moneda virtual, junto a Ethereum y Ripple. Están basadas en la criptografía como base al sistema creado para el desarrollo de las monedas virtuales, no muy aceptadas en el conjunto de los países tanto a nivel europeo como a nivel mundial.

PALABRAS CLAVE:

Dinero; Criptomoneda; Bitcoin; Blockchain; Minado.

ÍNDICE

CAPÍTULO 1: INTRODUCCIÓN.

1.1. INTRODUCCIÓN.

El estudio de las criptomonedas está indisolublemente vinculado con el dinero y la criptografía.

El dinero suele estar asociado con monedas, billetes o tarjeta de crédito de manera inmediata, ya que son las formas más conocidas en las que se manifiesta materialmente. Sin embargo, a lo largo de la historia se han empleado distintas técnicas pero que realizan la misma función. Hoy en día, el crecimiento del comercio electrónico ha convertido al dinero en algo intangible que cambia de manos con el simple traslado de números y claves. Se ha producido una transición del sistema basado en el patrón oro hasta el sistema fiduciario, basado en la confianza que la sociedad tiene en el Estado como garantizador del sistema monetario. La emisión y el control de este sistema está gestionado por organismos supranacionales, como el Fondo Monetario Internacional o el Banco Central Europeo. Será en el Capítulo 2 donde se estudie en profundidad el marco conceptual, justificado en una referencia histórica del dinero y su evolución hasta la actualidad, la definición de moneda y de criptomoneda.

Por otro lado, cabe destacar que la criptografía pretende proteger la información de determinados propietarios frente a terceros no legitimados para acceder a ella, así como impedir que se alteren en su perjuicio. Esta es la forma de garantizar la privacidad entre las partes y de asegurarse la veracidad de la información. La criptografía es uno de los pilares básicos en los que se fundamenta la tecnología Blockchain o Cadena de Bloques, la cual se estudiará en el Capítulo 4, con el análisis completo del funcionamiento, valoración, utilidad, riesgo e impacto económico del Bitcoin.

La unión de la criptografía y el dinero son el fruto de las criptomonedas, cuyo estudio se profundizará en el Capítulo 3: su historia, las razones que explican la creación de este tipo de monedas, las funciones principales de la criptografía, los elementos principales de las criptomonedas y las criptodivisas que dominan actualmente el mercado.

En el Capítulo 5 se hace un análisis de dos de las criptomonedas más fuertes junto al Bitcoin: Ethereum y Ripple, definición y valoración de ambas monedas, además de su comparativa con respecto a la criptomoneda principal.

En el Capítulo 6 se realiza una simulación real de una inversión en las criptomonedas estudiadas en los anteriores capítulos y el resultado obtenido con el paso del tiempo en las distintas criptodivisas. Finalmente, en el Capítulo 7 se recogen una serie de conclusiones personales.

El objetivo de este trabajo radica en profundizar en el estudio de las criptomonedas, una materia muy actual pero a su vez desconocida, por su falta de transparencia y por sus elevados riesgos. En especial, la finalidad radica en tratar de analizar en rigor el Bitcoin y sus principales magnitudes, para conocer esta moneda cada vez más distinguida, su funcionamiento y sus ventajas e inconvenientes a la hora de invertir en ella.

CAPÍTULO 2: MARCO CONCEPTUAL.

2.1. EL DINERO.

2.1.1. Breve referencia histórica.

El dinero puede definirse como todo activo o bien que es aceptado como un medio efectivo de pago o como una medición del valor para los intercambios que realizan los agentes económicos. La economía, mediante monedas y billetes, le da forma al dinero.

El dinero debe cumplir con tres propiedades básicas. En primer lugar, ser una unidad de cuenta, para poder fijar los precios de los bienes y servicios. Al utilizar el dinero como unidad de cuenta, se van a reducir los costes de transacción al disminuir el número de precios existentes en la economía y de esta forma se facilitan las operaciones comerciales. En segundo lugar, el dinero debe ser un medio de pago mediante el cual se hará posible la compra y la venta de los bienes de consumo y los servicios. Esta función distingue al dinero del resto de los activos financieros que existen en la economía. El dinero es válido para realizar transacciones de compraventa de bienes y servicios sin necesidad de cuestionarse su aceptación como forma de pago. En tercer lugar, el dinero debe ser un depósito de valor, esto es, el dinero debe conservar su valor a lo largo del tiempo pues debe posibilitar la compra de bienes y servicios futuros. El dinero es el activo más líquido.

El dinero surge en el neolítico con los excedentes de producción agrícola y ganadera. Ese excedente se ponía a disposición de las personas que no disponían de tierras o ganaderías, a cambio de otros productos a los que sí tenían acceso. Esta es la primera forma de comerciar y recibe el nombre de trueque, el intercambio directo de unos bienes por otros. Con el tiempo fue perdiendo eficacia y se comenzaron a acuñar las primeras monedas por el pueblo lidio entre el siglo V al VII a.C. Por lo tanto, el dinero surge por la intensificación de los intercambios comerciales y como alternativa al truque.

Desde la creación de las primeras monedas se usaron metales preciosos como el oro y la plata por la posibilidad de ser acuñados sin perder parte de su valor. Cada país usaba el patrón monetario que consideraba más oportuno. En la segunda mitad del siglo XIX se consolidó el patrón oro internacional, impulsado por Gran Bretaña, estando su centro en Londres, su capital. El periodo de máxima implementación fue desde que Estados Unidos lo asumió en 1897 hasta su finalización con la Primera Guerra Mundial. La emisión monetaria se basaba en las reservas de oro.

El segundo patrón monetario no se establecerá hasta 1944 en los Acuerdos de Bretton Woods y fue el patrón cambios-oro, que se basaba en la fortaleza del dólar americano a nivel internacional. El gobierno americano de Richard Nixon se encontró con el problema de que el dólar superaba a las reservas de oro que tenía el país, por lo que el sistema del patrón cambios-oro ya no era efectivo ni viable. Richard Nixon siguió las recomendaciones de Milton Friedman y eliminó la convertibilidad del dólar en oro puesto que la propia moneda tenía valor propio por el respaldo institucional del gobierno de los Estados Unidos. De esta forma, el 15 de agosto de 1971, Richard Nixon declaró de manera unilateral la inconvertibilidad del dólar en oro, rompiendo de esta forma con los Acuerdos de Bretton Woods. Es el inicio del actual sistema fiduciario.

En la actualidad, el patrón monetario y de relaciones entre las distintas monedas no se basa en acuerdos internacionales, aunque existe una cooperación jurídico-económica entre los distintos países. El sistema sigue un patrón fiduciario, basado en la fe o confianza de la comunidad: no se respalda por metales preciosos ni nada que no sea una promesa de pago por parte de la entidad emisora. El patrón fiduciario se basa simplemente en su declaración como dinero garantizado por el Estado.

2.1.2. Definición de moneda.

Una moneda se define como dinero de curso legal que es emitido por las entidades e instituciones oficiales de un país o de ámbito supranacional, como es el caso de la emisión del Euro en la Unión Europea, emitido por el Banco Central Europeo. La moneda está formada por un conjunto de elementos o instrumentos metálicos, además de en forma de papel, que sirven para realizar el pago en una operación comercial. Esta es su función principal.

Las funciones de las monedas están estrechamente vinculadas con las funciones o propiedades del dinero anteriormente identificadas, debido a que la moneda es la representación básica y fundamental del dinero, aunque pueden existir otros tipos de representaciones.

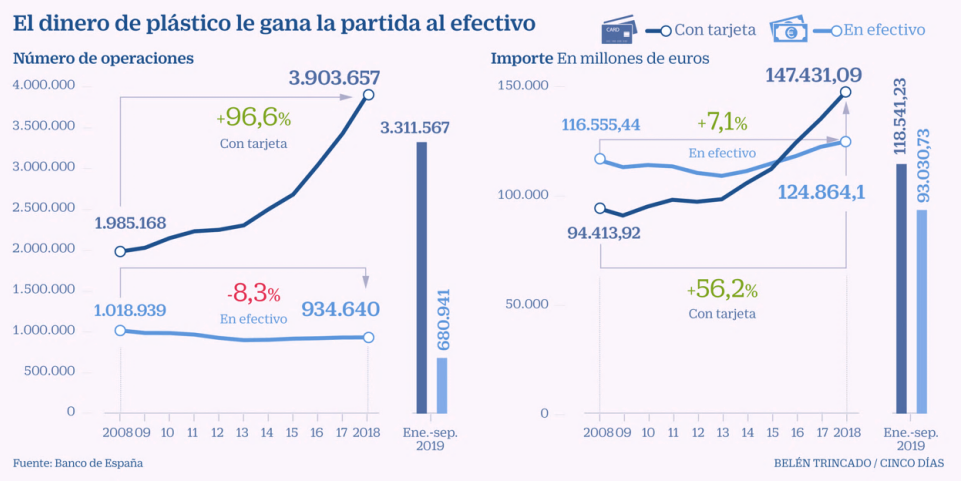
Las monedas deben ser:

- **Fungibles**. Las monedas deben poder intercambiarse entre ellas.
- **Duraderas**. Una moneda se debe repetir sin que conlleve un deterioro material de la misma.
- **Portable**. Las monedas deben tener la capacidad de que las personas puedan llevarla encima en cualquier momento para poder realizar operaciones comerciales con ellas.
- **Uniforme**. Todas las monedas que pertenezcan a la misma divisa van a tener el mismo valor y, por lo tanto, se tendrá la misma capacidad adquisitiva y de compra con ellas.
- **Deben tener limitada su oferta**. En el caso del Euro, su oferta está delimitada por el Banco Central Europeo, controlando la emisión de nuevas monedas como prevención a las inflaciones y devaluaciones de la moneda. La finalidad de la limitación de la oferta de monedas es que el valor de las divisas sea constante en el tiempo.
- **Aceptable**. Dar la posibilidad a cualquier persona de llevar a cabo operaciones comerciales con tan solo disponer de la moneda.
- **Divisible**. Es la capacidad que tienen las monedas o papel-monedas para ser dividida una misma cantidad en unidades más pequeñas, sin perder su valor.

2.1.3. Evolución del dinero.

El auge de la tecnología conllevará en un futuro a la desaparición del dinero físico. En la estadística sobre los pagos de 2018 emitida por nota de prensa el 26 de julio de 2019 por el Banco Central Europeo, se observa un incremento del 7,9% con respecto al 2017 en base al total de operaciones de pago realizadas con instrumentos distintos del efectivo en la zona euro. Los pagos con tarjeta supusieron el 46% del total de pagos efectuados distintos al físico y las transferencias y los adeudos directos supusieron el 23% cada uno.

Figura 2.1. El dinero de plástico le gana la partida al efectivo.



Fuente: Banco de España y Cinco Días.

En esta gráfica se puede observar cómo el dinero electrónico está desbancando al dinero físico. El número de operaciones que se realizan actualmente con tarjeta es muy superior a las realizadas con dinero en efectivo, quintuplicando su cifra (3.311.567 operaciones con tarjeta frente a las 680.941 operaciones en efectivo a cierre del tercer trimestre de 2019). A pesar de esto, no fue hasta el año 2016 cuando el importe de dichas transacciones con tarjeta no superó al importe de las efectuadas en efectivo.

En el tercer trimestre del 2019, las operaciones con efectivo descendieron un 4,13% hasta las 230.444, al igual que en el trimestre anterior. El importe retirado también decreció un 1,1% hasta los 32.304 millones de euros. Mientras tanto, el número de operaciones realizadas con tarjeta se incrementó un 16,8% hasta las 1.180.000 transacciones.

Los cambios en los hábitos de consumo llevarán a la desaparición del dinero físico, lo que propugna la generación de las nuevas monedas electrónicas y virtuales, las criptomonedas.

2.2. ¿QUÉ SON LAS CRIPTOMONEDAS?

La irrupción del e-commerce ha generado una nueva perspectiva con la que ver todos y cada uno de los aspectos de la vida cotidiana de las personas. Uno de estos grandes cambios ha sido la adaptación del dinero que tradicionalmente conocíamos en su forma material de moneda o papel moneda.

Antes de dar una definición exacta de qué son las criptomonedas, hemos de diferenciarla del dinero digital y del dinero virtual. El dinero digital o electrónico es aquel medio de pago que se almacena en un soporte electrónico. En este tipo de dinero se incluyen las tarjetas de crédito, de prepago o monederos electrónicos como el pago con el móvil, para el cual se requiere conexión a internet. En la misma línea, el dinero virtual es aquel que se emplea en ciertas instancias de la web, como en el caso de los videojuegos en el que se dan recompensas económicas con la que adquirir servicios en dicha instancia.

En la misma línea, es posible definir a las criptomonedas como una forma de intercambio utilizada por la criptografía con la que se pretenden asegurar las transacciones y controlar la creación de nuevas unidades de una manera descentralizada. Este tipo de moneda virtual, como el Bitcoin, no tiene un emisor concreto. Está protegida por la criptografía, que es el “arte de escribir con clave secreta o de un modo enigmático”. Su coherencia está salvaguardada por una comprobación de usuarios de manera global, pero su control está descentralizado, no tiene un respaldo bancario o institucional. Se basa en la criptografía para evitar la manipulación de sus miembros. Posteriormente se detallará un estudio de las criptomonedas más fuertes, en especial, del Bitcoin.

CAPÍTULO 3: LAS CRIPTOMONEDAS.

3.1. ¿CUÁNDO Y CÓMO SE CREAN LAS CRIPTOMONEDAS?

El origen de las criptomonedas se remonta a los años 70 con el movimiento Cypherpunk. Con anterioridad a esa fecha, la encriptación se usaba para motivos militares. Cabe destacar la máquina Enigma usada por las fuerzas armadas nazis antes y durante la Segunda Guerra Mundial, que permitía cifrar y descifrar mensajes.

La criptografía irrumpió en el mundo con la presentación de "Data Encryption Standard" por el Gobierno de los Estados Unidos y por el libro "New Directions in Cryptograpfy", de los doctores Whitfield Diffie y Martin Hellman. Pero no será hasta el año 1980 cuando se escriba por vez primera sobre el dinero digital anónimo y los sistemas de reputación seudónima. Fue el Dr. David Chaum con su publicación "Security without Identification: Transaction Systems to make Big Brother Obsolete". Supuso un gran paso para lo que hoy día se conoce como criptomoneda.

En 1992 un grupo de criptógrafos en San Francisco empezaron a trabajar en los cimientos de lo que sería la lista de correo Cypherpunk. A finales de ese año, Eric Hughes publicó "A Cyberpunk's Manifesto" plasmando los ideales del movimiento que había surgido. Abogaban por la necesidad de la defensa de la privacidad y el anonimato, para revelar lo que consideren conveniente en el momento oportuno, mediante la creación de sistemas anónimos basados en la criptografía.

En 1997 se crea HashCash como medida contra el spam. Al año siguiente, se ideó el concepto de proof of work que se analizará posteriormente. Años más tarde, en 2005, se publica una propuesta para Bit Gold, con la idea de valorar cada unidad de acuerdo con la cantidad de poder computacional que se requería para crearla. No será hasta 2008 cuando se publique, por Satoshi Nakamoto, el libro blanco del Bitcoin.

De esta forma, el movimiento Cypherpunk unido a la criptografía hizo nacer una moneda basada en la tecnología, garantizando la privacidad selectiva por la que abogaban los cypherpunks: el Bitcoin, la primera criptomoneda. En abril de 2011 surge Namecoin, la primera alternativa y en octubre de ese mismo año, Litecoin. Se diferencian con el Bitcoin en que utilizan script para prueba de trabajo en lugar de hash.

3.2. LAS RAZONES DE SU CREACIÓN.

Para conocer la razón principal de la creación de las criptomonedas hay que retrotraerse al pasado. En 2008 una dura grave crisis económica azotó a las finanzas de los Estados Unidos y se extendió rápidamente a todo el mundo, como consecuencia de la concesión de hipotecas de alto riesgo por parte de los bancos. Los expertos comenzaron a cuestionar la estabilidad y transparencia del sistema bancario global debido a los rescates, lo que llevó a la Gran Recesión. Los gobiernos se vieron obligados a rescatar a los bancos con el dinero de los contribuyentes, devaluándose la oferta de dinero existente.

Esa controversia llevó a la ideación de una moneda descentralizada, una innovación disruptiva, alejada del sistema tradicional que conllevó a tal desastre económico mundial. En lugar de estar controlada la moneda por un gobierno nacional o un banco central, estaría determinada por un protocolo, una serie de reglas que, en el caso del Bitcoin, sería un proof of work que regularía la emisión de monedas.

Esta es la principal razón que explica la creación de las criptomonedas como una nueva forma de dinero, dándole cierta independencia financiera y con vistas a crear una mejor sociedad para el futuro. Una moneda sin cadenas de transferencias y sin ningún equipo que tome decisiones que afecten a las personas que usan las monedas, sin intermediarios. Una moneda que le pertenezca a las personas que la usan y a nadie más.

3.3. FUNCIONES PRINCIPALES DE LAS CRIPTOMONEDAS O CRIPTOGRAFÍA.

Las criptomonedas garantizan su seguridad en la criptografía para tutelar la intimidad y asegurar el tráfico digital en la red de usuarios. Esto se consigue gracias a la matemática criptográfica para reemplazar el modelo basado en la intervención de terceros. De esta forma, es posible crear, almacenar y transferir datos informáticos de valor patrimonial o documental entre las partes.

Las funciones de la criptografía son cuatro: autenticación, intimidad, integridad e irrevocabilidad. Partiendo de la autenticación de la propia identidad, consiste en la forma digital que tiene una persona para demostrar válidamente que es ella, siendo una proyección externa de su intimidad, como la firma digital. En segundo lugar, asegurar que la información que se transmite entre las partes, receptor y emisor, sea privada y no se emita a terceros ajenos a dicha relación. En tercer lugar, el compromiso de que el mensaje enviado entre las partes llegue a su receptor sin alteraciones. En cuarto y último lugar, la irrevocabilidad o no repudio que permita comprobar que el remitente envió realmente el mensaje que ha llegado al receptor.

3.4. CARACTERÍSTICAS O ELEMENTOS PRINCIPALES DE LAS CRIPTOMONEDAS.

Jan Lansky pubicó en el 2018 “Possible State Approaches to Cryptocurrencies” en el que fijó una serie de condiciones para considerar a un sistema monetario como criptomoneda.

Las condiciones que estudió Jan Lansky son las siguientes:

a) Es un sistema descentralizado que no necesita una autoridad central para su control, que se basa en un consenso distribuido de manera global entre todos sus usuarios.
b) Es el propio sistema el que mantiene las unidades junto con sus propietarios.
c) Es un sistema que gestiona mediante protocolos específicos la emisión de nuevas monedas, determinando las circunstancias para ello.
d) La propiedad de cada moneda se asegura de manera criptográfica.
e) El sistema permite transferir las monedas entre los distintos propietarios, pero solamente cuando se pueda comprobar que la transacción es efectuada por el verdadero propietario. Esto se consigue mediante la firma digital y una serie de claves públicas y privadas.

