GRADO EN COMERCIO

TRABAJO FIN DE GRADO

“Nuevas tendencias en medios de pago. Blockchain y Criptomonedas.”

JACOBO DEL CAÑO ZAMORA

FACULTAD DE COMERCIO VALLADOLID, MAYO 2022

FACULTAD DE COMERCIO
Universidad de Valladolid

UNIVERSIDAD DE VALLADOLID, GRADO DE COMERCIO

CURSO ACADÉMICO 2021/2022

TRABAJO FIN DE GRADO

“Nuevas tendencias en medios de pago. Blockchain y Criptomonedas.”

Trabajo presentado por: Jacobo Del Caño Zamora

Tutor: José Ignacio Pérez Garzón

FACULTAD DE COMERCIO

Valladolid, junio 2022

CONTENIDO

1. Introducción 6

1.1. Motivo de elección del tema seleccionado 6
1.2. Agradecimientos 7

2. Nuevos medios de Pago 8

2.1. Introducción 8

2.1.1. Trueque 8
2.1.2. Moneda 8
2.1.3. Papel-Moneda 9
2.1.4. Era moderna 9

2.2. ¿Fin del dinero tal y como lo conocemos? 10
2.3. Medios de pago digitales 12

2.3.1. Tarjetas bancarias 12
2.3.2. PayPal 13
2.3.3. Transferencia bancaria 14
2.3.4. Financiación 14
2.3.5. Pago móvil 14
2.3.6. Criptomonedas 15

2.4. Nuevas tendencias de pago 16

2.4.1. Compras a través del teléfono 16
2.4.2. Pagos invisibles. 18
2.4.3. Pago fraccionados 18
2.4.4. Otras tendencias 19

3. Blockchain 20

3.1. ¿Qué es el Blockchain? 20
3.2. Características del Blockchain 21

3.2.1. Peer to Peer 21
3.2.2. Consenso, o nula dependencia 22
3.2.3. Proof of work 22
3.2.4. Seguridad 22
3.2.5. Transparencia 23
3.2.6. Descentralización 23

3.3. ¿Cómo funciona? 24
3.4. Tipos de Blockchain 25

3.4.1. Publicas 25
3.4.2. Privadas 25
3.4.3. Híbridas 26

3.5. Aplicaciones del Blockchain 26
3.5.1. Almacenamiento en la nube 27
3.5.2. Registros de datos 27
3.5.3. Sistema de votaciones electrónicas 28
3.5.4. Smart Contracts 28
3.5.5. Sistemas financieros y monedas digitales 30
3.5.6. Cadenas de suministros 31
3.5.7. Industria 4.0 e Internet de las cosas 31
4. Criptomonedas 33
4.1. Orígenes 33
4.2. Criptografía 35
4.2.1. Tipos de criptografía 35
4.3. Características de las criptomonedas 36
4.3.1. Características generales 37
4.3.2. Ventajas frente a sistemas tradicionales 38
4.4. Monederos 39
4.5. Bitcoin 41
4.6. Ethereum 45
4.7. Otras criptomonedas importantes 47
4.7.1. Tether y las stablecoins 47
4.7.2. Ripple, Litecoin y Cardano 48
4.8. Fiscalización de las criptomonedas 48
4.8.1. Criptomonedas como medio de pago 48
4.8.2. Criptomonedas como inversión 48
4.8.3. Criptomonedas como actividad económica, minería. 49
4.8.4. Fiscalidad de los NFT 49
4.9. Contabilidad de las criptomonedas 49
5. Conclusiones 51
6. Bibliografía 53

Índice de Ilustraciones y Gráficos

Gráfico 1 Dispositivos utilizados para comprar online en España 2016-2021 (en %) 17
Gráfico 2 Uso del Bizum por generación, en España (% del gasto total) 17
Gráfico 3 Evolución tasa de cambio €/$, 1999-2012..... 33
Gráfico 4 Evolución histórica de la tasa de cambio del BTC respecto al $..... 44
Gráfico 5 Evolución histórica de la tasa de cambio del ETH respecto al $..... 46
Gráfico 6 Volumen de negocio de los NFTS en millones de dólares 47

Ilustración 1 Trueque..... 8
Ilustración 2 Dracmas Griegos 9
Ilustración 3 Papel moneda chino..... 9
Ilustración 4 Cuentas Bancarias y PayPal 12
Ilustración 5 Apple Pay..... 15
Ilustración 6 Bitcoin y monedero..... 16
Ilustración 7 Click and collect, El Corte Ingles 18
Ilustración 8 Comparativa entre sistemas centralizados y descentralizados..... 21
Ilustración 9 Funcionamiento del Blockchain..... 25
Ilustración 10 Microsoft Azure 27
Ilustración 11 Funcionamiento de un Smart Contract 30
Ilustración 12 Emisión y recepción de un mensaje con criptografía asimétrica..... 36
Ilustración 13 Tipos de monederos de criptomonedas..... 40
Ilustración 14 Monedero Ledger..... 40
Ilustración 15 Búsqueda de “Bitcoin” en Google, desde su origen..... 41
Ilustración 16 Logo del Bitcoin..... 42
Ilustración 17 Mensaje original de Laszlo Hanyecz 42
Ilustración 18 Bitcoin aceptado por Microsoft 45
Ilustración 19 Logo de Ethereum..... 45
Ilustración 20 Logo de Tether..... 47

1. Introducción

1.1. Motivo de elección del tema seleccionado

El principal motivo de selección de este tema ha sido mi desconocimientoen el mismo y mis ansias de adquirir conocimientos sobre una de las tecnologíasque están a punto de cambiar, si no lo han hecho ya, la forma que tenemos de ver este mundo.