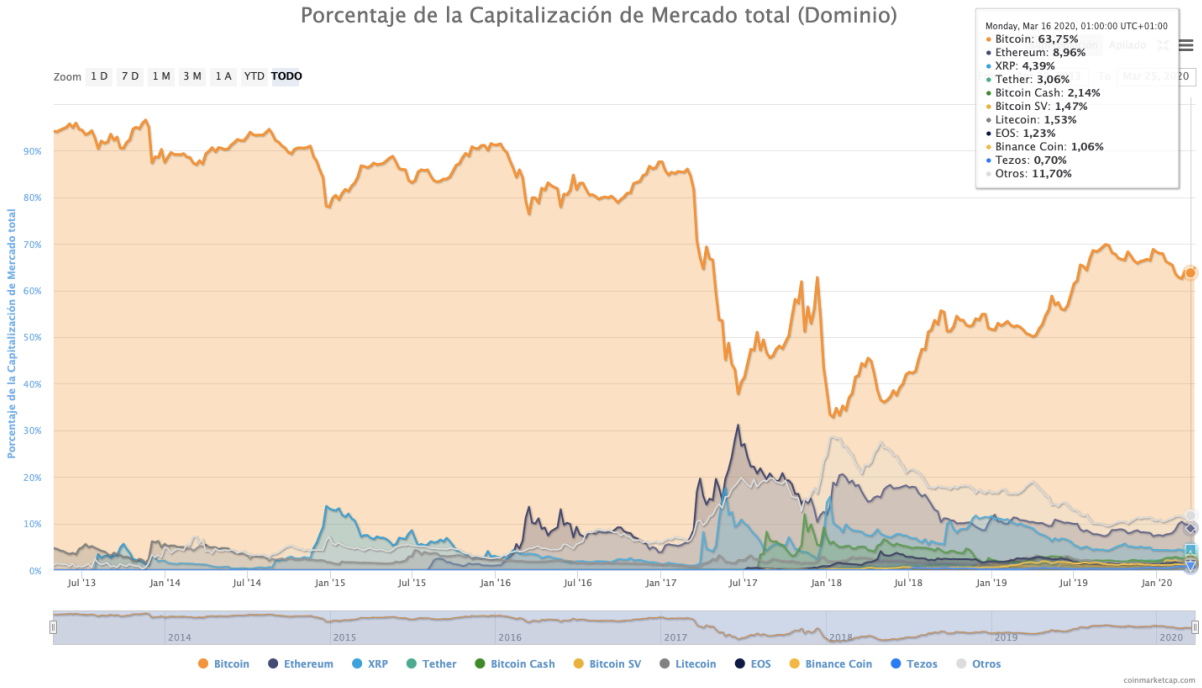
El sistema monetario que cumpla con estas seis condiciones será considerado como criptomoneda.

3.5. LAS CRIPTOMONEDAS MÁS FUERTES.

Actualmente existen una gran cantidad de criptomonedas. Desde la aparición de la primera criptomoneda, el Bitcoin, surgieron distintos proyectos que fueron creando sus propias criptodivisas. El número existente va variando diariamente pero la que domina el mercado es el Bitcoin, por ser la primera y por contar con la cotización más alta. A día de hoy, 25 de marzo de 2020, en el mercado existen un total de 2.796 tipos de criptodivisas, estando encabezado por: Bitcoin, Ethereum, Ripple y Tether. La capitalización de mercado total es de $185.256.643.347 y el volumen en las últimas 24 horas ha sido de $142.078.739.663.[1]

[1] Datos obtenidos de https://es.investing.com/crypto/currencies consultada el 25/03/2020.

Figura 3.1. Porcentaje de la Capitalización de Mercado total de los últimos siete años.



Fuente: www.coinmarketcap.com

La gráfica representa el porcentaje de capitalización de mercado total, es decir, el dominio que tienen las diferentes criptomonedas en el mercado global de criptodivisas. El Bitcoin es la moneda más fuerte de entre todas, su dominio es casi absoluto hasta el año 2017 en el que comienzan a emerger con fuerza otras criptomonedas, alcanzando ese año un gran decrecimiento en su porcentaje. En ese ejercicio, el Bitcoin decrece del 86,06% en febrero al 37,84% en junio de ese mismo año, ganándole un gran porcentaje la segunda criptomoneda más fuerte, Ethereum, con un 31,17% de capitalización.

En enero del 2018 se produce el mínimo histórico de capitalización del Bitcoin, llegando al 32,81% y siendo la capitalización de "otras criptomonedas" de 28,61% tan solo por debajo del Bitcoin. Este ejercicio fue complicado para casi todos los activos financieros, de acuerdo con un reportaje de CNBC. Esto ocurrió porque el Sistema de Reserva Federal de los Estados Unidos endureció la política monetaria con un enfoque de aumento de las tasas de interés. Por ello, casi todos los activos registraron un rendimiento negativo o sin grandes cambios durante el ejercicio, desde acciones en todo el mundo, deuda pública y bonos del Estado. No obstante, el Bitcoin no llegó a arrojar números rojos.

A mitad del ejercicio de 2018, el Bitcoin comienza a ganar capitalización en el mercado de criptomonedas hasta llegar a consolidar de nuevo su dominio mundial. Actualmente (última actualización, 25 de marzo de 2020), Bitcoin representa el 67,81% del mercado de criptodivisas, seguido con mucha distancia de Ethereum (8,36%), Ripple (3,93%), y Tether (2,24%).

Figura 3.2. Porcentaje de la Capitalización de Mercado total del último año.

Fuente: https://es.tradingview.com/markets/cryptocurrencies/global-charts/

Se puede confirmar que las cinco primeras criptomonedas representan un 82,34% del volumen de capitalización total a nivel mundial en el mercado de criptodivisas, lo que supone un 0,17% del número de criptomonedas existentes hoy (2.796 en total).

Las cinco principales monedas por volumen de 24 horas (Tether, Bitcoin, Ethereum, Bitcoin Cash y Litecoin) acumulan un total de $115.994.026.427, lo que supone un 83,13% del volumen total ($139.524.677.162). El volumen de 24 horas es el *"movimiento total del mercado en las últimas 24 horas, expresado en moneda fiduciaria"* (Miguel Arroyo, 25 de julio de 2018, párrafo 8).

CAPÍTULO 4: EL BITCOIN, LA CRIPTOMONEDA MÁS FUERTE.

4.1 ¿QUÉ ES EL BITCOIN?

4.1.1. Definición de Bitcoin.

El Bitcoin es una moneda digital creada en el año 2008 por un programador con el pseudónimo de Satoshi Nakamoto mediante un algoritmo matemático. Bajo dicho anonimato, Nakamoto publicó en 2009 la prueba del concepto en una lista de correo electrónico: "Bitcoin: un sistema de efectivo electrónico usuario-a-usuario". Desde aquel momento, la comunidad de usuarios se ha desarrollado exponencialmente.[2]

El Banco Central Europeo da una definición negativa de lo que es Bitcoin, ya que no lo encuadra en la definición de moneda. Lo considera como un activo especulativo en lugar de como moneda. Lo define en puridad como una "unidad de valor digital que puede ser intercambiada electrónicamente" (Banco Central Europeo, 13 de febrero de 2018, párrafo segundo). Lo define como un elemento virtual pero no como una moneda, dando las razones de que no goza de un respaldo institucional por una autoridad pública central, lo que no le permite tener un valor estable en el tiempo ni garantizar que los propietarios de estos activos puedan adquirir bienes de consumo con el valor que dicen representar. Además, establece que no es un medio de pago que sea aceptado generalmente porque su volatilidad es elevada y las monedas deben ser depósitos de valor fiable.

Sin embargo, expertos en criptomonedas defienden que el Bitcoin sí es una moneda y dan distintas definiciones del mismo. Murad Mahmudov, al respecto, señala que:

> 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 (párrafo 3).

Tal y como establece Iacopo Piersantelli, CEO de Cryptounify, el Bitcoin ha de tomarse como una moneda digital descentralizada que está conformada por una cadena de bloques o códigos denominada Blockchain, unos códigos que se transmiten a los distintos propietarios de esta moneda a través del protocolo Bitcoin y se consigue mediante la encriptación y el cifrado. Lo que se pretende con ello es evitar la duplicación. Ese mismo protocolo es el encargado de crear nuevas monedas y se hace mediante recompensas a los encargados de la validación de las transacciones, de mantener la seguridad global de la moneda y de añadir los bloques.

En el dominio oficial utilizado para la criptomoneda, se da una definición de Bitcoin centrada en dos puntos de vistas. Lo considera, por un lado, como una red consensuada y descentralizada de usuarios, que tiene la facultad de ser un sistema efectivo de pago y, por otro, como una moneda digital. Es un sistema de contabilidad de triple entrada que pretende superar las deficiencias del principio de partida doble y dar una mayor seguridad.[3]

Mientras que el sistema de partida doble se basa en la anotación contable de las transacciones en el debe y el haber, el sistema de triple entrada pretende separar los hechos de los pronósticos y así ganar fiabilidad en la información que se recoge. Esto se consigue mediante la tecnología blockchain, siendo un método para la contabilidad más accesible y rápido, con un alcance de información mucho mayor y más seguro, además de transparente.

En el sistema de triple entrada existen dos partes que deben estar de acuerdo con las transacciones anteriores y hay una tercera entrada que es tanto un recibo como una transacción. Todas ellas se ingresan en la cadena de bloque con la intención de que sea una prueba que pueda demostrar que la transacción se realizó correctamente entre las dos partes.

[2] https://bitcoin.org/es/faq#quien-creo-bitcoin consultado el 17/04/2020.
[3] https://bitcoin.org/es/faq#general consultado el 17/04/2020.

El Bitcoin, a pesar de no tener una autoridad central gubernamental que lo controle, es gestionado por cada uno de los usuarios que tiene en todo el mundo. Del mismo modo, los usuarios utilizan un mismo software implementado en las reglas del protocolo de Bitcoin y de esta forma son compatibles entre ellos. Para el correcto funcionamiento de Bitcoin, los usuarios deben estar en consenso y adoptar decisiones.[4]

Por ende, podemos concluir (Tulio Rosembuj, 2015) que el Bitcoin pretende una doble función, la de ser moneda digital y la de ser una red de pagos en línea distribuida, sin el respaldo de autoridades centrales monetarias ni intermediarios. Es una moneda cuya emisión está regulada por las leyes matemáticas de la criptografía, que se configura como un sistema peer to peer mediante una red de ordenadores con conexión a Internet. Es una moneda alejada de la ley y del control de los gobiernos, bancos centrales y entidades financieras.

4.1.2. Características del Bitcoin.

Las características fundamentales del Bitcoin son las que se detallan a continuación:

- **Moneda descentralizada**. El Bitcoin está respaldado por la matemática criptográfica y su valor se incrementa paulatinamente gracias a la confianza que los usuarios depositan en la moneda. Esto se mide con el crecimiento de usuarios, comerciantes y empresas que lo utilizan. A medida que su uso es mayor, el valor de la moneda será también mayor.[5]
- **Sin intermediarios**. "Lo que se necesita es un sistema de pago electrónico basado en la prueba criptográfica en lugar de la confianza, permitiendo la transacción directa entre dos partes que la quieran celebrar entre sí, sin necesidad de una tercera parte de confianza". (S. Nakamoto, 2008, p.1). De esta forma, se consigue un sistema autónomo e independiente de entidades financieras como intermediarios de las transacciones económicas realizadas entre particulares.
- **Privacidad absoluta**. Es controlado por el conjunto de los usuarios de Bitcoin siguiendo la misma tecnología que la del correo electrónico. No tiene propietarios que puedan recibir información confidencial de los participantes. No obstante, los programadores tienen la facultad de mejorar el software, dentro de las posibilidades que se establezcan en el protocolo del Bitcoin ya que todos deben seguir las mismas reglas para que su funcionamiento sea correcto en todos los usuarios.
- **Transacciones irreversibles**. Las transacciones realizadas con bitcoins no admiten devoluciones ni cancelaciones, se quedan registradas en la cadena de bloques y, al ser sucesivos todos los bloques, no cabe modificación alguna de los mismos. Esta es una característica esencial tanto del Bitcoin como de las demás criptomonedas debido a que, como no tienen un respaldo institucional, se pretende darle una seguridad especial.
- **Cambiar Bitcoin por divisas**. Al igual que el resto de las divisas, existen los *exchanges* en los que los usuarios pueden cambiar sus bitcoins por monedas tradicionales como el euro o el dólar y viceversa. Su funcionamiento es análogo al de cualquier mercado financiero como las bolsas o los mercados de divisas.
- **Imposible falsificar**. No cabe la falsificación debido a que los usuarios tienen el control absoluto sobre los pagos y cobros, que habrán de aprobarse previamente.[6]
- **La cotización no se detiene**. El Bitcoin no tiene un precio fijo sino que va variando a medida que se efectúan los intercambios internacionales durante las 24 horas del día ya que no hay apertura o cierre como en los mercados bursátiles.[7]

[4] https://bitcoin.org/es/sobre-nosotros consultado el 17/04/2020.
[5] https://bitcoin.org/es/faq#como-se-crean-los-bitcoins consultado el 17/04/2020.
[6] https://bitcoin.org/es/faq#es-bitcoin-util-para-actividades-ilegaleshttps://bitcoin.org/es/faq#es-bitcoin-util-para-actividades-ilegales consultado el 17/04/2020.
[7] https://btcdirect.eu/es-es/precio-bitcoin consultado el 17/04/2020.

A continuación se muestra una tabla comparativa de las características del Bitcoin, del euro (dinero en efectivo) y del oro (como el activo con mayor valor donde se respaldaba anteriormente el valor de las monedas).

FIGURA 4.1. Características del dinero.

CARACTERÍSTICAS DEL DINERO	ORO	EFECTIVO (EURO)	CRYPTOMONEDA (BITCOIN)
Fungible (intercambiable)	Alto	Alto	Alto
No desgastable	Moderado	Bajo	Alto
Portabilidad	Moderado	Alto	Alto
Durabilidad	Alto	Moderado	Alto
Divisibilidad	Moderado	Moderado	Alto
Infalsificable	Moderado	Moderado	Alto
Fácilmente manejable	Bajo	Alto	Alto
Escaso (suministro predecible)	Moderado	Bajo	Alto
Emitido por Gobiernos	Bajo	Alto	Bajo
Descentralizado	Bajo	Bajo	Alto
Inteligente (programable)	Bajo	Bajo	Alto

Fuente: Elaboración propia a partir de los datos obtenidos en www.academy.bit2me.com [8]

4.2. EMISIÓN Y VALORACIÓN.

4.2.1. Emisión y obtención de bitcoins.

La emisión o creación de los bitcoins se realiza vía Internet por los agentes especiales conocidos como "mineros" que disponen de un programa informático que persigue dicho fin, además de verificar las transacciones realizadas con bitcoins, recibiendo una compensación como contraprestación. Como resultado, se van generando nuevos bitcoins y se introducen en el mercado. El conjunto de mineros en todo el mundo crea una red sólida que hace del Bitcoin una moneda segura y a la vez descentralizada.

La minería queda recogida dentro del protocolo Bitcoin y está diseñada para que la moneda se cree con un ritmo fijo, haciendo de ella una actividad muy competitiva puesto que a mayor número de mineros en la red, menor es la posibilidad de conseguir bitcoins. El ritmo de emisión de la emisión está previamente determinado debido a que existe un límite máximo de monedas en circulación, 21 millones de bitcoins. Por esta razón, los bitcoins se van creando con un ritmo decreciente, reduciéndose a la mitad paulatinamente y así hasta que se paralice su emisión al llegar al límite, siendo un proceso que se prevé que finalice en el 2140 cuando se alcance la cifra de los 21 millones.[9]

[8] https://academy.bit2me.com/precio-bitcoin/ consultado el 18/04/2020.
[9] https://bitcoin.org/es/faq#como-se-crean-los-bitcoins consultado el 18/04/2020.

Según Tulio Rosembuj (2015) los mineros se encargan de respaldar la cadena de transacciones, recogiéndolas en bloques y verificando que se dan las condiciones de validez. Una vez hecho esto, se incluyen en orden cronológico en la Cadena de Bloques o Blockchain que es un registro público y oficial que se estudiará con profundidad en el apartado 4.3.1 del trabajo. Lo que se pretende con ello evitar el problema del *"double spending"* que consiste en gastar el mismo bitcoin en más de una operación, algo totalmete prohibido.

Haciendo referencia a lo expuesto anteriormente, los mineros reciben bitcoins a cambio de este trabajo. De ellos depende añadir o rechazar las transacciones en los bloques. Para verificar las transacciones, deben resolver un problema matemático y comunicarla a los demás mineros de la red y estos la aceptarán o la modificarán en el caso de contar con errores. Una vez que se han confirmado por una mayoría, se introducen las transacciones como nuevo bloques en Blockchain.

El añadido de nuevos bloques por parte de los mineros conllevaba en un principio una recompensa de 50 bitcoins pero esto va decreciendo gradualmente y se encuentra regulado en el libro blanco de Bitcoin. El 28 de noviembre de 2012 se redujo la recompensa a la mitad, 25 bitcoins, y actualmente se encuentra en 12,5 bitcoins por bloque. Esa recompensa por bloque recibe el nombre de halving.

Figura 4.2. Limitación en la emisión de bitcoins.

Bloque	Era recompensa	BTC/Bloque	BTC inicio	BTC añadido	BTC finales	%BTC del límite en circulación
0	1	50,00000000	0,000000	10.500.000	10.500.000	50,00000000%
210000	2	25,00000000	10500000,000000	5250000	15.750.000,000000	75,00000000%
420000	3	12,50000000	15750000,000000	2625000	18.375.000,000000	87,50000001%
630000	4	6,25000000	18375000,000000	1312500	19.687.500,000000	93,75000001%
840000	5	3,12500000	19687500,000000	656250	20.343.750,000000	96,87500001%
1050000	6	1,56250000	20343750,000000	328125	20.671.875,000000	98,43750001%
1260000	7	0,78125000	20671875,000000	164062,5	20.835.937,500000	99,21875001%
1470000	8	0,39062500	20835937,500000	82031,25	20.917.968,750000	99,60937501%
1680000	9	0,19531250	20917968,750000	41015,625	20.958.984,375000	99,80468751%
1890000	10	0,09765625	20958984,375000	20507,8125	20.979.492,187500	99,90234376%
2100000	11	0,04882813	20979492,187500	10253,9063	20.989.746,093750	99,95117188%
2310000	12	0,02441406	20989746,093750	5126,95313	20.994.873,046875	99,97558594%
2520000	13	0,01220703	20994873,046875	2563,47656	20.997.436,523438	99,98779297%
2730000	14	0,00610352	20997436,523438	1281,73828	20.998.718,261719	99,99389649%
2940000	15	0,00305176	20998718,261719	640,869141	20.999.359,130859	99,99694825%
3150000	16	0,00152588	20999359,130859	320,43457	20.999.679,565430	99,99847413%
3360000	17	0,00076294	20999679,565430	160,217285	20.999.839,782715	99,99923707%
3570000	18	0,00038147	20999839,782715	80,1086426	20.999.919,891357	99,99961854%
3780000	19	0,00019073	20999919,891357	40,0543213	20.999.959,945679	99,99980927%
3990000	20	0,00009537	20999959,945679	20,0271606	20.999.979,972839	99,99990464%
4200000	21	0,00004768	20999979,972839	10,0135803	20.999.989,986420	99,99995232%
4410000	22	0,00002384	20999989,986420	5,00679016	20.999.994,993210	99,99997616%
4620000	23	0,00001192	20999994,993210	2,50339508	20.999.997,496605	99,99998808%
4830000	24	0,00000596	20999997,496605	1,25169754	20.999.998,748303	99,99999405%
504000	25	0,00000298	20999998,748303	0,62584877	20.999.999,374151	99,99999703%
5250000	26	0,00000149	20999999,374151	0,31292439	20.999.999,687076	99,99999852%
5460000	27	0,00000075	20999999,687076	0,15646219	20.999.999,843538	99,99999926%
5670000	28	0,00000037	20999999,843538	0,0782311	20.999.999,921769	99,99999963%
5880000	29	0,00000019	20999999,921769	0,03911555	20.999.999,960885	99,99999982%
6090000	30	0,00000009	20999999,960885	0,01955777	20.999.999,980442	99,99999991%
6300000	31	0,00000005	20999999,980442	0,00977889	20.999.999,990221	99,99999996%
6510000	32	0,00000002	20999999,990221	0,00488944	20.999.999,995111	99,99999998%
6720000	33	0,00000001	20999999,995111	0,00244472	20.999.999,997555	99,99999999%
6930000	34	0,0000000	20999999,997555	0,00122236	20.999.999,998778	100,00000000%

Fuente: elaboración propia a partir de los datos de cointelegraph.com[10]

En la tabla se observa la regulación que hizo Satoshi Nakamoto a la hora de crear el Bitcoin para controlar de esta forma su emisión, reduciendo las recompensas de los mineros cada 210.000 bloques, cosa que ocurre cada 4 años aproximadamente.