Como estudiante de comercio los medios de pago son una pieza fundamental en el eje de mis estudios, todas las empresas realizantransacciones, y también los particulares, seas empresario o no. Actualmente vivimos en un mundo con un sistema económico que consideramos sólido, y enel que confiamos, porque esa es la base que lo sustenta, la confianza, pero hayalternativas, compatibles y sustitutivas a este sistema.

El Blockchain y las criptodivisas se crearon con un objetivo, ser una alternativa al sistema actual, responder a un sistema con gran inflación y brechascomo se pudo apreciar tras la gran crisis económica de 2008. La tecnología sirvepara cambiar el funcionamiento de la sociedad, para mejorar, buscar eficiencia ygarantizar una mejor calidad de vida de las personas, el Blockchain busca justoeso, hacer un sistema mucho más ágil, sin depender tanto de las personas y para las personas, un sistema mucho más seguro, sin fugas de datos ni de información, y un sistema independiente.

Al igual que yo no conocía mucho sobre este tema antes de realizar estetrabajo, muchas otras personas no lo conocen, todos hemos oído cosas como “invirtió la paga que le dieron y ahora es millonario” pero ninguno nos atrevemosa poner el pie en este campo e investigar al respecto. Mi objetivo con este trabajoes recopilar toda la información posible acerca de las criptomonedas y el bitcoin,para descubrir yo mismo de que trata esta nueva tecnología, que busca, qué ventajas tiene respecto al sistema actual, y que desventajas, así como descubrircómo puede cambiar y beneficiar a toda la sociedad global.

A lo largo de la carrera he ido consiguiendo, aprendiendo y asimilando información sobre economía, derechos, imposiciones, dirección de empresas, marketing, etc. todo enfocado a empresas y negocios, por lo que este trabajo defin de carrera, o de grado, el TFG, busca de una forma personal completar y complementar mis conocimientos en todos esos ámbitos con información sobrela que busca ser una de las grandes invenciones de este siglo, tanto económica como socialmente.

El TFG hace referencia a tres pilares principales a tratar: los medios de pago, los nuevos y por ende los antiguos, el Blockchain que da vida a estos nuevos medios, y por ultimo las criptomonedas.

Tanto el Blockchain como las criptomonedas son tecnologías en desarrollo por lo que lo tratado y mencionado en este TFG puede que, en el futuro, con más desarrollo cambie, el potencial es infinito.

Las criptomonedas son medios de pago, pero actualmente se tratan más como “mercancías”, o productos, y como todo producto puede triunfar, o desaparecer, hay quienes creen que sustituirán al sistema actual y otros que lo consideran una estafa a gran escala, pero de nuevo, eso es algo que aún no sepuede responder.

1.2. Agradecimientos

Me gustaría, antes de entrar en materia, agradecer tanto a mi tutor del TFG, José Ignacio Pérez Garzón por su paciencia a la hora de tutorizar este trabajo, así como por toda su labor realizada en las asignaturas que me ha impartido durante toda la carrera.

Y por supuesto me gustaría dar las gracias a Eulogio Alonso, el cual, de una forma absolutamente desinteresada en cuanto se enteró de que iba a tratar mi TFG, tras una conversación de apenas media hora y sin apenas conocerme, me ofreció una serie de artículos suyos y de sus colegas sobre el tema para que los usase de forma exclusiva para lograr un trabajo mucho más completo, y tratase unos temas que mucha gente olvida, los aspectos fiscales y contables del tema.

Además, también quiero agradecer a todos los profesores que me han impartido clase durante estos 4 años de carrera.

Muchísimas gracias.

2. Nuevos medios de Pago

2.1. Introducción

A lo largo de la historia los seres humanos hemos variado los medios de pago tanto en esencia como en forma a medida que avanzábamos y nos desarrollábamos. A día de hoy, en la época phygital lo esencial es ofrecer e integrar todos los métodos de pago posibles para que la transacción se pueda realizar satisfactoriamente.

Antes de hablar del presente, y del futuro como son las criptodivisas debemos mirar hacia atrás, ver como hemos cambiado y como todas esas propuestas que en su día debieron de considerarse “locuras” acabaron sustituyendo al modelo que había, o complementándolo.

2.1.1. Trueque

El primer punto que debo tratar para habar de transacciones y medios de pago es el trueque, ya que además tiene mucho que ver con el origen de la valorización de las criptodivisas en concreto las bitcoin. El trueque es a día de hoy el primer método de pago conocido de la historia, el cual consistía en un acuerdo voluntario entre dos partes las cuales atribuían un valor a sus pertenencias y los empleaban como “moneda” para realizar la transacción. El método más simple, yo te doy una cosa que quieres por otra que yo quiero.

Ilustración 1 Trueque

Fuente: Colegio El Valle

Antes de continuar al siguiente punto conviene decir que cada civilizacióntuvo un ritmo diferente por lo que mientras en una civilización se usaba un método en la otra se seguía usando el anterior y/o viceversa.

2.1.2. Moneda

En la civilización occidental el siguiente avance se produjo en la Antigua Grecia, allí por el siglo VII antes de Cristo, y se trata de la moneda, llamada Dracma. Este nuevo medio de pago, que sustituyó al trueque consistía en fabricar con metales preciosos (oro, plata y bronce) objetos con un valor calculado según el peso y el metal del que estuviese fabricada. La base de estemedio de pago y su valor era el propio valor del metal, el Patrón Oro.

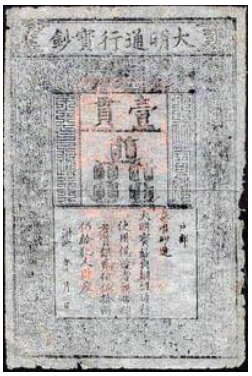
Ilustración 2 Dracmas Griegos

Fuente: blognumismatico.com

Con las monedas y los metales a lo largo de la historia se produjeron las primeras grandes devaluaciones de valor, por ejemplo, en el siglo XIV, a raíz de las importaciones de plata desde América por parte de los españoles, al haber exceso de plata, el valor de las monedas de plata cayó. En definitiva, era un sistema muy variable según la cantidad de metal en circulación.

2.1.3. Papel-Moneda

Ilustración 3 Papel moneda chino



Fuente: AEHE

Posteriormente, en el siglo XVII surgió en Suecia una nueva forma y mediode pago, los billetes, el papel-moneda. Un medio de pago que aún nos dura, al igual que las monedas, aunque la forma de valorar estas ha cambiado ya que junto al papel-moneda llegó el sistema fiduciario, sistema en el cual el valor del medio de pago no lo tenía el mismo, sino que la base de este modelo es la confianza de la sociedad en él.

El valor y la emisión del dinero dentro del sistema fiduciario está controlado y gestionado por organismos, como los bancos centrales o lasreservas nacionales, así como instituciones (FMI, BCE, BEI, etc.) los cuales velan por la autenticidad del sistema además de garantizar a la sociedad su valor.

2.1.4. Era moderna

Al llegar a la era “moderna” llegaron las tarjetas con todos sus tipos, crédito, débito, revolving, prepago, etc., aunque la primera concretamente fue creada por la Western Union como una tarjeta de fidelización para sus clientes vip, con accesoa un crédito para realizar las compras.

Y una vez alcanzado este punto podríamos decir que ya hemos tratado los medios de pago “tradicionales”, o más básicos, los que no requieren tener experiencia con las nuevas tecnologías, lo cual no pasa con los siguientes mediosde pago a tratar, los cuales están en auge y luchando por sustituir al efectivo tradicional, los medios digitales.

Acompañando a las tarjetas y al ecommerce han surgido los Wallets, o monederos digitales, los cuales son aplicaciones digitales en las que puedes introducir tus tarjetas y cuentas bancarias, además de las cuentas y tarjetas de fidelidad, socio de cines, restaurantes, tiendas, etc. Se han visto potenciados por el auge e implantación mayoritaria de los smartphones, y accesorios, en la sociedad, y han sido impulsados e implantados desde 2014 por las grandes empresas detecnología: Google Pay, Apple Wallets, Samsung Pay, etc.

Los Wallets no han sido los únicos medios de pago que han surgido, en 2009 empezó a surgir y a circular por la red una propuesta de un nuevo modelode pago sustentado por el Blockchain, las llamadas Bitcoin, y sus hermanas posteriores.

A día de hoy más de 20 millones de personas poseen Bitcoins, la mayoríaen los mayores núcleos de población lo cual ha hecho que empresas tradicionales de los países desarrollados comiencen poco a poco a plantearse eimplantar como opción de pago el uso de ese modelo puramente digital.

Todo esto nos lleva al siguiente punto de este trabajo el cual consistirá en una cuestión que cada ver resuena más en la sociedad: “¿Estamos ante los últimos días del dinero, tal y como lo conocemos hoy?”.

2.2. ¿Fin del dinero tal y como lo conocemos?

Cada vez más los pagos se producen por medios digitales, incluso a nivel minorista, el peso del efectivo en los pagos está cayendo y muchos economistas, empresas e incluso la opinión pública están afirmando que la era del efectivo seestá acabando.

Pasar de medios de pago físicos a puramente digitales está haciendo quese agilicen todos los pagos, desde una compra familiar hasta pagos transfronterizos que anteriormente eran caros, lentos y de difícil rastreo.

Algunos bancos están empezando a producir o a plantear sus propias monedas digitales además de dando “luz verde” a plataformas de estas (el Banco de España ha dado validez a la plataforma Bit2Me este pasado febrero; EL PAIS, 2021) y, sumado al auge social y económico de las criptodivisas la afirmación de que serían una moda pasajera que no afectaraal mercado financiero ha comenzado a cuestionarse.

Un informe del FMI de 2019 afirmaba que en el mundo se lavan alrededor de dos billones de dólares anuales procedentes de actividades ilícitasno reguladas, con el fin del anonimato de estas actividades esto podría frenarse.Aunque a nivel práctico se

acabarían encontrando otras formas de realizar talesactividades evitando la detección ¿tal vez una vuelta a un sistema de trueque?