10 https://es.cointelegraph.com/explained/what-is-halving-the-reward-for-a-block-and-its-impact-on-bitcoin consultado el 18/04/2020.

Actualmente, el Bitcoin se encuentra en su tercera era al llegar a los 420.000 bloques en la Blockchain, siendo la recompensa de 12,5 BTC por cada bloque publicado, y estando su cantidad entre los 15.750.000 y los 18.375.000 BTC. Concretamente, hay un total de 16.522.800 BTC en circulación, lo que supone el 78,68% del total.[11] Una vez que se superen los 6.930.000 bloques, en la era 34, la recompensa será de 0 BTC y se habrán alcanzado el límite de 21 millones en circulación. De ahí que los mineros, a medida que va pasando el tiempo, deban aumentar su eficiencia, reduciendo costes para aumentar sus beneficios.

La creación de los bitcoins por los mineros no es la única forma de obtenerlos. Al igual que se realiza en el mercado de divisas, los usuarios pueden cambiar moneda legal por bitcoin u obtenerlas a través de la compraventa de bienes o servicios. Las criptomonedas alcanzadas por una de estas formas se guardan en un billetero que tiene cada usuario en su plataforma digital. El billetero o monedero se analizará con más detenimiento posteriormente.

4.2.2. ¿Cómo se valora el bitcoin?

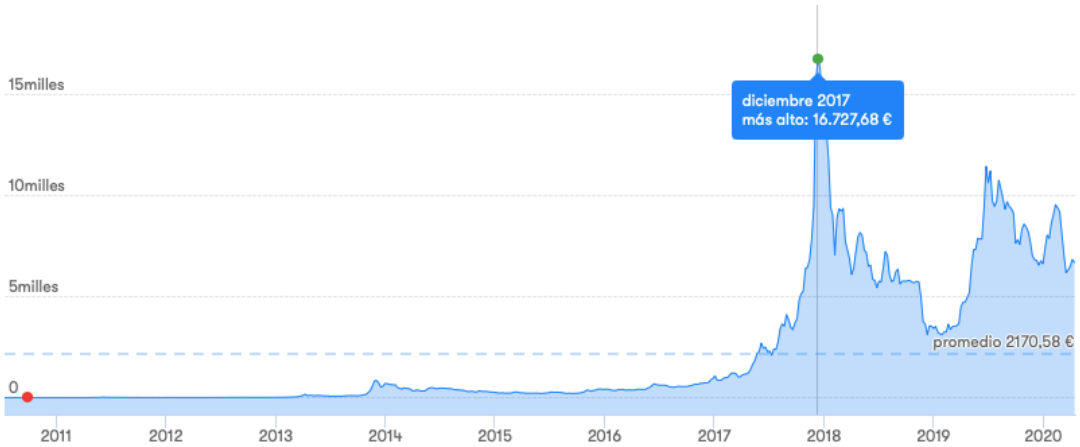
El valor del Bitcoin está determinado por la ley de la oferta de la demanda. A medida que sube la demanda, el precio se incrementa. Es el principal factor pero no el único, ya que influye la confianza o el número de transacciones. Además, el precio es el que los compradores estén dispuestos a pagar. Al fin y al cabo, funciona como cualquier otro activo financiero e incluso alimentos como la fruta: a menor oferta de naranjas y mayor demanda, el precio se incrementará. Otros de los factores que influyen es la limitación en la emisión y las recompensas (halving).

El valor de esta moneda varía a cada instante pero al ser un sistema descentralizado y no tener respaldo gubernamental, supera las carencias del dinero fiduciario: la hiperinflación, la distribución poco transparente y la producción inorgánica. Por esta razón, no hay un precio único y oficial del bitcoin aunque las casas de cambios mundiales tienden a equipararlos; va a depender de la capacidad para acceder a ellas. Las casas de cambios sitas en Alemania impondrán un precio menor que las establecidas en África, debido a que la accesibilidad es mucho más compleja en el segundo caso.

4.2.3. Historial de precios.

El precio del Bitcoin no es fijo sino que va alterándose momentáneamente pues, como se mencionó anteriormente, depende de factores como la oferta y la demanda. En la siguiente gráfica se muestra un estudio del historial de precios que ha tenido la moneda desde sus inicios hasta la actualidad.

Figura 4.3. Historial de precios del Bitcoin.



Fuente: https://btcdirect.eu/es-es/precio-bitcoin

[11] https://bitcoincharts.com/bitcoin/ consultado el 18/04/2020.

Los inicios del Bitcoin suponían una cotización casi nula de la moneda debido al desconocimiento generalizado que se tenía sobre ella. Desde su lanzamiento en el 2009 hasta la actualidad se observa un verdadero desarrollo y crecimiento en su capitalización.

El 22 de mayo de 2010, Laszlo Hanyecz realiza la primera transacción con la moneda Bitcoin, comprando dos pizzas de Papa John's pagándolas con 10.000 bitcoins. En ese momento, los bitcoins tenían un valor de unos 0,003 centavos de dólares, pagando por las pizzas unos 30 dólares. Hoy serían unos 67 millones de euros. Ese día se convirtió en el anecdótico "Bitcoin Pizza Day", como las pizzas más caras de la historia.

El mínimo histórico se da en septiembre del 2010 en el que el precio de cada moneda es de 0,04€ y no será hasta febrero de 2011 cuando el precio del Bitcoin supere el euro. Durante ese año llegaría a tener el precio máximo de 30 euros. El 2011 se cerró con una cotización de 2€ debido a las restricciones informadas por Silk Road y no remontará hasta el 2013, que se cerró con un precio de 1.000€. No obstante, el precio del bitcoin volvió a caer por el hackeo de la mayor casa de cambio hasta entonces, MtGox, en el que desaparecieron 850.000 bitcoins, pasando su precio de 800€ a menos de 500€.[12]

En el 2017 se incorpora al bitcoin por vez primera en una bolsa de los Estados Unidos y alcanzará su valor máximo de todos los tiempos en diciembre de 2017, valorándose cada bitcoin por 16.727,68€. A partir de este último valor, la cotización disminuye hasta los 3.114,04€ un año después (se produce un decrecimiento de 13.613,64€ en tan solo un año). Hasta marzo del ejercicio de 2019, la cotización estará en torno a los 3.500€ y será a partir de abril de 2019 cuando comience a incrementarse de nuevo, desde los 4.492,81€ hasta el máximo anual de 11.426,17€ el 27 de junio de 2019.

El ejercicio 2020 comienza con una cotización del Bitcoin en los 6.412,85€ y subirá paulatinamente hasta los 9.528,79€ el 15 de febrero de 2020 (máximo anual hasta la actualidad). A partir de ese momento, el precio comienza a decrecer como consecuencia de la crisis originada por la pandemia de la COVID-19, llegando a los 4.509,86€ tan solo un mes después, el 17 de marzo de 2020. A partir de ese momento, los precios vuelven a remontar pero no alcanzan el promedio anual con respecto al ejercicio abril 2019-abril 2020 que estaría en torno a los 7.737,14€.

Figura 4.4. Precios del Bitcoin abril 2019 - abril 2020.

Fuente: https://btcdirect.eu/es-es/precio-bitcoin

[12] https://es.cointelegraph.com/bitcoin-price-index consultado el 19/04/2020.

4.3. FUNCIONAMIENTO.

La publicación de Satoshi Nakamoto constó de dos partes, una primera en la que se desarrollaba el funcionamiento del sistema y una segunda en la que se facilitaba el software para poder llevar a cabo las transacciones. El sistema Bitcoin funciona mediante una red *peer to peer* (P2P) al igual que grandes programas informáticos del pasado como eMule o Ares.

La red P2P o red entre partes es un sistema utilizado para compartir archivos de todo tipo entre usuarios conectados a Internet, en cualquier lugar y en cualquier momento. Así, el material ubicado en un dispositivo con conexión puede obtenerse en otro dispositivo conectado a la misma red y así sucesivamente, hasta el punto de que dicho material llegue a estar ubicado en tantos dispositivos que su obtención sea verdaderamente rápida y sencilla.

Es posible hacer una aplicación analógica del sistema Bitcoin al programa Ares para hacer una aproximación al funcionamiento del sistema. El programa Ares no cuenta con un servidor central en el que se disponen los archivos multimedia a los que se tiene acceso. Ares cuenta con una red formada por miles de usuarios que suben y descargan material. Al descargar una película desde Ares, ese dispositivo se convierte en servidor de otro dispositivo de origen. De esta forma, los datos van de usuario a usuario, de par a par.

Esta es la tecnología que Satoshi Nakamoto aplica al sistema Bitcoin, considerando que es la mejor forma para gestionar el dinero que tiene cada persona mediante un registro global o libro de transacciones público al que tenga acceso todos los usuarios. En ese libro se incluirán todas las transacciones ocurridas desde su creación, facilitando así la posibilidad de trazar el recorrido que ha hecho cada una de las monedas desde su inicio hasta la actualidad. Un control diferente para una moneda descentralizada, distinta. Un control respaldado por los propios usuarios en lugar de por una autoridad gubernamental pública.

Para que el control sea efectivo, el libro de registro debe ser público y accesible por los usuarios en cualquier momento. Esa publicidad iría contra la regla de la criptografía que, como se analizó anteriormente, se basaba en la privacidad. No obstante, las transacciones son anónimas y eso hace que, aunque el registro sea público, no es posible conocer la identidad de los sujetos que realizan las transacciones. Se consigue gracias a la encriptación asimétrica. El libro de registro es lo que se conoce como Cadena de Bloques o Blockchain.

4.3.1. Monedero digital.

El monedero o billetero digital en Bitcoin es una aplicación móvil o de escritorio en la que existen un par de claves criptográficas que están interconectadas con las direcciones. Una de las claves es conocida públicamente mientras que la otra es privada. La clave pública se conoce como dirección o billetero Bitcoin y de cada clave se generan dos claves privadas, de las que solo tendrá conocimiento cada usuario. A partir de ambas claves, ya será posible firmar transacciones y verificar posteriormente dichas firmas.

Una dirección Bitcoin es una cadena alfanumérica de 33 caracteres, aunque pueden oscilar entre los 27 y los 34, cuyo fin es identificar un lugar donde hay o ha habido vinculados un número concreto de bitcoins. La dirección se forma mediante el algoritmo ECDSA que consiste en la encriptación asimétrica mediante una ecuación matemática y algorítmica bastante compleja que hace imposible conseguir la clave pública a partir de una clave privada.

La única persona que puede desbloquear y usar los fondos depositados en el monedero es el propietario, que será el que tenga acceso a la clave privada. La clave pública (dirección o billetero) será la que posibilita que se verifiquen las firmas digitales. En cambio, la clave privada es la firma de donde procede efectivamente dichas firmas digitales. Mientras que la clave pública es compartida y permite crear la dirección de Bitcoin, la clave privada es personal e intransferible y prueba la titularidad y propiedad que tiene cada persona en el libro de registros de Bitcoin. Ambas claves funcionan de manera complementaria y en par.

En el caso de que un propietario de bitcoins perdiera o transfiriera su clave privada, estará ante el peligro de perder toda las monedas que tenga vinculada a ese billetero pues el que haya obtenido el acceso a dicha clave, tendrá la posibilidad de robar y transferir los bitcoins rápidamente a otras cuentas sin ningún tipo de obstáculos.

Cada bitcoin emitido tiene que estar unido ineludiblemente con una dirección, con su correspondiente clave pública y privada. De esa forma, el titular podrá realizar operaciones con su moneda. El que envía la moneda, esto es, el remitente, firma que se va a producir una transferencia de una clave pública a otra, de un monedero a otro. Para que sea válida la transacción, el remitente debe firmar digitalmente con su clave privada. Será en ese momento cuando la operación se transmita a la red y se haga irrevocable.

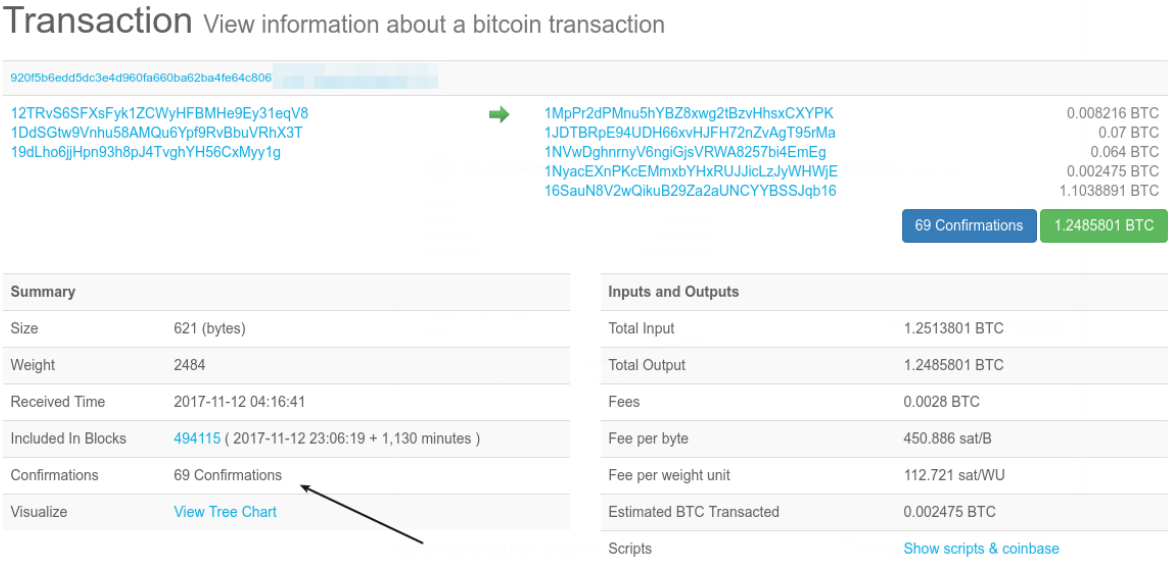
Según Tulio Rosembuj (2015) la localización del monedero virtual es relevante a la hora del blanqueo de capitales y de conocer a qué territorio estará sujeto para determinar la regulación que le correspondería y la sujeción o no a determinados tributos como el Impuesto de Patrimonio o el Impuesto sobre la Renta de las Personas Físicas.

4.3.3. Transacción.

Una transacción es una operación comercial que se realiza entre dos o más partes que se comprometen al pago de un precio como contraprestación a la entrega de un bien o a la prestación de un servicio. El Bitcoin funciona de la misma forma, existiendo la posibilidad de pagar ese precio con la moneda virtual y la transacción se efectuaría trasladando los bitcoins desde una dirección a otra, lo que conlleva el cambio de la titularidad de dichas monedas. En la transacción debe recogerse: la cuantía de bitcoins que se transfieren, la dirección desde la que se emiten y la dirección hacia dónde se remiten.

Las transacciones son emitidas a la red global de usuarios de Bitcoin y es la propia red la que debe confirmarla. Es necesario traer a colación lo visto con respecto a la red P2P. Con la confirmación por parte de la red de usuarios se consigue verificar la transacción y, una vez que se demuestra su validez, se añade a un bloque. Para que una transacción se considere válida se requieren un mínimo de seis confirmaciones.

Figura 4.5. Una transacción de bitcoins.



Fuente: https://support.uphold.com/hc/es/articles/115005486886--Porque-está-my-transacción-bitcoin-pendiente-

En el ejemplo de la Figura 4.5 se observa una transacción que se realiza desde tres direcciones diferentes a cinco direcciones independientes, las cuales reciben 0.008216 BTC, 0.07 BTC, 0.064 BTC, 0.002475 BTC y 1.1038891 BTC, haciendo una suma total de 1.2485801 BTC. En la columna derecha de la figura se observan dos parámetros esenciales en cualquier transacción: los inputs y los outputs. El primero se relaciona con el output de una transacción anterior mientras que el segundo contiene una serie de mecanismos que con los que se pretenden hacer llegar una cantidad de bitcoins a una dirección nueva.

Tal y como establece el protocolo Bitcoin y como se observa en el ejemplo, la suma total de los outputs tiene que ser menor o igual que la suma de los inputs. El total de inputs es 1.2513801 BTC frente al total de outputs, 1.2485801 BTC. La diferencia que existe entre uno y otro es la comisión que cobra el emisor de la transacción. En este caso, la comisión sería de 0.0028 BTC. A mayor comisión por cada transacción, más rápida será la confirmación por parte de los usuarios de la red. En el ejemplo se observan un total de 69 confirmaciones, por lo que se podría entender como validada la transacción.

La validación de las transacciones reside en los usuarios, debido a que no hay intermediarios que controlen y regulen su veracidad. Por ello, las transacciones tienen que introducirse en la Blockchain para que los participantes muestren su conformidad. Esto se consigue con un sistema de transacciones ordenadas cronológicamente y con los conceptos que se desarrollarán a continuación: bloque, cadena de bloque y algoritmo de proof of work.

4.3.4. ¿Qué es el hash?

La palabra “hash” puede traducirse al español literalmente como “picar” o “moler” pero en el ámbito informático la traducción correcta es “función hash” o “resumen criptográfico”. Esa función consiste en una ecuación criptográfica formada por una combinación de números (entre el 0 y el 9) y de letras (entre A y F). El algoritmo convierte cualquier cantidad de datos, por grande que sea, en un hash de una extensión limitada.