Para los consumidores también es un avance ya que facilita el acceso para realizar transacciones sin necesidad de usar una tarjeta física o una cuentadel banco.

Otra de las virtudes seria la seguridad de no deber tener precaución con el efectivo y con miedo de pérdida o robo físico. Ya que el robo solo puede darse mediante hackeos y perdida de la clave personal, la cual debe ser intransferible porque de ella depende el acceso a tu dinero.

Aunque como todo, tiene luces y sombras como perder el anonimato a la hora de realizar una transacción, quedando está registrada, y por supuesto, la más relevante, el hecho de que no todas las personas tienen los conocimientos necesarios para dar este salto. De hecho, aún hay personas que van frecuentemente a su sucursal más cercana para actualizar la cartilla, por lo que ni siquiera han empezado a dar el paso al cambio. Actualmente hay un gran problema de educación digital que debe solventarse para dar el paso.

A nivel de dividas no deberia haber muchos cambios yaque, a día de hoy la gran mayoría, por no decir todas, de las operaciones entre distintos países y fronteras ya se realizan a través de medios digitales.

Otra consecuencia del fin del efectivo y dinero tradicional, ligada al acceso más simplificado a las futuras monedas de las reservas centrales seria la disponibilidad de las grandes monedas mundiales, como por ejemplo el dólar digital, en cualquier país del mundo, lo que permitiría sustituir las monedas de países pequeños o con economías y gestiones frágiles o de nula confianza, permitiéndoles usar unos medios de pago de mayor confianza y valor.

A finales de 2019 la compañía INTRUM, afirmaba en su Informe Europeo de Pagos que más del 43% de empresas minoristas y mayoristas de España considera que alrededor de 2030 el dinero en efectivo será sustituido por pagos digitales, aunque en Castilla y León Murcia y Galicia esa cifra no llegaba al 30%. En su mismo informe del año 2021 esos datos rondaban el 75%. (INTRUM, 2019, https://www.intrum.es/soluciones-empresariales/sala-de-prensa/noticias/3-de-cada-4-empresas-espanolas)

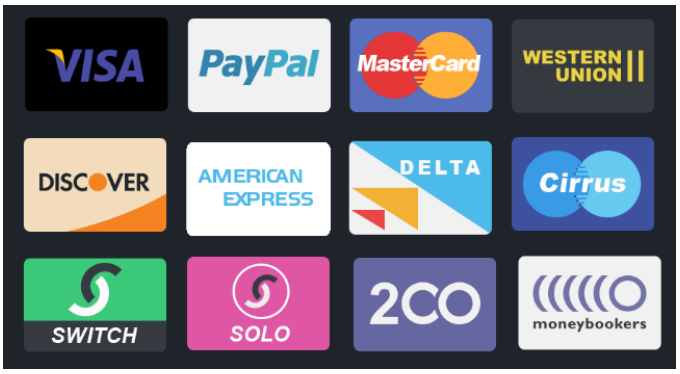
Países como Suecia, Noruega y Dinamarca ya están dando pasos para que esto suceda, incluso España presentó en 2020 un plan para reducir el uso del efectivo en el país, actualmente el límite de pagos en efectivo está en 2500€ y el gobierno desea reducirlo a 1000€ como en Francia o Portugal, nuestros vecinos, no obstante el Banco

Central Europeo no lo permitió, afirmando que sería reducirlo demasiado y que en caso de problemas electrónicos el efectivo puede seguir usándose para garantizar transacciones legitimas. (Xakata.com, 2020)

Lo que es una certeza es que a día de hoy hemos llegado a un punto de nulo retorno, los medios digitales han llegado para quedarse. El siguiente punto de este trabajo hace referencia precisamente a esos nuevos, yano tanto, medios de pago en el mercado.

2.3. Medios de pago digitales

Ilustración 4 Cuentas Bancarias y PayPal



Fuente: MagazineTeralco

2.3.1. Tarjetas bancarias

En la actualidad la forma más simple de pago online estandarizada son las ya mencionadas anteriormente tarjetas, de crédito y de débito, más concretamente Visa, MasterCard, etc., las cuales la gran mayoría del mundo poseen y saben utilizar por su sencillez, simplemente deberás añadir el númerode tu tarjeta, la fecha de caducidad y el código trasero y ya estarás realizando sin problema pagos online en todas las tiendas online (Amazon, El Corte Inglés,Carrefour, etc.).

Las ventajas de las tarjetas son:

- su **inmediatez**, ya que no necesitas intermediarios para realizar el pago, ya se encarga el banco de efectuarlo una vez que tu confirmes la compra
- su **seguridad**, la que te otorgan los propios bancos
- su **alta aceptación** en la mayoría de las tiendas, por no decir todas
- su **altísima confianza** otorgada por los clientes y el respaldo de las entidades

Mientras que **los contras** de este medio de pago son:

- las **comisiones** para los distintos vendedores que varían según el emisor de la tarjeta en cuestión
- el **grado de adaptación de estas** ya que tienen limitaciones como el No poder realizar grandes pagos a través de ellas.