La gran cuestión que debe superar los hashes para que sean realmente efectivos y seguros en la criptografía es evitar la colisión. Por colisión se entiende la entrada de diferentes datos que dan lugar a un mismo algoritmo hash. Una función hash criptográfica debe dar un algoritmo diferente para cada entrada de datos. Aunque varíe en tan solo una letra, el hash debe ser completamente distinto, como se muestra en el siguiente ejemplo.

Figura 4.6. Un ejemplo de hash.

Input		Digest
El Bitcoin.	Función hash criptográfica	244B 799D 5997 6381 8D53 727A 327C F632 C6CE F3D3
El Bitcoin es una criptomoneda.	Función hash criptográfica	ACF1 F0F8 2D6F 2488 861E 3807 63F8 D04C 8BCF 5D6C
El Bitcoin es una criptomoneda creada por Satoshi Nakamoto.	Función hash criptográfica	F3FE EC2C 3CCB 7927 0C2E DB9B 1C9D 50B8 AA20 5AFD
El Bitcoin es una criptomoneda creada por Satoshi Nakamoto en 2009.	Función hash criptográfica	188F E7A4 0D7A A82A 5F37 C921 06FC 4AFE A684 6374

Fuente: elaboración propia a través de los datos obtenidos por https://herramientas-online.com/generador-hash-online.html#resp

La particularidad de los hashes es que su creación es realmente sencilla. Sin embargo, es realmente complejo deducir a partir de un hash el contenido de los datos iniciales porque no siempre se conocen las instrucciones para resolverlo.

Para la explicación del hash, se pone el siguiente ejemplo. Una persona acude a un restaurante y cena un plato elaborado con una serie de ingredientes que, al probarlo, no logra distinguirlos. Al no ser capaz de ello, acude al *maître* pero su respuesta no le resuelve su duda. Al llegar a casa, el sujeto pretende cocinarlo pero al probarlo, el sabor no es el mismo.

Esto ocurre con los hashes: si no se conocen las instrucciones que se han dado para alcanzar el algoritmo será muy complicado llegar a los datos que representa. Al igual que el comensal que pretende elaborar él propio el plato sin haber podido saber cada uno de los ingredientes que lo conforman ni la forma con la que se ha llevado a cabo. El resultado no será el correcto. Es muy fácil obtener un hash pero muy difícil saber de dónde o cómo se obtiene. Se utilizan para dos cuestiones muy importantes: las direcciones y la minería.

4.3.5. Bloque.

El bloque es una secuencia púbica de transacciones inalterables y ordenadas cronológicamente que han sido previamente lanzadas a la red por los emisores. Una vez confirmadas las transacciones por un número relevante de participantes, se introducen en el bloque y adquieren validez. Este es el proceso de la minería, analizado anteriormente, llevado a cabo mediante la prueba de trabajo o proof of work.

El contenido de un bloque va a ser analizado a través de la explicación del último bloque publicado antes de las 1:55 horas del día 26 de abril de 2020.

Figura 4.7. El bloque 627.501.

Hash	00000000000000000108f924215768081300a4ebd478704fcab33e96ccbddda
Confirmaciones	1
Fecha y Hora	2020-04-25 01:47
Altura	627501
Minero	Poolin
Número de transacciones	2636
Dificultad	15.958.652.328.578,42
Raíz Merkle	26c81691a2ea7e850e3d6ae5f6d5703276f8ecf10da66d0b23a3143517cfeb94
Versión	0×20000000
Bits	387.031.859
Peso	3.992.780 WU
Tamaño	1.239.206 bytes
Nonce	2.317.874.484
Volumen de la transacción	5317.45291533 BTC
Recompensa de Bloque	12.50000000 BTC
Remuneración por la comisión	0.16685594 BTC

Fuente: https://www.blockchain.com

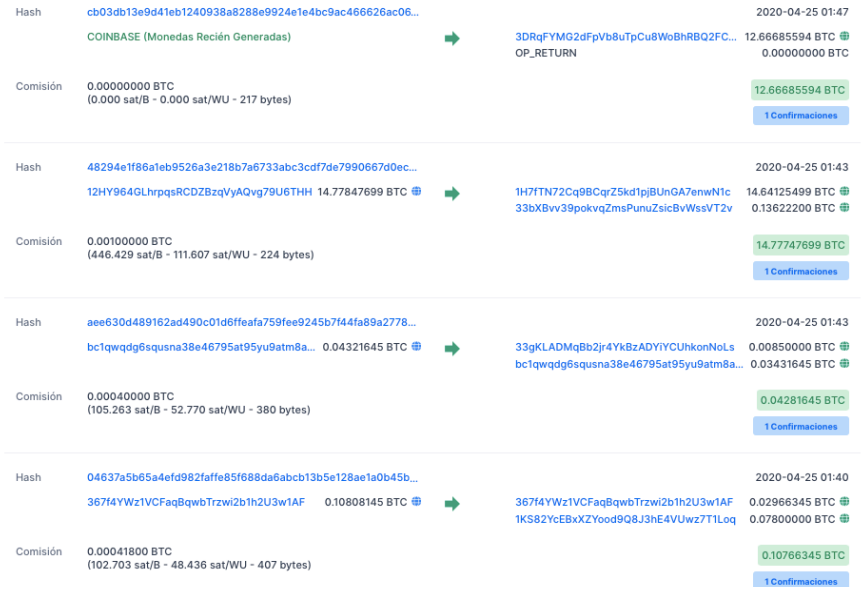
Los elementos que integran cualquier bloque incluido en la red Bitcoin son los siguientes:

- **Número de transacciones**. Es un indicador que muestra la cantidad de transacciones válidas que se han incluido en el bloque. En el caso hay un total de 2.636 transacciones.
- **Altura.** Es la posición que tiene el bloque con respecto al primero creado en 2009 por Satoshi Nakamoto y denominado “bloque génesis”. En el caso es el número 627.501.
- **Timestamp o fecha de creación.** Es el momento en el que se mina el bloque, en este caso, el día 25 de abril de 2020 a las 1:47 horas.

- **Minero.** Muestra el nombre, si es público, de la persona, grupo de personas o institución que ha conseguido minarlo. En este caso, el nombre es público: Poolin.
- **Dificultad.** Como su propio nombre indica, la dificultad es la complejidad que encuentran los mineros para publicar un bloque. A medida que el número de mineros se va incrementando y estos van adquiriendo más y mejores dispositivos para realizar la actividad de la minería, la dificultad crece al igual que la competencia. Mientras que en los inicios de 2009 se podían minar bloques desde un teléfono móvil, hoy se requieren grandes conjuntos informáticos formados por miles de dispositivos y controlados por expertos para poder realizar la tarea de minar. En sus inicios, la dificultad era 1 (no había competencia, el único minero era su creador). La dificultad se sustancia en la forma en que se mantiene la tasa de diseño, que establece que ha de generarse un bloque cada 10 minutos. En este último bloque publicado, la dificultad es de 15.958.652.328.578,42.
- **Bits.** Es el número de bits que entran dentro de un bitcoin, en este caso, 387.031.859.
- **Tamaño del bloque.** Es el contenido máximo de capacidad que puede tener un bloque, que suele ser de 1 MB. En este caso, el tamaño es de 1,239206 MB.
- **Versión.** Es el número de la versión del protocolo Bitcoin que se ha utilizado para la publicación del bloque. En este caso, la versión es la número 0x20000000.
- **Nonce.** Es un número arbitrario combinado con el hash utilizado por la criptografía, para autenticar efectiva al bloque. En este caso, el número nonce es: 2.317.874.484.
- **Recompensa de bloque.** Las recompensas que cada minero obtiene por la publicación de cada bloque se desarrollaron en el *epígrafe 4.2.1: "emisión y obtención de bitcoins"*. El halving obtenido por Poolin es de 12,5BTC, puesto que estamos en la tercera era de recompensa. Además, obtendrá una remuneración por comisión de 0,16685594 BTC.
- **El valor de la raíz del árbol de Berkle.** Es un valor hash que condensa toda la información que se encuentra en el bloque. En este caso, el hash es 26c81691a2ea7e850e3d6ae5f6d5703276f8ecf10da66d0b23a3143517cfeb94.

Estos elementos formarían parte del encabezado del bloque. En segundo lugar, se encuentra el cuerpo del bloque que contiene todas y cada una de las transacciones que los forman. En la siguiente figura se ve el cuerpo del bloque analizado anteriormente.

Figura 4.8. El contenido del bloque 627.501.



Fuente: https://www.blockchain.com [13]

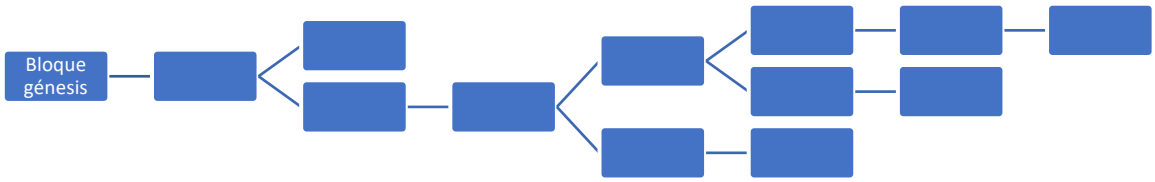
13
https://www.blockchain.com/btc/block/000000000000000000108f924215768081300a4ebd478704fcab33e96ccbddda consultado el 26/04/2020.

4.3.6. Cadena de bloques o Blockchain.

La Cadena de Bloques o Blockchain es un registro permanente, inmutable y público en el que se recogen todas y cada unas de las transacciones que se han realizado con la moneda Bitcoin desde su creación, mediante bloques encadenados entre sí. Con esto se pretende poder verificar que el flujo de bitcoins ha sido correcto y no se ha quebrantado ese encadenamiento, desde el bloque génesis (el primer bloque) hasta el último generado.

Con la Blockchain se supera el problema del doble gasto o *"double spending"*. Será muy difícil utilizar un mismo bitcoin para más de una transacción ya que los bloques están perfectamente conectados y la más mínima separación a esa cadena produciría la no confirmación por parte de los participantes en la red, no llevándose a cabo nunca.

Figura 4.9. Cadena de bloques desde el "bloque génesis".



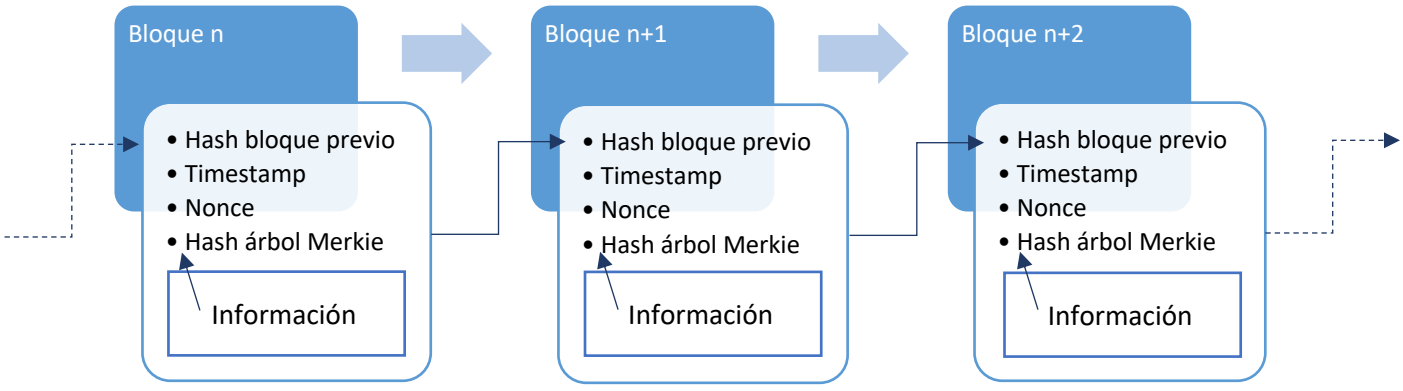
Fuente: elaboración propia a partir de los datos obtenidos en http://www.criptored.upm.es [14]

En la Figura 4.9 se observa que la cadena es una intersección única de bloques conformada por un único camino posible, cuyo inicio es el bloque génesis y el final, el último bloque publicado. En consecuencia, pueden existir *forks* o bifurcaciones, que ocurren cuando un minero cambia el protocolo inicial. La bifurcación puede ser suave o dura. En la primera, el cambio en el software es mínimo y no es necesario actualizar la versión para que sean compatibles. Sin embargo, en la segunda se crea un software paralelo: la versión nueva es totalmente distinta y no es posible conectarlas para transmitirse información entre ellas.

El 1 de agosto de 2017 se produce una bifurcación dura en Bitcoin que conllevó a la creación de la nueva moneda, el Bitcoin Cash. En ese momento, los propietarios de bitcoins pasaron a tener en sus monederos la misma cantidad pero en la nueva moneda.

En la siguiente figura se amplía y se detalla la anterior, observándose los elementos que han de incluirse en cada bloque y cómo han de relacionarse entre ellos para salvaguardar la cadena desde el bloque génesis hasta el último publicado.

Figura 4.10. Estructura de los bloques en la Blockchain.



Fuente: elaboración propia a partir de los datos obtenidos en www.mincotur.gob.es [15]

[14] http://www.criptored.upm.es/crypt4you/temas/sistemaspago/leccion3/leccion03.html#apartado335 consultado el 26/04/2020.

[15] https://www.mincotur.gob.es/Publicaciones/Publicacionesperiodicas/EconomiaIndustrial/RevistaEconomiaIndustrial/405/DOLADER,%20BEL%20Y%20MUÑOZ.pdf consultado el 26/04/2020.

La creación de nuevos bloques en la Blockchain se consigue mediante la prueba de trabajo o proof of work que se examinará a continuación.

4.3.7. Prueba de trabajo o proof of work.

La prueba de trabajo o proof of work es el algoritmo utilizado para crear hashes válidos de los bloques. En esta tarea que realizan los mineros tiene mucho que ver la dificultad de la que se hacía referencia anteriormente, que se aumenta a medida que se van añadiendo ceros a la izquierda del hash. Ese número de ceros se regula según el target: cada 2.016 bloques, que se produce cada 14 días aproximadamente, se aumentan. Es la forma para conseguir que los bloques se publiquen cada 10 minutos y no en menos tiempo.

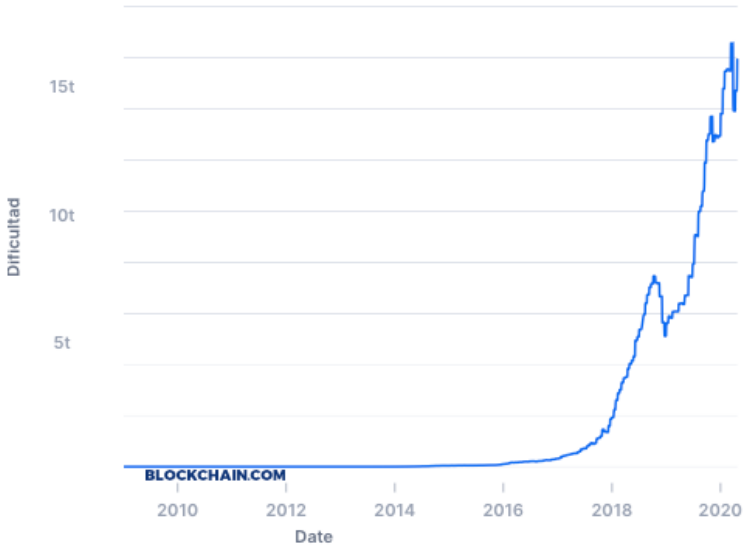
Lo que deben conseguir los mineros es un nonce que consiga un valor hash del bloque. Para obtener un bloque válido, los mineros deben de llevar a cabo un procedimiento para comprobar cada uno de los valores hasta dar con un nonce válido, lo que supone un proceso realmente costoso y esto es lo que se conoce como prueba de trabajo. Es como un rompecabezas que deben resolver los mineros y la dificultad aumenta a medida que se imponen ceros a la izquierda.

La dificultad se calcula de la siguiente forma (Retamal Dolater, Bel Roig, Muñoz Tapia, 2017, p.34):

$$Dificultad\ nueva = \frac{dificultad\ previa * 2\ semanas}{tiempo\ en\ minar\ los\ últimos\ 2.016\ bloques}$$

En la siguiente figura se puede observar cómo ha ido incrementando la dificultad como consecuencia de la entrada de nuevos mineros y al aumento de la competencia para publicar bloques en la Blockchain. Es necesario traer a colación lo analizado en los elementos que componen un bloque, en concreto, "la dificultad". Actualmente, la dificultad es de casi 16 billones frente a la dificultad 1 con la que se inició el proceso con la publicación del bloque génesis en el año 2009.

Figura 4.11. El proceso de la dificultad.



Fuente: https://www.blockchain.com/charts/difficulty

4.4. UTILIDAD.

4.4.1. El Bitcoin en España. Regulación y jurisprudencia.

Para el análisis correcto en cuanto a la regulación y lo que establece la jurisprudencia sobre qué es el Bitcoin, hay que estudiar el concepto jurídico -no económico- de dinero.

En primer lugar, en el ordenamiento jurídico español, el dinero se define por las funciones que cumple que son dos (Paz-Ares, 1994): (i) función de medida del valor de las cosas y derechos; (ii) función de cambio (sirve para adquirir cosas). Es necesario incidir en que esta segunda función puede ser cumplida de la misma forma por otros bienes, en la medida en que estos pueden constituir el objeto de una obligación correspectiva a otra de entrega de otras cosas o derechos. Es decir, bienes, derechos o servicios pueden cambiarse por bitcoins si las partes lo acuerdan. Cuando esto sucede, el tipo contractual será diferente: si se entregan bitcoins como pago de un precio por la contraprestación a la entrega de un bien sería un contrato de permuta, mientras que si es dinero de curso legal es una compraventa.

A la hora de valorar un bien o derecho para fijar una indemnización, el valor no puede hacerse en bitcoins. Las partes pueden establecerlo pero igual que podrían hacerlo en esmeraldas o diamantes. A falta de acuerdo, un tribunal deberá condenar, si lo considera oportuno y en base a la ley, abonar en dinero y no otra cosa: ni esmeraldas, ni diamantes, ni bitcoins. Esto es porque, actualmente, el acreedor no tiene la obligación de aceptar una liberación de la deuda si no es en dinero, salvo que se produjera un cambio del sistema legal.

En segundo lugar, es interesante la Sentencia del Tribunal Supremo 313/2019, de 20 de junio, especialmente en la referencia al recurso interpuesto por la acusación. En la nota publicada por el Profesor Carrasco Perera, decía que la Sala 2ª del Tribunal Supremo dictaminó que la restitución del daño a realizar conforme a los artículos 110 y 111 del Código Penal no puede llevarse a cabo en bitcoins, debido a que no es dinero de curso legal ni electrónico, al no ajustarse a la definición del artículo 1.2 de la Ley 21/2011, de 26 de julio.

El artículo 1.2 de la Ley 21/2011[16] establece:

> Se entiende por dinero electrónico todo valor monetario almacenado por medios electrónicos o magnéticos que represente un crédito sobre el emisor, que se emita al recibo de fondos con el propósito de efectuar operaciones de pago según se definen en el artículo 2.5 de la Ley 16/2009, de 13 de noviembre, de servicios de pago, y que sea aceptado por una persona física o jurídica distinta del emisor de dinero electrónico.

En el caso analizado, el condenado por estafa había acordado con las víctimas la realización de un negocio “high frequency trading” en bitcoins, a cambio del pago por ellos en euros por el importe de la inversión. La alegación particular aboga porque el tribunal condenase al acusado a restituir en bitcoins, como se acordó entre las partes, y en el caso de estar ante la fase de ejecución en el que tuvieran que hacerse frente al pago de unos intereses de demora, entonces proceder a su valoración en euros. La Sala del Alto Tribunal desestima el alegato particular argumentando que el bitcoin no es dinero y que no satisface de forma efectiva y real la reparación de daños que establece el Código Penal.

Sin embargo, el Código Civil en su artículo 1.170 establece que el pago indemnizatorio ha de hacerse en la “especie pactada”. Con ello, debería admitirse el recurso y estimar la demanda. El problema es que el bitcoin no puede ser impuesto como moneda de pago frente a terceros porque no es una moneda de curso legal, como establece el Código Civil. Solamente podría indemnizarse en la misma especie cuando las partes lo hayan acordado, como se hace en el caso: tanto el pago de la indemnización por incumplimiento como de indemnización por la mora deberían haberse realizado en bitcoins. Otro problema es que la mora complementaria se valora en función del interés legal del dinero y no existe un “interés legal del bitcoin”, por lo que en el contrato debería haberse establecido el interés legal del bitcoin, sino tendría que aportarse en euros.

[16] Ley 21/2011, de 26 de julio, de dinero electrónico (BOE núm. 179, de 27 de julio de 2011).

Según Asensio Borellas (2019) para definir el Bitcoin desde una perspectiva jurídica, hay que hacer un estudio previo de dicha moneda como derecho de propiedad intelectual y como bien patrimonial inmaterial, documento electrónico. Rechaza que el bitcoin sea un derecho de propiedad intelectual como moneda virtual y medio de pago; sí sería considerado como propiedad intelectual el protocolo Bitcoin publicado por Satoshi Nakamoto, pero las monedas que se general a raíz de aquel no pueden tener dicha consideración.

Una vez analizados esos dos puntos de vista, da la siguiente definición: "objeto de derecho de contenido patrimonial, de transmisión personalísima mediante un sistema abstracto determinado informáticamente y de carácter transnacional" (párrafo 20).

Categorizar al bitcoin como una cosa y como todas las cosas, pueden ser objeto de apropiación, según establece el artículo 333 del Código Civil. Cabe la apropiación en el bitcoin porque se permite su transmisión y también se podría inutilizar en el caso de pérdida, destrucción o robo del mismo. Por todo ello, cabe establecer que el bitcoin es un objeto de derecho y como tal, un derecho patrimonial.

En cuanto a la transmisión del bitcoin, el sistema por el que se traslada la propiedad es abstracto. Se requiere de una emisión de la orden a una red global de participantes que la van repitiendo entre ellos y confirmándola o no. Una vez confirmada, será susceptible de acceder a la Cadena de Bloques y la transacción deviene irreversible: ha pasado de una dirección a otra y ya no puede haber vuelta atrás.

El Bitcoin goza de una naturaleza trasnacional, por lo que sus reglas no se sujetan al derecho de ningún Estado, sino al software creado por Satoshi Nakamoto. El protocolo no es inmutable pero cambiarlo supone de la decisión por todos los participantes de manera conjunta, no depende de ninguna autoridad. Por ende, su transmisión no va a regularse por el derecho español, no cabe en la definición que el artículo 609 del Código Civil hace en cuanto a la transmisión de la propiedad y de los demás derechos reales. En dicho precepto, el Código Civil establece que la propiedad y demás derechos reales se transmiten mediante la tradición, que es el acto por el cual se entrega una cosa física a una persona física o jurídica y, en ese momento, se cambia la propiedad de dicho bien. En este caso no ocurre así porque no hay un traslado físico de bitcoins de una dirección a otra, sino que se produciría un traslado de la propiedad pero mediante una traditio ficticia.

Las transacciones son personalísimas porque se realizan en virtud de una serie de claves públicas y privadas de las que solamente tienen acceso aquellos sujetos que disponen en sus monederos virtuales de bitcoins. Después de todo, los bitcoins son fungibles porque son susceptibles de sustitución un monto de dinero en otro tanto de la misma divisa.

4.4.2. Tributación del Bitcoin.

A la hora de establecer la tributación del bitcoin como moneda, hay que atender a dos puntos de vista: la consideración del bitcoin como divisa o la consideración del bitcoin como bien.

El Tribunal de Justicia de la Unión Europea ha defendido la primera consideración en la Sentencia de 22 de octubre de 2015, David Hedqvist, asunto C-264/14. El tribunal señaló que el bitcoin es un medio de pago entre los operantes que lo acuerden como tal, considerando exentas del Impuesto sobre el Valor Añadido de aquellas operaciones en las que se practique un cambio de Bitcoin por otras divisas, ya que acepta al bitcoin como una divisa más.

En virtud de dicha sentencia y otras (como la Sentencia del Tribunal de Justicia de la Unión Europea de 12 de junio de 2014, Granton Advertising, asunto C-416/12), la Dirección General de Tributos española ofrece una Resolución Vinculante (V1748-18 de 18 de junio de 2018) en la que niega la deducción del IVA soportado a un empresario que se dedica a la minería pues la actividad no está sujeta a IVA. La minería consiste en actividades que dan lugar a la creación de una moneda virtual que es considerada como divisa y, por lo tanto, exenta de IVA. Al ser una operación no sujeta a IVA, no cabe deducción alguna por IVA soportado.

La Administración tributaria justifica la Resolución Vinculante en el artículo 20.Uno.18º, letra j) de la Ley 37/1992[17], que establece que están exentas:

> Las operaciones de compra, venta o cambio y servicios análogos que tengan por objeto divisas, billetes de banco y monedas que sean medios legales de pago, a excepción de las monedas y billetes de colección y de las piezas de oro, plata y platino.

En consecuencia, Administración tributaria española, a raíz de la jurisprudencia europea, considera al bitcoin como divisa y medio de pago, por lo que la compraventa de bitcoins no está sujeta a IVA.

Cuestión distinta es la regulación que establece el Impuesto sobre la Renta de las Personas Físicas. En este caso, la operación tributará como ganancia o pérdida patrimonial en el momento en que se transmita el activo por lo que, en este caso, se va a considerar a la criptomoneda como cualquier activo: desde acciones hasta bienes inmuebles.

Las ganancias obtenidas a partir de un contrato de compraventa se gravan a un tipo de interés progresivo del 19%, 21% y 23% como renta del ahorro. En el caso de que la compraventa generase una pérdida, existe la posibilidad de compensar según las reglas que establece el tributo. En el siguiente cuadro se refleja cómo tributan las ganancias de forma general en el IRPF, en las que se incluye las ganancias obtenidas como consecuencia de una transmisión de bitcoins:

Figura 4.12. Base imponible del ahorro en el IRPF.

Base imponible.	Tipo aplicable.
Desde 0 hasta 6.000€	19%
Desde 6.000€ hasta 50.000€	21%
Más de 50.000€	23%

Fuente: elaboración propia a través de los datos obtenidos de la Agencia Tributaria.

La ganancia patrimonial se calculará mediante la diferencia entre el valor de adquisición y el valor de transmisión, en el caso de la compraventa. En el supuesto de estar ante un contrato de permuta, esto es, usar el bitcoin como moneda y forma de pago como contraprestación a la compra de bienes o servicios, la ganancia patrimonial se obtiene de la diferencia entre el valor de adquisición del bitcoin y el mayor valor del mercado, del bien recibido o de la criptomoneda en sí (Niubó, 2017).

Cabe destacar que en la actividad de la minería, el minero genera un ingreso mediante la utilización de unos recursos propios, por lo que entra en la definición que el IRPF hace como rendimiento de actividad económica. De esta forma, son deducibles los gastos que sean necesarios para realizar la actividad, como puede ser la amortización de los dispositivos electrónicos, la luz o el agua. Para ello, la Dirección General de Tributos requiere darse de alta en el Ministerio de Hacienda y en la Seguridad Social.

En el caso de considerar al bitcoin como un bien o derecho patrimonial, estaría sujeto al ámbito de aplicación del Impuesto sobre el Patrimonio, cuya valoración se atenderá al precio de mercado a la fecha en que se devengue el impuesto.[18]

Desde finales de 2013 existe la obligación de declarar ante el Impuesto del Patrimonio aquellos bienes y activos que estén en el extranjero pero cuya valoración sea mayor de 50.000€. En el ámbito de las criptomonedas, al ser una moneda descentralizada, no está sujeta a ningún lugar físico. Habrá que atender a la ubicación donde se encuentre el monedero virtual para establecer un ámbito territorial donde proceder a la comprobación del mismo a efectos del tributo sobre el patrimonio.

[17] Ley 37/1992, de 28 de diciembre, del Impuesto sobre el Valor Añadido (BOE núm. 312, de 29 de diciembre de 1992).
[18] Consulta Vinculante de la Dirección General de Tributos V0250-18.

4.5. RIESGO E IMPACTO EN LA ECONOMÍA MUNDIAL.

4.5.1. Seguridad: fondo de cobertura.

En el Diccionario del español jurídico (2020) se define al fondo de cobertura como: "fondo en el gestor goza de gran libertad para colocar los recursos, por lo que suele asumir ciertos riesgos e invertir de manera bastante dinámica tratando con ello de obtener una rentabilidad superior a la media del mercado".

En el mercado de criptodivisas cada vez son más frecuentes los fondos de coberturas que comenzaron su actividad a partir de 2018, como Alliance Capital o Digital Currency Group (fondo de capital riesgo). En un informe publicado por PwC en el año 2019, la inversión se traslada a 100 fondos de cobertura con una financiación de 21.9 millones de dólares. Aunque la inversión tiene unos datos exitosos, la situación del mercado en el ejercicio 2018 fue más complicada y la mediana del fondo de cobertura tuvo una pérdida de más del 40% del valor. La mayoría de estos fondos se encuentran en los Estados Unidos.

La pérdida de valor que tuvo tanto el bitcoin como el resto de las criptomonedas se debió principalmente a las regulaciones estrictas que hicieron los gobiernos de Corea del Sur y China. En Corea se prohibieron las casas de intercambio y en China, se prohibió tanto aquello como intercambiar divisas como el euro o el dólar por criptomonedas como el ether o el bitcoin. La mayor pérdida de valor fue sufrida por las criptomonedas alternativas al Bitcoin.

Sin embargo, la Comisión de Valores y Bolsa de los Estados Unidos de América (SEC) sigue negándose a admitir los fondos negociados en bolsa, como la petición de la empresa de gestión de inversiones Wilshire Phoenix. Esta empresa pretendía garantizar la volatilidad de Bitcoin percibiendo Bonos del Tesoro de los Estados Unidos.

4.5.2. El Bitcoin en la pandemia del Covid-19.

Durante la realización de este Trabajo Fin de Grado, el mundo atraviesa una situación de pandemia declarada por la Organización Mundial de la Salud como consecuencia de la enfermedad originada en China, la COVID-19, que afecta a más de 2,87 millones de personas.

Esta situación de alerta sanitaria está conllevando la paralización de todos los sectores económicos, debido al confinamiento de la población en la mayor parte del mundo. La paralización está afectando a la economía mundial que está viendo un retroceso absoluto que alcanza a día de hoy mínimos históricos que se asemejan a los de la crisis del 2008.

El 27 de enero se decretó en el epicentro de la epidemia, en Wuhan, la cuarentena de la población que se prolongó durante 76 días, hasta el 8 de abril. Unas semanas más tarde, el 21 de febrero, los contagios empiezan a expandirse por distintos países, en especial Italia, donde se decreta el estado de emergencia dicho día con el confinamiento de la población y la consecuente paralización de los sectores productivos a nivel general.

No será hasta el 11 de marzo cuando la OMS decrete la enfermedad por la COVID-19 como pandemia mundial. En España se decreta el estado de alarma tres días más tarde.

La incertidumbre acompañada del desconocimiento en los mercados de valores está haciendo desplomarse su capitalización. El 16 de marzo amaneció con caídas de casi el 10% en la bolsa de Nueva York o la pérdida de un 28,9% de capitalización en el mercado del Ibex 35. Como consecuencia de ello, el valor de las criptomonedas ha decrecido en gran medida.

Las bolsas están relacionadas con la evolución de la economía real porque tienen una dinámica muy especulativa, basada en algoritmos y operaciones de alta frecuencia. En los últimos años se había producido una sobrecotización artificial en las bolsas, sobre todo en la de los Estados Unidos. La posibilidad de obtener ganancias había sido muy alta, de aproximadamente el 36% en Wall Street, generando burbujas. Las grandes empresas, en lugar de invertir lo que hacían era autocomprar: operaciones "buy back" que están prohibidas en los Estados Unidos pero se hacen condicionadas a determinadas normas que se saltan.

Las bolsas estaban muy por lo alto y se tenía conocimiento de su caída, no con la pandemia pero ante esa situación descontrolada de la capitalización. La respuesta de la Reserva Federal ha sido dar 700 mil millones para hacer compras ilimitadas: es una operación destinada exclusivamente a garantizar el patrimonio de los propietarios de acciones. En Estados Unidos, el 10% más rico de la población tiene el 80% de los títulos que se cotizan en bolsa.

Figura 4.13. Capitalización del Bitcoin durante la crisis de la COVID-19.

Fuente: https://es.investing.com/crypto/bitcoin/chart?cid=1057388

En la Figura 4.13 se observa cómo ha afectado la crisis de la COVID-19 a la capitalización del Bitcoin. Mientras que a mediados de febrero, concretamente el día 14 de dicho mes, la capitalización continuaba con una tendencia en alza de su valor, alcanzando los 9.551,4€ de capitalización, con la expansión de la pandemia esa tendencia se invierte y comienza a decrecer. Febrero se cerró con una pérdida del 7,44% del valor de Bitcoin[19]. El día 11 de marzo, día en que se produce la declaración de pandemia por parte de la OMS se produce una caída de 7.048€ a 4.415€ en tan solo un día. Desde entonces, la capitalización del Bitcoin se ha mantenido a la baja y, aunque va reputando, no logra superar la media del primer cuatrimestre del ejercicio de 2020, 7.000€ de capitalización. Actualmente, a las 23:48 horas del 25 de abril de 2020, el precio del bitcoin es de 6.967,6€.

El mercado del Bitcoin no ha seguido la misma tendencia que los demás mercados. Esto es porque esta moneda fue diseñada como consecuencia y para superar la crisis financiera del 2008, por lo que en momentos de recesión, tiene la finalidad de mantenerse a flote. El mercado de las criptomonedas solo ha sufrido un descenso del 5% frente al desplome del 22% de los índices bursátiles como consecuencia de la pandemia.

El Bitcoin es considerado como un activo refugio, consiguiendo incrementar su capitalización desde el inicio de la pandemia. Esto es porque los inversores han aumentado su visión en este tipo de activo que consideran que será el que menos sufra a raíz de esta crisis sanitaria y económica mundial.

[19] https://www.criptonoticias.com/negocios/asi-afectando-coronavirus-ecosistema-bitcoin-blockchains/ consultado el 25/04/2020.

CAPÍTULO 5: ETHEREUM Y RIPPLE.

5.1. EL ETHEREUM.

5.1.1. ¿Qué es el Ether?

Ethereum no es una simple criptomoneda como el Bitcoin sino que va más allá. El joven programador ruso Vitalik Buterin propuso a finales de 2013 un nuevo sistema descentralizado que saldría a la luz el 30 de julio de 2015. Su función principal es crear acuerdos de contratos inteligentes o smart contracts basado en la Blockchain y ser una plataforma donde ejecutarse aplicaciones descentralizadas. Siguiendo la idea del Bitcoin, Buterin creó un nuevo protocolo que superase las limitaciones de su lenguaje de programación, que consideraba insuficientes.

Los contratos inteligentes o smart contracts es un programa informático por el cual, cuando dos o más partes pactan un acuerdo y se ajusta a las condiciones, se produce la ejecución automática del mismo en función de unas cláusulas. Al ser un sistema descentralizado, los contratos no están regulados ni intervenidos por ninguna de las partes. Las partes programan las condiciones, firman y se implanta en la Blockchain para que quede protegido. Su objetivo es dar mayor seguridad que la de los contratos tradicionales y reducir costes y tiempo.

Junto al sistema de smart contracts, Buterin desarrolló una moneda virtual, el ether, utilizada por los participantes de esta red. La oferta de ethers quedó establecida en la preventa que se hizo en el 2014 y es la siguiente: 60 millones de ethers para los contribuyentes en dicha preventa, 12 millones para el fondo de desarrollo de Ethereum, 5 ethers son creados y entregados a los mineros como recompensa a la publicación de cada nuevo bloque, producidos entre 15 o 17 segundos, y 2 o 3 ethers para aquellos mineros que, aunque no consiguieron publicar su bloque e incluirlo en la cadena, encontraron la solución. La emisión está limitada a 18 millones de ethers por año, por lo que tiene una tendencia inflacionaria.

Por cada transacción o contrato inteligente ejecutado, las partes deben pagar una comisión denominada gas price o, simplemente, gas. El gas es un aliciente que se le entrega a los mineros para que validen la operación y le den prioridad a la hora de incluirla en la Blockchain.

A pesar de las muchas características que poseen de manera conjunta Bitcoin y Ethereum, como la tecnología de la Blockchain, la consideración de criptomonedas descentralizadas, la creación de monedas a través de la minería o el sistema de prueba de trabajo o proof of work, son otras muchas las diferencias entre ambas criptomonedas.

Esta moneda no es creada por el mismo sujeto. Mientras que Bitcoin fue creado bajo un pseudónimo que podría ser una persona física o jurídica, o un grupo de ellas, Ethereum fue creado por Vitalik Buterin junto con Gavin Wood y Joseph Lubin. El primer bloque publicado en la red Ethereum se produce el 30 de julio de 2014, fecha de su nacimiento, mientras que el bloque génesis fue publicado el 3 de enero de 2009, 5 años, 6 meses y 27 días antes. Mientras que Bitcoin es un protocolo que se basa exclusivamente en un sistema de pago, Ethereum es un sistema de aplicaciones descentralizadas y smart contracts. Utilizan algoritmos de seguridad diferentes al igual que distintos lenguajes de programación, aplicando el Turing complete, un nuevo lenguaje que supera las deficiencias del Bitcoin.

Es conveniente señalar que los bitcoins son monedas que compiten contra el oro y el dinero fiduciario, mientras que los ethers son unas fichas o tokens que representan un activo digital. La emisión máxima es diferente: en Bitcoin existe el límite de emisión por un valor de 21 millones mientras que en Ethereum se limita la emisión anual. Como se ha apreciado anteriormente, la recompensa de la minería es diferente a la del Bitcoin, actualmente de 12,5 BTC, y va de entre 2 o 3 a 5 ETH, además del gas. El tiempo de procesamiento de los bloques se generan de forma distinta, mientras que en Bitcoin se publica uno cada 10 minutos, en Ethereum el tiempo es de 16 segundos. El tamaño de los bloques en Ethereum es inferior al de los bloques de Bitcoin (1 MB).