2.3.2. PayPal

Además de las tarjetas el otro medio de pago más conocido y usado por los consumidores es PayPal, aunque actualmente está cayendo en desuso. PayPal surgió en 1998, y pasó a ser una filial de eBay en 2002.

Como anotación sobre PayPal hay que señalar que, de trabajadores de esta, apodados como, “La Mafia de PayPal” surgieron otras empresas comoson Tesla, LinkedIn, SpaceX, YouTube, etc., varias de ellas (Tesla y SpaceX)fundadas por Elon Musk una de las personas más influentes en el mercado de criptodivisas.

Una vez comentado esto toca remarcar la función de PayPal que es la deser una plataforma de gestión de pagos electrónicos, la cual en su día revolucionó los pagos online, la cual funciona como intermediaria a la hora de efectuar una compra. Funciona a través de una tarjeta vinculada a la cuenta de la aplicación.

Las **ventajas** que nos ofrece son:

- Su **valor como marca**, lo cual le da una alta confianza.
- el **respaldo de las instituciones bancarias**
- su **gran integración** en la mayoría de las tiendas online
- la **privacidad** que ofrece a los consumidores ya que no deben otorgar todos sus datos personales a la hora de realizar las operaciones

Y por otro lado las **desventajas** de este medio de pago son:

- las **comisiones** por cada transacción (variables desde 3,5% hasta 2% según el volumen de compra)
- **necesidad de un intermediario**, por lo que el cliente no paga directamente en la tienda y que el pago no pasa inmediatamente.

2.3.3. Transferencia bancaria

El tercer método de pago más integrado en las tiendas online es la transferencia bancaria, el cual es un método mucho más sencillo que PayPal yaque son las propias entidades bancarias los intermediarios.

Las **ventajas** de este modelo son bastante similares a las de las tarjetas bancarias**, la confianza** otorgada por los bancos a sus clientes**, la seguridad a través de la protección de datos** y el hecho de **no tener comisiones para el vendedor.**

Mientras que la **desventaja** principal de este sistema es la **operatividad** debido a que el banco debe efectuar los pagos y esto puede producir grandes retrasos de hasta 24 horas haciendo que el pedido se demore también.

2.3.4. Financiación

El siguiente método, menos empleado por los consumidores generales,pero más por las PYMES o empresas es la financiación.

A través de este método de pago el cliente llega a un acuerdo con una entidad, para fraccionar los pagos en cuotas y los plazos de financiación.

Hay distintas empresas encargadas de realizar estas financiaciones, algunas conocidas son Aplázame o Instant Credit, o las mismas entidades bancarias.

La ventajas de este medio son la rapidez de pedido ya que el vendedor recibe todo el dinero en el momento de solicitud y la reducción de impagos.

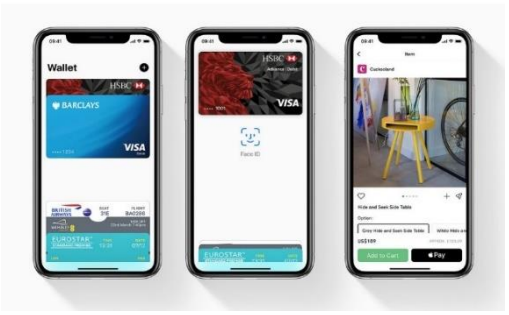
Y las desventajas para el consumidor son que el proceso de pago sealarga en el tiempo.

2.3.5. Pago móvil

Los pagos a través del móvil tienen muchísimas variables, hay pagos contarjeta a través del móvil usando la característica NFC de los dispositivos con aplicaciones tales como Samsung Pay, WeChat Pay (sustituto de WhatsApp enChina), Apple Pay, Google Pay, y las aplicaciones de los propios bancos como Santander Wallet entre otros.

Además, en los Wallets o carteras digitales donde guardamos nuestras tarjetas del banco, también podemos guardar las tarjetas de socio de cualquier negocio, como, Yelmo Cines, Zara, Scalpers, entre otros.

Ilustración 5 Apple Pay



Fuente: Apple

Otra opción, en auge desde hace unos años y muy aceptada ya en muchas tiendas minoristas, y por supuesto mayoristas, es el Bizum, una aplicación asociada a los principales bancos a través de la cual podemos realizar transferencias directas tanto de pequeñas como grandes cantidades de dinero, sin comisiones, y de forma instantánea.

Según un estudio realizado por Pecunpay, una Fintech española, en el que participaron 2000 personas en diciembre de 2020, más del 34% de los participantes afirman realizar pagos con el móvil frecuentemente, y alrededor deun 10% los utiliza siempre que se dé la opción, incluso en tiendas físicas. Las tarjetas de crédito y débito siguen siendo el medio de pago favorito en tiendas físicas con un 60%.

Las ventajas que ofrecen los pagos con el móvil son las siguientes:

- La facilidad de pago a través de las habilidades, aunque aún no todala población sabe manejar las nuevas tecnologías.
- El respaldo de todas las entidades, o la gran mayoría, y las propiasmarcas de los smartphones para otorgar fiabilidad y seguridad.
- La reducción de contacto entre personas, algo que se ha acrecentadogracias a la pandemia.
- La rapidez de los pagos y cobros, siendo casi instantánea.