Por otro lado, la velocidad con la que cambia la dificultad en Ethereum es mayor, cada vez que se mina un bloque (cada 16 segundos) frente a la de Bitcoin, que se cambia cuando se minan 2.016 bloques, lo que supone un total de 20.160 minutos, esto es, 336 horas: 14 días.

5.1.2. Valoración: precios e historial de precios.

Actualmente, Ether es la segunda criptomoneda con mayor capitalización en el mercado de criptodivisas, de 20.037.724.174,94€ y un precio de 181,50€. Tiene un total de acciones en circulación de 110.680.316 ETH y el cambio producido en las últimas 24 horas es del 0,23%.[20]

Figura 5.1. Capitalización del Ethereum.

Fuente: https://btcdirect.eu/es-es/precio-ethereum

Para el estudio de las siguientes gráficas, es necesario traer a colación lo analizado en las Figuras 3.1 y 3.2. El precio del Ethereum tiene una media de 186,94€ desde su nacimiento en 2015 hasta la actualidad. El mínimo precio se da en octubre de ese mismo año, con la cifra de 0,55€ por cada ether. En enero de 2018 se produce una disminución en la capitalización del Bitcoin en la que el resto de las criptomonedas le quita parte de su supremacía absoluta hasta el momento. En ese periodo, el Ethereum alcanza su máximo histórico con un precio de 1.187,55€, pero esa tendencia alcista comenzará a disminuir y volver a la media.

Figura 5.2. Capitalización del Ethereum desde mayo de 2019 a la actualidad.

Fuente: https://btcdirect.eu/es-es/precio-ethereum

[20] https://coinmarketcap.com/es/ consultado el 26/04/2020.

La crisis de la pandemia por la COVID-19 hace disminuir la cotización de esta criptomoneda, pasando de 262,44€ el 14 de febrero de 2020 a la cifra de 98,88€ tan solo un mes después, el 15 de marzo de 2020, momento en el que la enfermedad es considerada pandemia mundial. A partir de ese momento, se observa un repunte en la capitalización y, en estos momentos, el precio está por encima de la media: 181,05€ (a las 18:41 horas del 26 de abril de 2020).

5.2. EL RIPPLE.

5.2.1. ¿Qué es el XRP?

Hay que hacer una primera pero muy importante precisión a la hora de analizar el Ripple. Ripple es una compañía privada que desarrolla una plataforma de red de pagos (RippleNet) sobre una base de datos denominada Ledger XRP. Este sistema dispone de una criptomoneda denominada XRP que es la utilizada para realizar distintas transacciones.

Chris Larsen y Jed McCaleb fueron los fundadores de la compañía Ripple, en 2012, en California (Estados Unidos). A finales del 2015, la red RippleNet estaba afianzada. XRP se define como un activo público que cotiza en el mercado abierto y está diseñado para unir todas las divisas del mundo. En su creación, el libro mayor XRIP suministró 100 mil millones de unidades a sus fundadores le entregaron el 80%, en concreto, a la empresa Ripple, para aportarle fondos suficientes para desarrollar todo el sistema. Es por ello por lo que se considera una moneda centralizada, de modo que el 80% de las monedas creadas están a disposición de sus creadores.

Ledger XRP, el libro contable, lleva a cabo la actividad de una forma descentralizada y mediante un algoritmo que se basa el consenso de los participantes, cuyo objetivo es la liquidación y registro de operaciones sin ninguna autoridad central que lo controle.

Entre Bitcoin y XRP existen grandes diferencias. Entre ellas, XRP no pretende competir con las divisas actuales sino servir de conexión entre todas ellas y ofrecer una red que permita transacciones de forma rápida y segura, mientras que Bitcoin pretende desplazar al dinero fiduciario y convertirse en una moneda con la que realizar todo tipo de operaciones comerciales. De igual modo, la principal atención que el Bitcoin pone en la minería no tiene la misma importancia en el caso de XRP y esto es debido a que nace con la emisión de todas las monedas. Por ello, en XRP no existen conceptos como halving, dificultad o proof of work ni tampoco Blockchain. Esta es, sin duda, la principal diferencia con el Bitcoin. XRP no se basa en una tecnología basada en la cadena de bloques como lo hacen todas las criptomonedas ya que utiliza un sistema de consensos para validar las operaciones. Los participantes de la red son los que las validan y las cifran dentro de RippleNet.

En ocasiones, a XRP se le denomina la criptomoneda de los bancos y esto es porque otro de sus objetivos es servir de apoyo al sistema financiero ya que da la posibilidad de realizar transferencias de activos en tan solo 4 segundos y con unas comisiones mínimas. Esto es posible mediante la compra de XRP por parte de los bancos, luego acceden a RippleNet para que dichas monedas se reciban en la cuenta del banco y el banco cambia los XRP por cualquiera de las divisas mundiales. Esto hace que el precio de XRP no sea tan volátil, lo que lo sigue diferenciando en gran medida del Bitcoin.

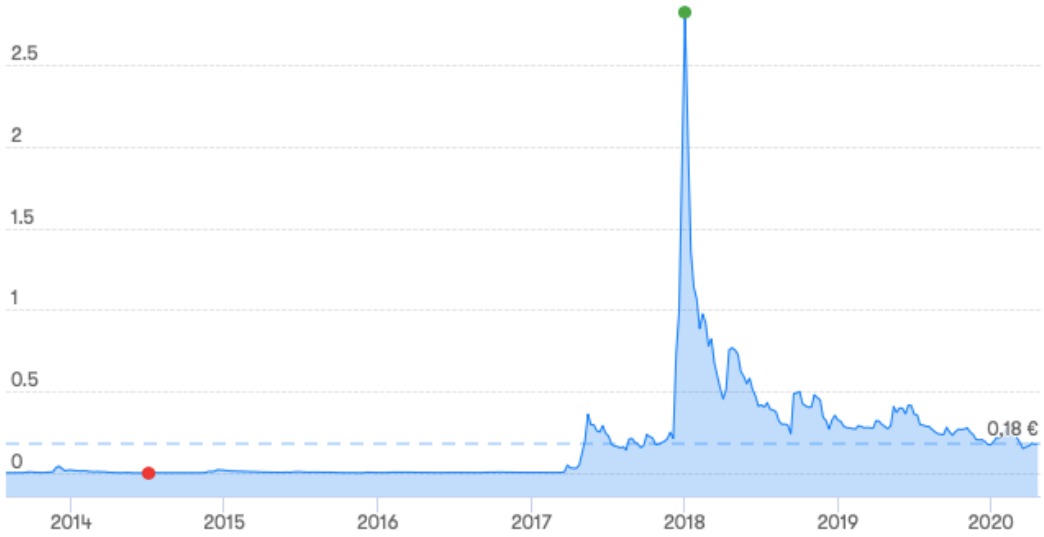
5.2.2. Valoración: precios e historial de precios.

Actualmente, Ripple se encuentra en la tercera posición del mercado de criptodivisas en cuanto a su capitalización de 7.961.519.412,68€ y un precio de 0,18€. Tiene un total de acciones en circulación de 44.089.620.959 XRP y el cambio que se ha producido en las últimas 24 horas ha sido del 0.41% (datos a las 20:18 del 26 de abril de 2020).[21]

[21] https://coinmarketcap.com/es/ consultado el 26/04/2020.

Hay que recordar que las acciones máximas son 100.000.000.000 XRP, por lo que hay en circulación un 44,09%.

Figura 5.3. Capitalización del XRP.



Fuente: https://btcdirect.eu/es-es/precio-ripple

Al igual que anteriormente, para su correcto estudio es necesario traer a colación las Figuras 3.1 y 3.2. El precio de XRP es mucho más estable que en el caso del bitcoin o el ether, por la relación que tiene con el sistema financiero. Desde su creación hasta la actualidad, el precio del XRP ha tenido una media del 0,18€, precio en el que se encuentra en el momento en el que se está desarrollando este trabajo.

En julio de 2014 se produce su mínimo histórico, haciéndose nulo el precio de esta criptomoneda. En enero de 2018, con la caída de la capitalización del Bitcoin y el auge del resto de las criptomonedas, se observa el máximo histórico en el precio de XRP, alcanzando los 2,82€, desde los 0,21€ en los que cotizaba a principios de diciembre de 2017 (se incrementa en 2,61€ en un mes). A partir de dicho momento, el precio del XRP decrece y se mantiene en torno a la media.

Figura 3.4. Capitalización del XRP desde mayo de 2019 hasta la actualidad.

Fuente: https://btcdirect.eu/es-es/precio-ripple

Es preciso hacer una análisis más detallado de la situación actual en la capitalización del XRP como consecuencia de la situación de emergencia decretada como consecuencia de la enfermedad de la COVID-19. En el periodo que oscila entre mayo de 2019 y abril de 2020, la actualidad, el precio medio de XRP es de 0,25€ y se observa cómo en el último mes y medio está muy por debajo de la media. Al igual que coincide con el resto de las criptomonedas, el 14 de febrero supone un precio por encima de la media de 0,31€ pero a medida que pasan los días, el precio comienza a disminuir. El 11 de marzo, día en el que la OMS decreta la pandemia global, el precio baja hasta los 0,19€ y dos días más tarde. El 13 de marzo sigue disminuyendo hasta los 0,12€. A partir de ese momento se observa un paulatino crecimiento de la capitalización. Actualmente, el valor es de 0,18€, valor de la media de precios desde el inicio del XRP hasta la actualidad, pero por debajo de la media en 0,07€ si se observa desde mayo del pasado año hasta la actualidad.

5.3. COMPARATIVA DE LAS CRIPTOMONEDAS MÁS FUERTES: BITCOIN, ETHER Y XRP.

En la siguiente tabla se resumen esquematizados los aspectos principales de las tres criptomonedas más fuertes y las estudiadas en este trabajo: Bitcoin, Ether y XRP.

Figura 3.5. Comparativa de las criptomonedas más fuertes.

	BITCOIN	ETHEREUM	XRP
Nacimiento de la plataforma	18 de agosto de 2008: registro de www.bitcoing.org. 31 de octubre de 2008: publicación del White Paper. 3 de enero de 2009: creación el bloque génesis.	Diciembre de 2013: publicación del White Paper. 30 de julio de 2014: publicación del primer bloque.	2004: se concibe la idea. 2012: se emiten todas las monedas XRP.
Creador de la plataforma.	Autor o autores anónimos bajo el pseudónimo Satoshi Nakamoto.	Vatalik Buterin junto a Gavin Wood y Joseph Lubin.	Ryan Fugger y Jed McCaleb.
Función principal de la plataforma.	Sistema de pago descentralizado, rápido y seguro.	Plataforma que ejecuta smart contracts y aplicaciones descentralizadas.	Red de pagos y activo público que cotiza en el mercado abierto y pretende unir todas las divisas.
Tecnología usada.	Blockchain (Cadena de Bloques).		xCurrent, xRapid y xVia.
Redes usadas.	Mainnet (red principal) y Testnet (red de prueba).		RippleNet.
Algoritmo de seguridad.	SHA256.	Ethash.	Algortimo de consenso.
Lenguaje de programación.	C++.	Turing Complete.	Java.

Moneda descentralizada.	Sí.	Sí.	No.
Nombre de la criptomoneda.	Bitcoins (BTC).	Ether (ETH).	XRP.
Creación de criptomonedas.	Minería		Emisión 100% monedas: año 2012.
Halving (recompensa mineros)	Por validación de bloques: actualmente 12,5 BTC.	Por validar bloques (5 ETH: general) y ejecutar contratos inteligentes (comisión).	No utiliza la Blockchain.
Procesamiento de los bloques.	Cada 10 minutos.	Cada 16 segundos.	No utiliza la Blockchain.
Tamaño de los bloques.	1 MB como máximo.	Sin definir: por debajo de 1 MB.	No utiliza la Blockchain.
Cálculo de la dificultad.	Cada 2.016 bloques minados (14 días).	Cada bloque minado (16 segundos).	No utiliza la Blockchain.
Coste de las transacciones.	Todas por igual.	Depende del gas (comisión).	No utiliza la Blockchain.
Oferta máxima de monedas.	21 millones BTC.	Sin límite: máximo 18 millones ETH anuales.	100.00 millones (ya emitidos)
Capitalización de mercado.	$139.947.935.158	$21.668.662.611	$8.609.843.613
Precio de las criptomonedas.	$7.627,92$	$195,77	$0,195281
Volumen (24h).	$31.805.284.773	$17.501.473.378	$1.636.028.389
Número de monedas en circulación.	18.346.812 BTC	110.681.898 ETH	44.089.620.959 XRP
Cambio (24h).	1,02%	0,61%	0,47%

Fuente: elaboración propia a partir de los datos obtenidos en https://www.miethereum.com/ether/bitcoin-vs-ethereum/#toc1, https://www.ig.com/es/trading-de-criptomonedas/comparativa-criptomonedas y https://coinmarketcap.com/es/.

CAPÍTULO 6: SIMULACIÓN REAL.

6.1. ¿CÓMO SE CONTRATA UNA INVERSIÓN?

Existen varias posibilidades para obtener bitcoins: mediante la minería analizada anteriormente, por la compra de bitcoins desde el propio sistema o vender un producto o servicio cuyo pago del precio sea en bitcoins.

Como se ha especificado anteriormente, el Bitcoin es una criptodivisa en la que se puede invertir para obtener una rentabilidad con el tiempo, aunque está sujeta a un riesgo más elevado que los activos financieros tradicionales (acciones, Letras o Bonos del Estado).

Para llevar a cabo la compra de bitcoins hay que acudir a una plataforma de inversión de bitcoins o bróker, lugar donde se almacenan estas monedas. Hay dos tipos según la seguridad que ofrecen: los monederos para ordenador a través de un software instalado en el mismo y los monederos online. Ambos tienen riesgos, el primero porque puede que ocurra un error en el dispositivo y se eliminen los bitcoins y el segundo puede ser hackeado al estar en la nube.

Los monederos más conocidos son Coinbase y Kraken. Coinbase almacena los datos de los bitcoins de sus usuarios mediante una plataforma que ofrece una seguridad basada en cifrados, exigiendo como contraprestación unas comisiones. Por su parte, Kraken ejecuta únicamente operaciones de grandes cuantías, exigiendo menores comisiones que Coinbase.

Una vez que una persona ha realizado la inversión en bitcoins puede tener acceso a su evolución en cualquier momento mediante dichas plataformas que van indicando el valor al igual que lo haría un mercado de valores. La ventaja frente a la compra de acciones es que no es obligatorio comprar bitcoins completos, es decir, se pueden elegir porciones de bitcoins para invertir una cantidad específica.

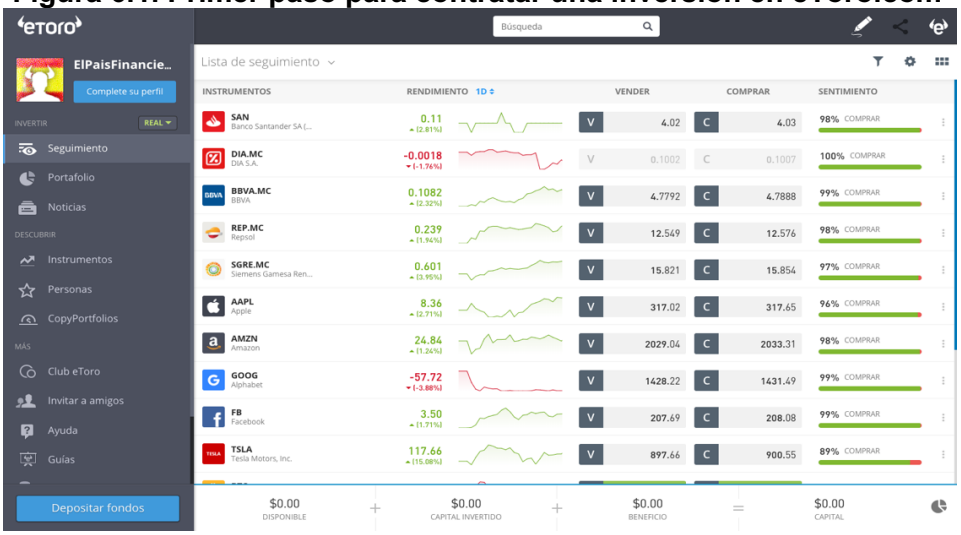
En el caso de que el inversor esté interesado en comprar otras monedas que no sea Bitcoin, las altcoins (resultado de aplicar el concepto de “alternativa” y “Bitcoin”), la alternativa más sencilla es adquirir bitcoins y después transformarlo en la criptomoneda específica en la cual esté interesado en plataformas como Coinbase o BitPanda.

6.1.1. Compra de bitcoins en eToro.com.

Como se especifica en la página web oficial de la compañía, eToro se define como una compañía líder en el sector de plataformas de trading social, que da la posibilidad de invertir tanto en acciones como en criptomonedas y otros activos financieros.

La primera operación sería inscribirse en eToro y crear una cuenta para adquirir bitcoins.

Figura 6.1. Primer paso para contratar una inversión en eToro.com

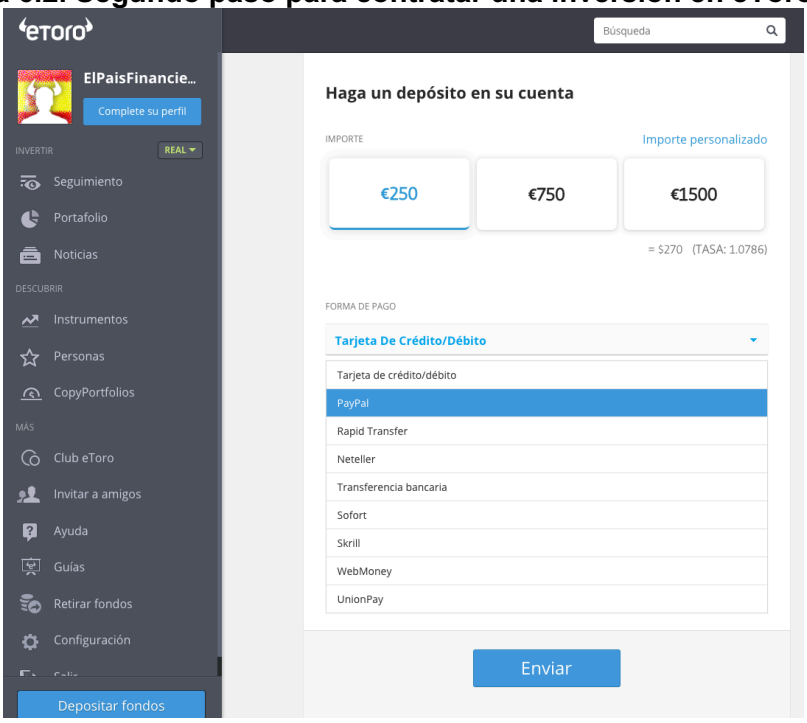


Fuente: https://elpaisfinanciero.com

En la imagen adjunta se puede observar cómo, una vez creada la cuenta, se muestran una serie de activos financieros, en este caso, acciones de empresas como Santander, Grupo Día, BBVA o Repsol, en las que el nuevo usuario podrá invertir en ellas. En la parte inferior se hace un resumen de las operaciones realizadas por el participante. En este caso, al ser el momento inicial, el saldo disponible es de 0€, al igual que el capital invertido y el beneficio, por lo que el capital es igualmente nulo.