Y como única desventaja remarcable, y cada vez con menos peso, el hecho de que no todos los dispositivos son compatibles con las aplicaciones porsus versiones. Actualmente se renueva el smartphone cada pocos años, y se tienen wearables tales como las Mi Band o Apple Watch los cuales también cuentan con NFC, por lo que este problema o desventaja tiene una fácil solución.

2.3.6. Criptomonedas

Este medio de pago es el tema principal de este trabajo de fin de grado, por lo que será tratado más en profundidad más adelante, hablando de su origen, funcionamiento, sus distintas monedas, y sus características y funciones, pero como

pequeño resumen previo cabría decir que aún no están implantadas, aceptadas y sobre todo conocidas por los negocios minoristas o mayoristas ni por la sociedad.

Son un medio de pago que poco a poco va usándose más pero aún estáen proceso de aceptación social porque aún no cuentan con el respaldo de las entidades internacionales.

Ilustración 6 Bitcoin y monedero

Fuente: Esic.edu

Este medio de pago actuaria de una forma similar a un pago con tarjeta o con Bizum, pero eliminando a las entidades como intermediarios, garantizan unaseguridad casi absoluta gracias a los algoritmos y el Blockchain, y un seudoanonimato (ya que siempre puede ser identificado si las autoridades lo requieren) a la hora de realizar las operaciones. Son pagos inmediatos, sin falsificaciones, universal y con comisiones ínfimas o nulas, que poco a poco deberán ir aceptándose igual que lo han hecho los Wallets o Bizum, pero a nivel global, gubernamental y comercial.

2.4. Nuevas tendencias de pago

Gracias a la aparición de los nuevos medios de pago ya mencionados (Wallets, Criptomonedas, etc.) y sumado a la pandemia, aunque ya empezaron a surgir antes, han aparecido una serie de nuevas tendencias en los pagos, principalmente ecommerce las cuales buscan ofrecer a los clientes todas las facilidades posibles, garantizando la seguridad de sus pagos y ahorrando tiempo a la hora de efectuar los pagos.

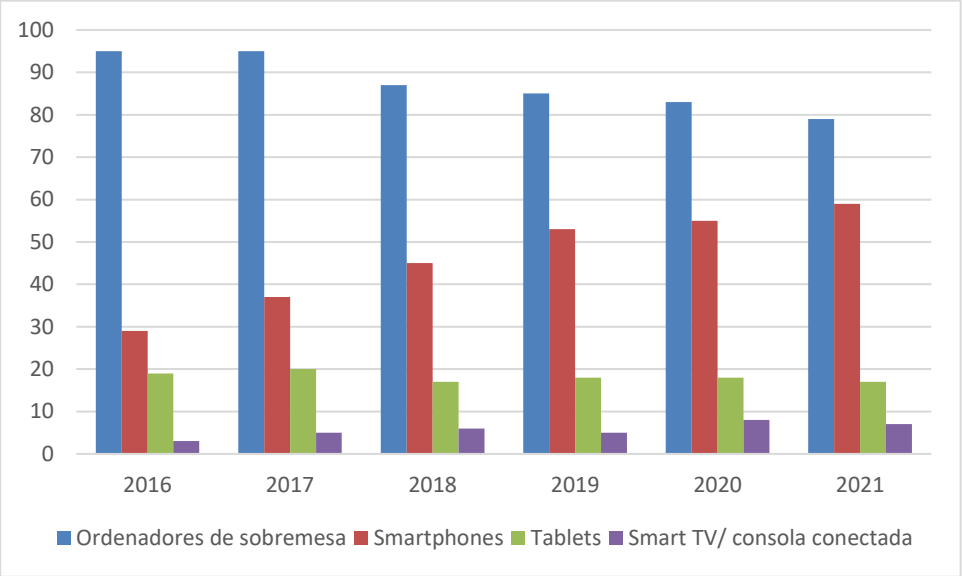
Algunas de estas tendencias son:

2.4.1. Compras a través del teléfono

El teléfono móvil como ya hemos mencionado hace, las funciones de tarjeta tradicionales, por lo que puedes pagar en cualquier establecimiento sin necesidad de llevar una encima.

Otro factor que demuestra esta tendencia es el hecho de que muchas de las compras realizadas por internet las realizamos a través del móvil, siendo la segunda plataforma de compra online, por detrás del ordenador.