El segundo paso es depositar dinero con la cantidad que el usuario esté dispuesto a invertir.

Figura 6.2. Segundo paso para contratar una inversión en eToro.com



Fuente: https://elpaisfinanciero.com

En la figura aportada se observa cómo el inversor puede elegir entre distintas cantidades a depositar en dólares, debido a que esta plataforma funciona con dicha divisa. Es en este momento donde el inversor tendrá que elegir entre distintas opciones cómo realizar el ingreso de dinero para poder, posteriormente, adquirir los bitcoins. Entre las opciones de las que dispone eToro para ingresar fondos, puede escoger: tarjeta de crédito o débito, PayPal, Rapid Transfer o transferencia bancaria, entre otras.

El tercer y último paso sería buscar Bitcoin en los activos financieros disponibles en eToro.

Fuente 6.3. Tercer paso para contratar una inversión en eToro.com

Fuente: https://elpaisfinanciero.com

En la figura anterior se muestra el precio en dicho momento del Bitcoin y, dentro del depósito que el inversor ha realizado en la plataforma web, en este caso, $500, podrá comprar bitcoins hasta dicha cantidad máxima de dólares. Por último, al hacer clic sobre "ejecutar operación" se produce la adquisición de la criptomoneda y el usuario será propietario de $500 de bitcoins que podrá vender en cualquier momento.

6.2. INVERSIÓN EN DISTINTAS CRIPTOMONEDAS: BITCOIN, ETHER Y XRP.

Se va a analizar un supuesto en el que se invierten un total de 10.000€ en las distintas criptomonedas para analizar de esta forma cuál habría sido la evolución de dicha inversión y la ganancia o pérdida que se obtendría en el caso de comprar bitcoins, ethers y XRP.

Este planteamiento se realiza a día 8 de mayo del año 2020, cuyo valor actual del bitcoin es de 9.207,38€, y se proponen varias situaciones a relacionar con el momento actual: la primera, invertir 10.000€ el 8 de mayo de 2011; la segunda, invertir dicha cantidad el 8 de mayo de 2012 y así sucesivamente hasta el 8 de mayo del año 2019.

- **Inversión el 8 de mayo de 2011**. En dicho momento, el valor del bitcoin era de 2.6828€ por unidad de bitcoins, por lo que se habrían podido adquirir un total de 3.727,449 BTC. A día de hoy, esa cantidad de bitcoins se valoran a un precio de 34.378.858,52€, por lo que la ganancia sería del 343.689%.
- **Inversión el 8 de mayo de 2012.** A dicha fecha, el valor del bitcoin era de 3,8802€/BTC, con lo que se habrían adquirido un total de 2.577,187 BTC, lo que supondría hoy día un valor de 23.749.499,82€. La ganancia sería de 237.394,99%.
- **Inversión el 8 de mayo de 2013.** En este momento, el valor del bitcoin era de 85,563€/BTC, por lo que se habrían adquirido un total de 115,523 BTC, valorados actualmente en 1.064.574,33€. La ganancia sería del 10.546%.
- **Inversión el 8 de mayo de 2014.** A dicha fecha, cuyo valor del bitcoin era de 314,6023€/BTC, se habrían podido comprar un total de 31,7861BTC, lo que supondría en la actualidad un valor de 292.968,07€. La ganancia sería del 2.830%.
- **Inversión el 8 de mayo de 2015.** En dicha momento, cuyo valor del bitcoin era de 216,1662€/BTC, se habrían obtenido 46,048 BTC, con un valor actual de 424.599,86€. La ganancia sería del 4.146%.
- **Inversión el 8 de mayo de 2016.** A dicha fecha, el valor del bitcoin era de 405,0696€/BTC, se podrían haber adquiridos 24,810BTC valorados actualmente en 228.748,70€. La ganancia sería del 2.187%.
- **Inversión el 8 de mayo de 2017.** A dicha fecha, el valor del bitcoin era de 1.500,87€/BTC, por lo que se habían obtenido 6,663 BTC lo que supone en la actualidad 61.450,72€. La ganancia desciende a 515%.
- **Inversión el 8 de mayo de 2018.** En dicho momento, el precio del bitcoin era de 7.739,05€/BTC, por lo que se habrían adquirido 1,292 BTC, valorados actualmente en 11.913€. La ganancia es de tan solo el 19%.
- **Inversión el 8 de mayo de 2019.** En este momento, el precio del bitcoin es de 5.385,63€/BTC, por lo que se habrían adquirido 1,857 BTC, valorados en 17.119,18€. Esto supone una ganancia del 71%.[22]

Como se observa en los distintos supuestos, las ganancias son muy dispares debido a que el Bitcoin es un activo muy especulativo pero se puede observar cómo dichas ganancias tienden a decrecer con el paso del tiempo. Esto es debido a los factores que se analizaron anteriormente, fundamentados en la cada vez más demanda que existe de bitcoins a nivel mundial, que hace que la competencia sea más fuerte y que, por lo tanto, la ganancia de este activo cada vez sea menor.

[22] https://criptomo.com/calculadora/ consultado el 8/05/2020.

A 8 de mayo de 2019, en el caso de que se produzca la venta, se produciría la realización del hecho imponible establecido en el Impuesto sobre la Renta de las Personas Físicas, correspondiente a una ganancia como consecuencia de la transmisión onerosa de activos financieros. La ganancia sería de 7.119,18€ que serán declaradas según el tipo aplicable del 21% (figura 4.12), lo que conllevaría una cuota tributaria de 1.495,0278€.

El siguiente planteamiento se hace de la misma forma que con el Bitcoin pero con la moneda de Ethereum. A las 9:12 del 9 de mayo de 2020, el ether cotiza a 194,02€. Se analizarán los supuestos a partir del año 2016, debido a que la creación de esta moneda se retrasa en el tiempo en comparación con el Bitcoin, como se analizó anteriormente.

- **Inversión el 9 de mayo de 2016.** En dicho momento, invertir 10.000€ en Ethereum supondría una compra de 1.198,610 ETH al estar en un valor de 8,343€/ETH. Actualmente estarían valorados en 234.819,69€, por lo que se habría obtenido una ganancia del 2.248%.
- **Inversión el 9 de mayo de 2017.** A dicha fecha, el valor del ether era de 78,78€/ETH por lo que se habrían adquirido 126,936 ETH valorados actualmente a 24.870.57€. Supone una ganancia del 149%.
- **Inversión el 9 de mayo de 2018.** En este momento, el precio de ether era de 629,81€/ETH por lo que se habrían adquirido 15,878 ETH, valorados actualmente en 3.112,56€. Se habría obtenido una pérdida del 69%.
- **Inversión el 9 de mayo de 2019.** El precio del Ethereum estaba en 151,49€/ETH por lo que se habían obtenido un total de 66,011 ETH, lo que supone actualmente 12.927,59€. La ganancia es del 28,99%.

En el caso de que se produzca la venta de estos activos a 9 de mayo de 2019, la ganancia obtenida sería de 2.927,59€ que tributarían en el Impuesto sobre la Renta de las Personas Físicas al tipo impositivo del 19% como ganancia patrimonial (figura 4.12), lo que conllevaría una cuota tributaria de 556,2421€.

El último supuesto se hace en relación con la moneda de Ripple, XRP. A las 9:18 del 9 de mayo de 2020, el XRP cotiza a 0,22333€. Se analizan los supuestos a partir del año 2015:

- **Inversión el 9 de mayo de 2015.** A dicha fecha, el precio de cotización era de 0,006441€/XRP por lo que podrían haberse adquirido un total de 1.552.553,951 XRP, valorados actualmente en 319.981,37€. La ganancia habría sido del 3.100%.
- **Inversión el 9 de mayo de 2016.** En este momento, el XRP cotizaba a 0,005573€, por lo que se podrían haber adquirido 1.793.400,287 XRP, valorados actualmente en 369.440,46€. Esto supondría una ganancia del 3.594%.
- **Inversión el 9 de mayo de 2017.** A dicha fecha, XRP cotizaba a 0,1686€, por lo que se habrían comprado un total de 59.311,981 XRP, valorados hoy día en 12.218,27. Supone una ganancia del 22%.
- **Inversión el 9 de mayo de 2018.** El precio del XRP es de 0,2654€ en este momento. Se habrían adquirido un total de 37.678,975 XRP valorados hoy día en 7.761,87, lo que supone una pérdida del 22%.
- **Inversión el 9 de mayo de 2019.** El precio de XRP es de 0,2654€. Se habrían podido adquirir un total de 37.678,975 XRP valorados hoy día en 7.761,87€. Supone una pérdida del 22%.[23]

En el caso de vender las criptomonedas a 9 de mayo de 2019, la pérdida sería de 2.238,13€. En el caso de que tanto la ganancia como la pérdida por la venta fuera inferior a 1.000€ o a 500€, respectivamente, estarían exentas de declaración en el Impuesto sobre la Renta de las Personas Físicas. La pérdida se puede compensar con las ganancias que se obtengan como consecuencia de una venta de acciones u otro tipo de activo financiero.

[23] https://criptomo.com/calculadora/ consultado el 9/05/2020.

En el caso de que no se obtuvieran ganancias en ese mismo ejercicio, la pérdida obtenida se podrá compensar en los cuatro ejercicios siguientes, esto es, la pérdida de 2.238,13€ generada en 2019 se podrá compensar durante todo ese ejercicio y hasta 2023. La cuota tributaria a compensar sería de 2.238,13€*19% = 425,2447€.

El año 2018 supuso una paralización en el crecimiento de la capitalización del Bitcoin debido a la situación que se produjo de desconfianza que se produjo por parte de los gobiernos de Corea del Sur y China, lo que hizo detener la espectacular subida en su precio que llegó a ser de 16.727,68€ en diciembre de 2017. Sin embargo, fue un año en el que el resto de las criptomonedas aprovecharon la bajada del Bitcoin para incrementar su capitalización y aumentar su posición en el mercado. Dicha razón por explica que, tanto en Ethereum como en Ripple, se obtengan unas pérdidas de 69% y del 22%, respectivamente, ya que las cotizaciones de dichas monedas se incrementaron mientras que el Bitcoin llevaba una dirección totalmente opuesta.

A la hora de computar los valores para el cálculo de la ganancia o pérdida patrimonial como consecuencia de la compraventa de criptomonedas, hay que tener en cuenta los gastos relativos a dichas operaciones. Esto ocurrirá en todos los tipos de criptomonedas. El valor de adquisición será el valor del mercado en el preciso momento y se incrementará con los gastos en los que se incurra para realizar la compra, tales como gastos de notaría o de gestoría, aumentando igualmente en los tributos que sean esenciales para la realización de dicha actividad. Por otro lado, el valor de transmisión o venta será el resultado del valor actual que en ese momento tenga la criptomoneda con la deducción de los gastos que se contrajeron para la adquisición de estas.

En relación con el Impuesto sobre el Patrimonio, será obligatorio incluir las criptomonedas en la declaración cuando la cuota tributaria resultante del conjunto de bienes y derechos del sujeto pasivo sea mayor a 700.000€[24]. Si el sujeto pasivo tiene un patrimonio inferior a dicha cantidad, en el que se encuentren las criptomonedas, no tendrá que hacer la declaración en relación con este tributo y, por lo tanto, no declarará las criptomonedas. En ese caso, solamente tributará la ganancia o pérdida en el Impuesto sobre la Renta de las Personas Físicas cuando provengan de una transmisión onerosa *inter partes*.

6.3. PROYECCIÓN FUTURA DEL BITCOIN.

En el momento de redacción de este trabajo, el Bitcoin se halla inmerso en una desmesurada crecida de su capitalización a pesar de la crisis económica mundial por la enfermedad de la COVID-19. La razón es que se está alcanzando la fecha para su “halving” o el cambio de era que se produce cuando se publican 210.000 bloques en la Blockchain y se debe a la expectativa de un freno en la emisión de monedas.

Esa reducción en la emisión ocurre cada 4 años: el primero se produjo en 2012, el segundo en 2016 y el tercero se estima que se produzca el próximo 12 de mayo del 2020.

El Bitcoin ha superado los 10.000 dólares estadounidenses por vez primera desde febrero, superando el 100% de revalorización en tan solo dos meses. La recompensa para los mineros se reducirá a la mitad a partir del 12 de mayo, de 12,5 BTC a 6,25 BTC.

Reducir a la mitad las recompensas de los mineros suponen, por lo tanto, una crecida exponencial del precio del bitcoin. Con el halving del año 2012, el precio del bitcoin pasó de 12,5 dólares a 665 dólares en tan solo un año y medio, lo que conlleva un aumento del 5.320%; mientras que en el halving del 2016, el bitcoin pasó de valer 650 dólares al máximo histórico de casi 20.000 dólares a finales de 2017. Este aumento supuso un crecimiento del 3.080%.

[24] Artículo 18 del Decreto Legislativo 1/2018, de 19 de junio, por el que se aprueba el Texto Refundido de las disposiciones dictadas por la Comunidad Autónoma de Andalucía en materia de tributos cedidos (BOJA núm. 123, de 27 de junio de 2018).

Por lo tanto, la expectativa está clara: un año y medio después del halving que se produzca este 12 de mayo, aproximadamente, se producirá el máximo absoluto de capitalización del Bitcoin, esto es, en torno al mes de noviembre del año 2021.

Existe un modelo desarrollado por un programador que se hace llamar “Plan B” denominado Stock-to-Flow y está relacionado con la escasez.

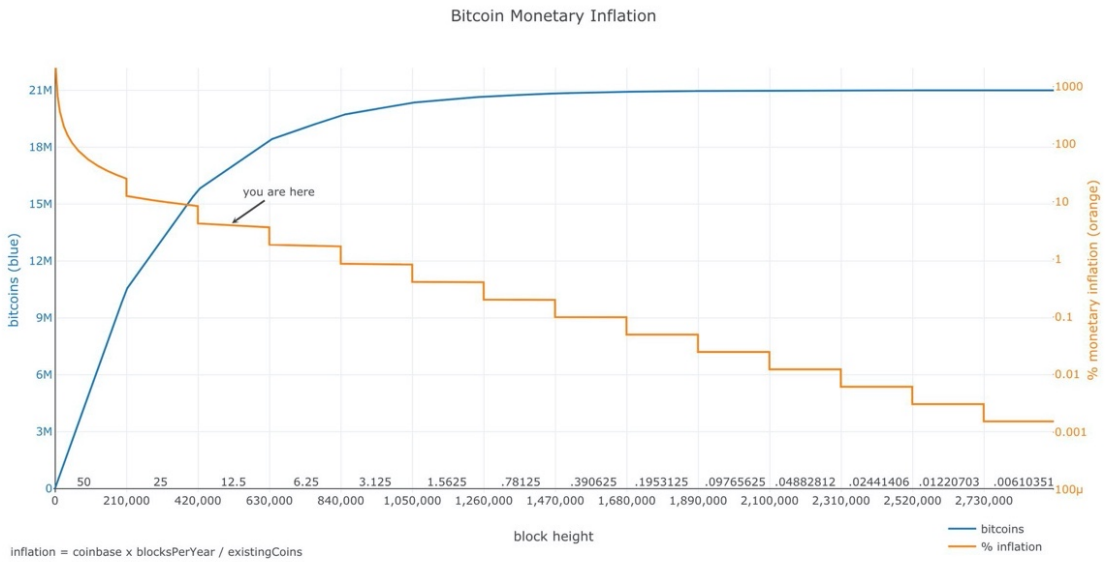
La escasez supone una situación en la que es difícil encontrar o hacerse con recursos que son altamente demandados y eso conlleva una subida de precio. Es lo que ocurre con el Bitcoin, al igual que con las antigüedades o la falta de suministros fósiles como el petróleo.

De esta forma, este programador establece una medición de la escasez basada en la fórmula SF:

$$SF = \frac{stock}{flujo}$$

Mientras que la primera variable, stock, supone el tamaño de las existencias actuales, el flujo es la producción de existencias anual.

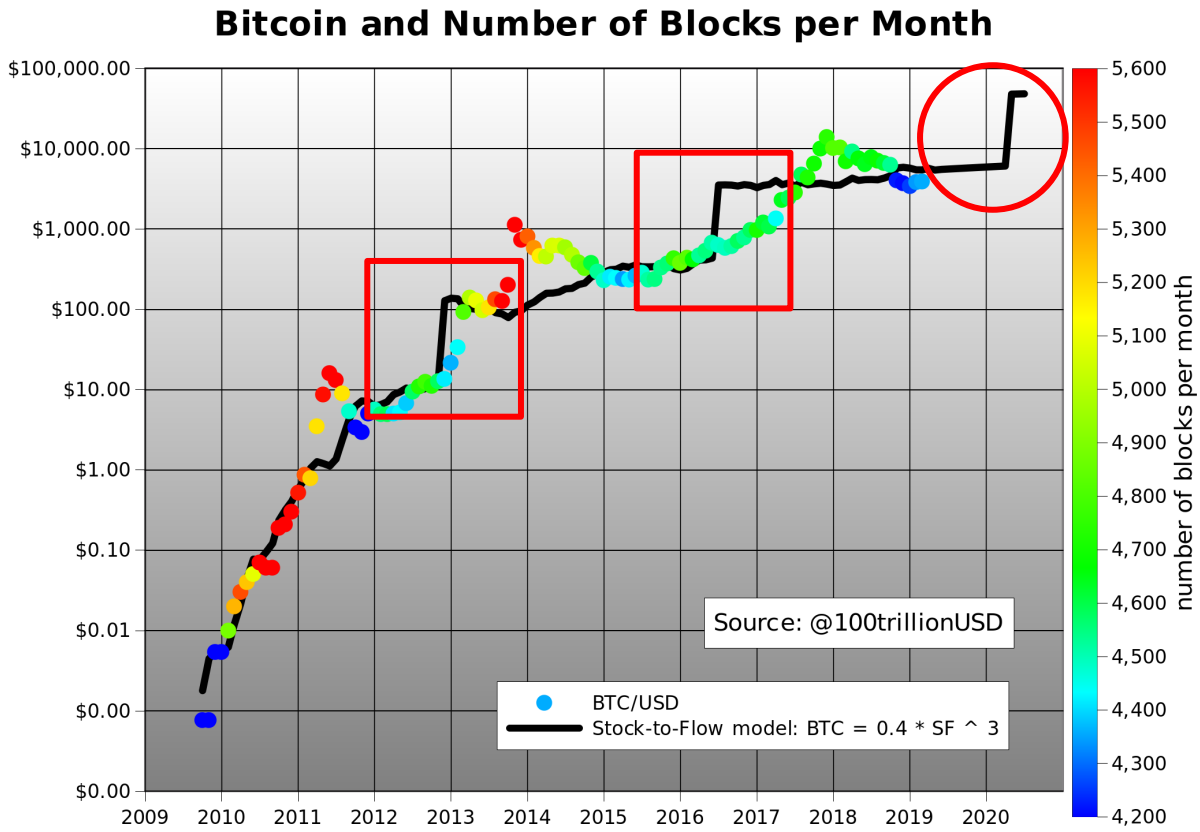
Figura 6.4. Crecimiento monetario del Bitcoin.