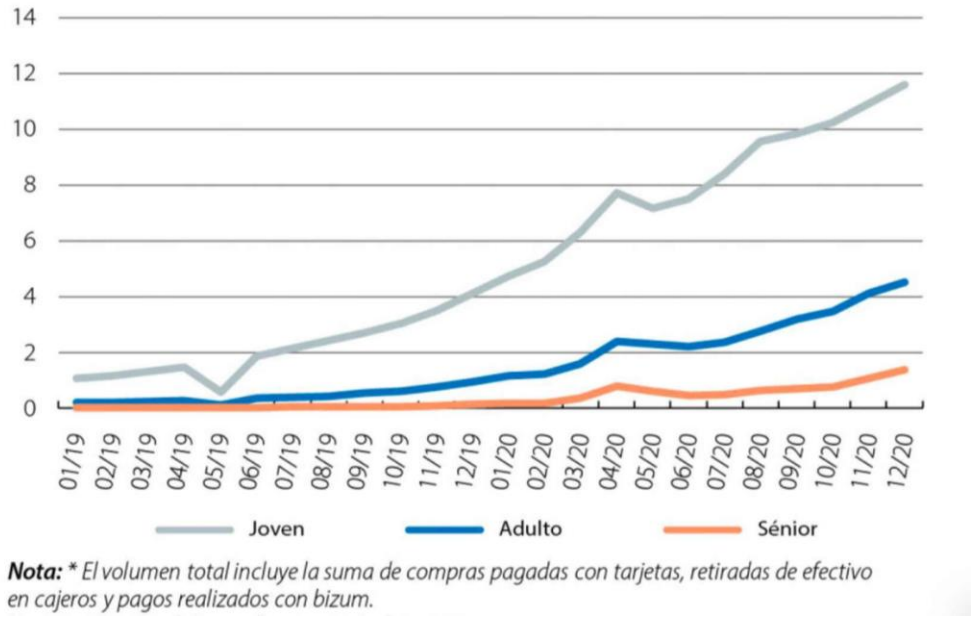
Gráfico 1 Dispositivos utilizados para comprar online en España 2016-2021 (en %)



Fuente: Elaboración propia con datos de IAB Spain; Elogia; 2016 - 2021

Además, el Bizum se ha posicionado como uno de los métodos de pago más usados en la actualidad, de hecho, muchas empresas ya lo aceptan como una alternativa de pago.

Gráfico 2 Uso del Bizum por generación, en España (% del gasto total)



Fuente: CaixaBank, 2021

2.4.2. Pagos invisibles.

Esta nueva tendencia consiste en realizar pagos sin ningún tipo de contacto, sin emplear tarjetas, con el objetivo de simplificar aún más el proceso de compra.

Un ejemplo de esto es “Compra en un solo click” de Amazon el cual sirve para saltarte todos los pasos de pago, y direcciones, con solo un click el sistema ya te gestiona el pago y envio a tu tarjeta y dirección de envio predeterminada (registradas previamente).

Otro ejemplo sería el “click and collect”, donde tu realizas el pago a través de internet y después, cuando recibes el SMS de recogida vas a la tienda a por el paquete, una empresa que aplica esto es El Corte Inglés.

Ilustración 7 Click and collect, El Corte Ingles

Fuente: El Corte Ingles

Y el último ejemplo en esta línea sería el denominado “Buy Now, Pay Later” el cual es un método de pago en el que tiene la oportunidad de adquirir el producto, y pagarlo si deseas quedarte con él o devolverlo. Al igual que el primer ejemplo, Amazon Prime ofrece esta posibilidad en muchos de sus productos, sobretodo en productos de ropa. Otra plataforma que lo permite es Afterpay, la cual es una plataforma de múltiples empresas asociadas como Reebok, Pandora, Nike, y te permite realizar compras de productos y que posteriormente, pasadas varias semanas del momento de la compra, se realice el pago.

2.4.3. Pago fraccionados

Esta nueva tendencia de la compra funciona igual que la financiación tradicional, pagos por cuotas y según la plataforma con o sin intereses (generalmente sin intereses para ser más atractivo).

Empresas como Amazon permiten realizar pagos de entre 75€ y 1000€ fraccionado en varias cuotas, pagando la primera el día de la recepción del productos. La empresa asociada que se encarga de financiarlo es Cofidis, pero otras empresas como El Corte Ingles tienen sus propias opciones de financiación (Financiación ECI).

2.4.4. Otras tendencias

En conclusión, cada vez surgen más y más opciones para los consumidores, y las empresas, siempre buscando reducir el contacto, la espera y los pasos al mínimo posible. Otras tendencias además de las mencionadas son los pagos biométricos, a través de la huella o la cara, el comercio social, a través de tiendas incorporadas dentro de las propias redes sociales (Facebook, Instagram, y en el futuro WhatsApp) y muchas más tendencias que irán surgiendo y que nos dejan cada vez más claro que el panorama actual está en continuo cambio y crecimiento.

3. Blockchain

3.1. ¿Qué es el Blockchain?

El Blockchain es una tecnología datada en 1991 (S. Habber, W.S. Stornetta – How to time-stamp a digital document, 1991) aunque su idea original era mucho más sencilla de lo que es hoy, surgió con la idea de ser un sistema que registrase digitalmente cualquier tipo de archivo, ya sea un texto, una imagen, un video, y clasificarlo según su autor y su fecha de registro.

Cuando surgieron las criptomonedas lo hicieron a través de Blockchain gracias a las características que este sistema ofrece precisamente para lo que estaban buscando, pero el Blockchain tiene muchas más aplicaciones que las criptomonedas, también sirve para registrar de forma descentralizada cualquier otro tipo de información, sistemas de votos, IDs, registros de propiedad, contratos inteligentes, etc.

Todo esto se debe principalmente a que el Blockchain es un registro masificado de información del tipo Peer to Peer, donde los distintos usuarios o participantes en el sistema no dependen los unos de los otros ya que se ejecuta un protocolo consensuado el cual garantiza la seguridad de todas las trasferencias de datos realizadas a través de él.