Fuente: http://plot.ly/~BashCo/5.embed

En la anterior figura se puede observar cómo la reducción de las recompensas son como consecuencia de un incremento de emisión de bitcoins. La emisión de monedas se va ralentizando porque se establece el límite máximo de 21 millones de monedas en circulación y se consigue reduciendo progresivamente la recompensa de los mineros o halving.

Figura 6.5. Bitcoin y número de bloques por meses.



Fuente: https://medium.com/@100trillionUSD/modeling-bitcoins-value-with-scarcity-91fa0fc03e25

En la anterior figura se observan tres variables: una línea temporal (desde 2009 hasta 2020), una línea económica (desde 0 dólares hasta los 100.000 dólares) y una línea que indica el número de bloques publicados por mes (desde 4.200 bloques a 5.600).

En la línea negra se muestra el SF bitcoin, el punto celeste muestra el valor real del Bitcoin con respecto al dólar en el tiempo y los puntos de los distintos colores indican el número de bloques publicados por mes. Como actualmente el Bitcoin se encuentra cercano al halving hay que tener en cuenta lo ocurrido en el 2012 y en el 2016, como se especificó anteriormente, para realizar una proyección futura del mismo.

Tras el halving del año 2012, con la consecuente reducción en la emisión, la cotización se disparó de manera inmediata. Con el halving del año 2016 se produce la misma situación pero de una forma más lenta, cuya razón puede deberse al crecimiento del Ethereum y al hackeo de DAO. Siguiendo con esta tendencia, el incremento que se producirá a partir del halving del año 2020 será el delimitado en el círculo en rojo de la gráfica anterior.

CAPÍTULO 7: CONCLUSIONES.

7.1. CONCLUSIONES.

Una vez analizado en profundidad el confuso y delicado mundo de las criptomonedas, en especial, el Bitcoin, se procede a dar unas pinceladas generales sobre el mismo. Se puede afirmar que la entrada del Bitcoin en el mercado ha supuesto la mayor lucha que se ha hecho en contra del sistema bancario tradicional, el cual quebrantó su propia transparencia con la crisis financiera mundial que se produjo en el año 2008.

Esta innovación disruptiva está haciendo que la industria monetaria internacional cambie y se adapte a la nueva era de la tecnología de la información y de la transparencia pero también de la privacidad y de la seguridad. Es la era de la Blockchain.

El Bitcoin aún no ha desplazado al dinero físico porque es difícil competir contra las principales divisas del mercado como son el euro o el dólar. Sin embargo, actualmente se encuentra en una posición equivalente al oro o a la plata, los materiales que respaldaban a las principales monedas antes del sistema fiduciario.

El Bitcoin no deja de ser un activo especulativo, rodeado por un riesgo enorme. Se puede perder absolutamente todo el valor de lo invertido fácilmente, porque no hay respaldo de ninguna autoridad que garantice su precio ni que responda por él. No existen mecanismos de protección como sí se establecen para el efectivo o para los valores que se depositan en las entidades de crédito por los ahorradores.

Este activo tan especulativo en el que predomina el riesgo, con una proyección actual alcista de su valor, se entiende tras lo analizado y por la complejidad del sistema que no cualquier ahorrador puede o debe invertir en este tipo de activos. El mercado de criptodivisas supone una mayor confusión que el mercado de valores y son programadores o pequeños inversores los que se atreven a introducir dinero en la compra de estas monedas virtuales. Ahora es el momento para invertir por parte de pequeños ahorradores que puedan y quieran hacer frente a ese riesgo.

Son muchas las ventajas que ofrece el Bitcoin frente a la moneda física, como el envío de dinero instantáneo sin apenas coste. Es una moneda inembargable, su seguridad basada en cifrados matemáticos hace que los usuarios efectúen transacciones bajo el anonimato. Es descentralizada, por lo que no depende de ningún intermediario ni ninguna autoridad financiera central. Es deflacionaria por su disminución de emisión de monedas con el paso del tiempo y además, es universal, libre y sus propietarios tienen el control absoluto de sus monedas.

Frente a ello, el Bitcoin tiene una serie de desventajas que el inversor debe tener en cuenta a la hora de depositar sus ahorros en este tipo de activos. El riesgo principal es la alta volatilidad, su falta de regulación, la posibilidad de hackeos en las cuentas y la pérdida de las contraseñas, la escalabilidad en cuanto a las transacciones por bloques, que son limitadas, y la custodia de las monedas ya que en el caso de perderlas, no será posible recuperarlas.

Tras el estudio realizado, es posible afirmar que el Bitcoin ha llegado con una pretensión y es desembarcar al sistema fiduciario, desenmascarar al sistema financiero y competir contra las principales divisas monetarias: el euro y el dólar.

El Bitcoin ha cambiado la visión del mercado de dinero tradicional.

CAPÍTULO 8: BIBLIOGRAFÍA.

0x noticias de Blockchain. (16 de mayo de 2019). Informe de PWC: los activos fijos de los fondos de cobertura de criptomonedas se triplicaron en el primer trimestre. Recuperado de https://es.0xzx.com/201905166075.html.

A. S. S. (8 de mayo de 2020). El Bitcoin, disparado en plena cuenta atrás para su "halving". *Exansión.* Recuperado de https://www.expansion.com/mercados/2020/05/08/5eb5319fe5fdea36778b45c4.html.

Academy bit2me. Explorado blockchain a fondo (IV): bloques. Recuperado de https://academy.bit2me.com/explorador-de-blockchain-a-fondo-bloques/.

Armknecht, F., Karame, G. O., Mandal, A., Youssef, F., & Zenner, E. (n.d.). Ripple: Overview and Outlook. Recuperado de http://www.ghassankarame.com/ripple.pdf

Asensio Borellas, V. J. (5 de julio de 2019). El Bitcoin: una primera aproximación jurídica en derecho civil español. *ElDerecho.com*. Recuperado de: https://elderecho.com/bitcoin-una-primera-aproximacion-juridica-derecho-civil-espanol.

Banco Central Europeo (13 de febrero de 2018). ¿Qué es el Bitcoin? Recuperado de https://www.ecb.europa.eu/explainers/tell-me/html/what-is-bitcoin.es.html.

Banco Central Europeo (26 de julio de 2019). Estadística sobre pagos: 2018. Recuperado de https://www.bde.es/f/webbde/GAP/Secciones/SalaPrensa/ComunicadosBCE/NotasInformativasBCE/19/presbce2019_103.pdf.

Beamonte, P. (27 de diciembre de 2018). 2018: el año del declive del Bitcoin. *Hipertextual.* Recuperado de https://hipertextual.com/2018/12/2018-declive-bitcoin.

Bernal, J. (15 de noviembre de 2018). Ethereum y su historia. *Criptoleaks.* Recuperado de https://criptoleaks.com/ethereum-historia/.

Binance Academy. Recuperado el 25 de marzo de 2020 de https://www.binance.vision/es/economics/the-2008-financial-crisis-explained.

Bitcoin organización: https://bitcoin.org/es

Carrasco Perera, A. (10 de julio de 2019). Sobre si el bitcoin es dinero con el que compensar daños y perjuicios. *Gómez-Acebedo & Pombo.* Recuperado de https://www.ga-p.com/publicaciones/sobre-si-el-bitcoin-es-dinero-con-el-que-compensar-danos-y-perjuicios/.

Cash, M. (23 de noviembre de 2019). ¿Cómo se determina el valor del Bitcoin? *Mercury.cash.* Recuperado de https://blog.mercury.cash/es/2019/11/23/como-se-determina-el-valor-del-bitcoin/.

Cointelegraph. ¿Qué es una "Hard Fork" (bifurcación dura)? Recuperado el 25 de abril de 2020 de https://es.cointelegraph.com/bitcoin-cash-for-beginners/what-is-hard-fork.

Cózar, R. C. (10 de febrero de 2020). El Bitcoin se vacuna del coronavirus y sube un 34% desde que comenzó la epidemia. *Crónica global.* Recuperado de https://cronicaglobal.elespanol.com/business/bitcoin-vacuna-coronavirus-sube-34-comenzo-epidemia_316979_102.html.

Criptonoticias (s.f.). ¿Qué es Ethereum? (ETH). Recuperado de https://www.criptonoticias.com/criptopedia/que-es-ethereum-eth/.

De la Cruz, I. (30 de diciembre de 2013). El abandono del patrón oro por Nixon, origen, causas y consecuencias. Recuperado de https://www.ismaeldelacruz.es/el-abandono-del-patron-oro-por-nixon-origen-causas-y-consecuencias/.

Dolater Retamal, C.; Bel Roig, J.; Muñoz Tapía, J.L.; (2017). La Blockchain: fundamentos, aplicaciones y relación con otras tecnologías disruptivas. *Economía industrial, 405, 33-40.*

El Economista. Diccionario de Economía. Recuperado el 24 de marzo de 2020 de https://www.eleconomista.es/diccionario-de-economia/dinero.

Fernández, F. (26 de junio de 2018). Cinco criptomonedas mueven más del 65% de todo el volumen del mercado. *Criptonoticias.* Recuperado de https://www.criptonoticias.com/mercados/cinco-criptomonedas-mueven-mas-65-todo-volumen-mercado/.

Gentile, N. [nategentile]. (7 de septiembre de 2017). Entiende Bitcoin y Ethereum - Explicación técnica a fondo en español sobre Criptomonedas [archivo de vídeo]. Recuperado de https://www.youtube.com/watch?v=YBNr69vrscw.

Horizen Academy. (Mayo de 2017). El movimiento Cypherpunk. Recuperado de https://academy.horizen.global/es/history/the-cypherpunk-movement/.

Iglesias, A. (13 de abril de 2020). ¿En qué se diferencia Bitcoin de Ripple?. *Criptotendencia.* Recuperado de https://criptotendencia.com/2020/04/13/en-que-se-diferencia-bitcoin-de-ripple/.

Jiménez, F. (octubre de 2010). *Elementos de teoría y política macroeconómica para una economía abierta. Segunda parte. Capítulo 6: Dinero y equilibrio en el mercado de dinero*. Recuperado de https://tmacroeconomica.files.wordpress.com/2010/09/elementos-de-teoria-y-politica-macroeconomica-para-una-economia-abierta-segunda-parte-capitulo-6-dinero-y-equilibrio-en-el-mercado-de-dinero.pdf.

Lansky, J. (Enero de 2018). Possible State Approaches to Cryptocurrencies. *Journal of Systems Integration. 9/1: 19-31. doi:10.20470/jsi.v9i1.335.*

Li, Y. (21 de diciembre de 2018). Nothing worked for investors this year — nearly every major asset class is in the red for 2018. *CNBC.* Recuperado de https://www.cnbc.com/2018/12/20/the-year-nothing-worked-every-asset-class-is-in-the-red-in-2018.html.

Lima, A. (19 de octubre de 2019). Comprender la criptografía: cómo funciona la criptomoneda [Parte 1]. *Morocotacoin.* Recuperado de https://www.morocotacoin.com/2019/10/comprender-la-criptografia-como-funciona-la-criptomoneda-parte-1/.

López Morales, G. (2 de noviembre de 2016). ¿Para qué se usa el dinero? *El Salmón Contracorriente.* Recuperado de https://www.elsalmoncontracorriente.es/?Para-que-se-usa-el-dinero.

Madeira, A. (21 de marzo de 2020). Fondo de inversión en criptomonedas se hunde después de que el precio de Bitcoin bajara a 3.800 dólares. Recuperado de https://es.cointelegraph.com/news/crypto-hedge-fund-goes-belly-up-after-bitcoin-price-drop-to-38k.

Mi Ethereum (s.f.). Bitcoins vs Ethereum. Recuperado de https://www.miethereum.com/ether/bitcoin-vs-ethereum/#toc1.

Mi Ethereum (s.f.). Smart Contracts o Contratos Inteligentes. Recuperado de https://www.miethereum.com/smart-contracts/#toc2.

Morales, J. (22 de diciembre de 2019). ¿Qué es halving? La recompensa por bloque y su impacto en Bitcoin. *Cointelegraph.* Recuperado de https://es.cointelegraph.com/explained/what-is-halving-the-reward-for-a-block-and-its-impact-on-bitcoin.

Muy Interesante. (15 de septiembre de 2017). El origen de las criptomonedas. Recuperado de https://www.muyinteresante.com.mx/ciencia-y-tecnologia/el-origen-de-las-criptomonedas/.

Nieto, A. (14 de febrero de 2018). Cuál es la diferencia entre criptomoneda, moneda virtual y dinero digital. *Xataca.* Recuperado de https://www.xataka.com/criptomonedas/cual-es-la-diferencia-entre-criptomoneda-moneda-virtual-y-dinero-digital.

Oro y Finanzas (27 de octubre de 2014). Definición criptomoneda: ¿qué es una criptomoneda? Recuperado de https://www.oroyfinanzas.com/2014/10/que-es-criptomoneda/.

Pastor, J. (24 de mayo de 2018). Cuando dos pizzas costaban 10.000 bitcoins: hoy equivaldrían a 70 millones de euros. *Xataca.* Recuperado de https://www.xataka.com/criptomonedas/cuando-dos-pizzas-costaban-10-000-bitcoins-hoy-equivaldrian-a-70-millones-de-euros.

Payeras Capellà, M. M.; Pere Isern Deyà, A.; Mut Puigserver, M. (2014). Lección 3: Introducción al Bitcoin. Islas Baleares: SeCOM de la Universitat de les Illes Balears.

Pedrosa, S. J. (10 de octubre de 2015). Moneda. *Economipedia.* Recuperado de https://economipedia.com/definiciones/moneda.html.

Plá Badenes, N.; Gambau-Suelves, B.; Navas Román, M. (2018). El concepto de criptomoneda y breves consideraciones en torno a su tributación. *Documentos de Trabajo 10/2018: VI Encuentro de Derecho Financiero y Tributario "Tendencias y retos del Derecho Financiero y Tributario" (1.ª parte). Instituto de Estudios Fiscales, 77-98.*

Plan B (22 de marzo de 2019). Modelando el valor de Bitcoin con escasez. *Medium.* Recuperado de https://medium.com/@100trillionUSD/modeling-bitcoins-value-with-scarcity-91fa0fc03e25.

Preukschat, A. (13 de enero de 2014). ¿Qué es, qué significa y para qué sirve un Hash en Bitcoin? (IV). *Oro y Finanzas.* Recuperado de https://www.oroyfinanzas.com/2014/01/hash-bitcoin-que-es-significa-sirve/.

Prialé, R. F. (4 de agosto de 2019). Contabilidad de triple entrada. *Café Viena.* Recuperado de https://www.cafeviena.pe/index.php/2019/08/04/contabilidad-de-triple-entrada/.

Ramires, A. (30 de enero de 2020). Te enseñamos todo sobre las transacciones irreversibles en Bitcoin. *Criptogaceta.* Recuperado de https://criptogaceta.com/aprende/te-ensenamos-todo-sobre-las-transacciones-irreversibles-en-bitcoin/.

REAL ACADEMIA ESPAÑOLA: *Diccionario de la lengua española,* 23.ª ed., [versión 23.3 en línea]. <https://dle.rae.es/criptograf%C3%ADa> [24 de marzo de 2020].

Redsys. (11 de agosto de 2016). ¿Qué es el P2P?: definición y usos. *Redsys.* Recuperado de https://blogreds.es/medios-pago/que-es-el-p2p-definicion-y-usos-1.

Rojas, E. (16 de abril de 2019). ¿Qué es Ripple y cómo funciona la "criptomoneda de los bancos"?. *Cointelegraph.* Recuperado de https://es.cointelegraph.com/explained/what-is-ripple-and-how-it-works.

Roldán, P.N. (30 de abril de 2017). Dinero electrónico. *Economipedia.* Recuperado de https://economipedia.com/definiciones/dinero-electronico-2.html.

Romero, D. (3 de marzo de 2020). 2020: ¿un gran momento para invertir en Bitcoin? *El País Financiero.* Recuperado de https://elpaisfinanciero.com/invertir-en-bitcoin/

Rosembuj, T. (2015). *Bitcoin*. Barcelona, España: El Fisco.

Segarra, P. (27 de septiembre de 2019). Criptomonedas: ventajas, riesgos y futuro según tres expertos. *20 minutos.* Recuperado de https://www.20minutos.es/noticia/3776869/0/criptomonedas-bitcoin-divisas-digitales-criptodivisas/.

Sevillano, E. (11 de marzo de 2020). La OMS declara el brote de coronavirus pandemia global. *El País.* Recuperado de https://elpais.com/sociedad/2020-03-11/la-oms-declara-el-brote-de-coronavirus-pandemia-global.html.

Tena, M. (1 de febrero de 2016). ¿Cuánto vale un bitcoin? *BBVA.* Recuperado de https://www.bbva.com/es/cuanto-vale-bitcoin/.

Tori, M. (21 de marzo de 2020). Un mes de confinamiento en Italia en cinco hitos. *Público.* Recuperado de https://www.publico.es/internacional/coronavirus-mes-confinamiento-italia-cinco-hitos.html.

Trecet, J. (23 de marzo de 2020). Invertir en bitcoins: lo que debes saber. *Finect.* Recuperado de https://www.finect.com/usuario/Josetrecet/articulos/invertir-bitcoins-debes.

Trincado, B. (26 de diciembre de 2019). El pago con efectivo se desploma y la brecha con las tarjetas toca máximos. *Cinco Días.* Recuperado de https://cincodias.elpais.com/cincodias/2019/12/26/companias/1577362666_510576.html.

Vanci, M. (23 de abril de 2020). Bitcoin resiste la crisis económica por coronavirus y hasta se fortalece, según análisis. *Criptonoticias.* Recuperado de https://www.criptonoticias.com/mercados/bitcoin-resiste-crisis-economica-coronavirus-hasta-fortalece-analisis/.

Villalba García, R. (13 de febrero de 2020). Impuestos y tributación de bitcon y criptomonedas. *Asepyme.* Recuperado de https://asepyme.com/impuestos-y-tributacion-de-bitcoin-y-criptomonedas-irpf-iva-itp-ip-is/#Tributacion_del_bitcoin_en_el_IRPF.

Wanden-Berghe Lozano, J. L. y Fernández Daza, E. (2018). *Una propuesta de aplicación de la contabilidad en Blockchain.* Recuperado de https://aeca.es/wp-content/uploads/2014/05/80g.pdf.

Wuhan, EFE. (8 de abril de 2020). Wuhan recupera su libertad: las imágenes del fin del confinamiento. *La Vanguardia.* Recuperado de https://www.lavanguardia.com/internacional/20200408/48385877056/wuhan-fin-confinamiento-imagenes-coronavirus.html.