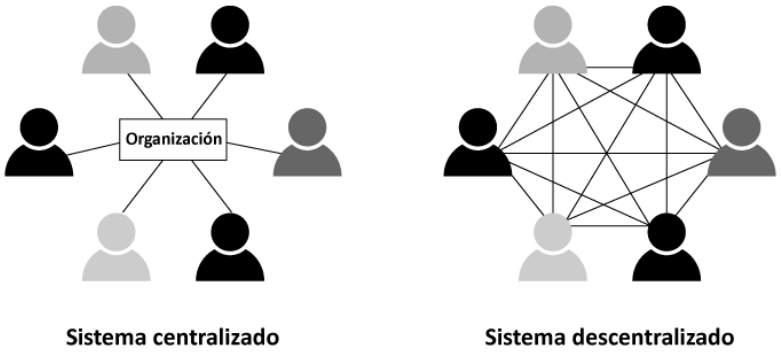
Todo el sistema funciona a través de una cadena de bloques de información ordenados de forma cronológica e identificados con un *hash* (número del bloque, identificativo) y además son validados por diferentes usuarios. Esto permite que un bloque ya validado no pueda ser modificado, se tendría que realizar una nueva operación que actualice la información ya que la original ya ha quedado registrada y es inmutable, garantizando la seguridad de cualquier transacción del registro, tampoco será posible eliminar información ya validada.

Cuando se habla de sistema descentralizado y Peer to Peer es porque existen diferentes tipos de sistemas de información, las bases de datos centralizadas almacenan todos sus datos en una base o servidor central accesible a través de distintos dispositivos dependientes del central, mientras que en las bases descentralizadas no se depende de un único servidor, la información se almacena en una red de varios servidores, todos interconectados.

El Blockchain consiste en un sistema descentralizado en el cual cada servidor tiene a su disposición toda la cadena de información, no una parte, la cadena completa, por lo que todos los servidores se encuentran al mismo nivel en cuanto a la validación de bloques,

es decir, al mismo nivel de jerarquía. Ningún servidor prevalece sobre el resto por lo que no puede realizar ninguna operación sin autorización consensuada.

Ilustración 8 Comparativa entre sistemas centralizados y descentralizados



Fuente: CO3, 2019

3.2. Características del Blockchain

En cuanto a las características del Blockchain, aunque ya mencionadas, son las siguientes:

3.2.1. Peer to Peer

Peer to Peer significa en español red entre pares y es la característica principal del Blockchain a pesar de ser más antigua, consiste en que un servidor manda su información a los servidores con los que está conectados, y estos a su vez a los conectados con ellos hasta que se envía a todos los miembros de la cadena. ¿Esto que permite? Que toda operación sea segura, sea enviada eficientemente, y el componente más importante, anónima.

El proceso, al ser compartido con toda la cadena no puede detenerse, editarse o eliminarse, la única forma de que se detenga es que no llegue a producirse dicha operación. Esto es muy sencillo de explicar tanto con datos como un ejemplo más sencillo, tú vas a comprar algo en efectivo, y no tienes dinero suficiente, por lo que no puedes realizar la compra y el proceso se anula, en el Blockchain funciona así también, si se da una orden que no puede ser completada, no se ejecuta.

3.2.2. Consenso, o nula dependencia

En un registro tradicional según el nivel jerárquico, alguien con un nivel superior puede introducir en la base de datos información a voluntad, incluso editar información ya existente, por lo que para evitar problemas debe generarse una confianza entre los usuarios del registro. En el Blockchain, al no haber jerarquía, y estar todos interconectados, además de validarse la información, no hace falta esa dependencia o confianza ya que ninguno de los usuarios puede alterar la información, y en caso de realizar una operación no confiable los demás servidores la rechazarían y no serían añadidos a la cadena de datos.

3.2.3. Proof of work

Una de las características más interesantes del Blockchain es el PoW, Proof of work, o en lenguaje coloquial, la recompensa por el trabajo realizado. Esto forma parte del sistema de consenso y consiste en dar una recompensa al nodo que otorga un *hash* (número de validación e identificación del bloque) al bloque anterior de la cadena. Cuanto mayor es la potencia computacional del ordenador más capacidad tiene de ser el que valide el bloque, y esto también tiene unos contras energéticos, ya que consumirá muchos más recursos (una de las principales polémicas del Blockchain).

El proceso de validación es lo que comúnmente se conoce como minar, que es el elemento más conocido de las criptomonedas las cuales lo heredan del Blockchain, y, de hecho, (en los Blockchain asociados a estas) suelen ser criptomonedas las recompensas por realizar el proceso de minado y encontrar el *hash* del bloque de información. Esto se realiza para motivar a los nodos a formar parte de la cadena y del proceso de validación y para garantizar el continuo flujo de información.

3.2.4. Seguridad

La seguridad radica en este proceso de validación a través de muchísimos servidores interconectados, si alguien desease modificar una cadena o un bloque, proceso el cual ya de por si es prácticamente imposible, deberia minar ese bloque y todos los de la cadena, en todos los servidores de esta. Además de que a mayor tamaño de la cadena más difícil resulta el proceso de validación haciendo que la dificultad para tratar de alterar la cadena y la energía necesaria para hacerlo sea tan excesiva que la probabilidad de que esto pasase es prácticamente nula en cadenas de muchos nodos y bloques.

Por si fuese poco las cadenas tienen la capacidad de recalcular la dificultad de *hashing* en función del número de servidores y del tiempo promedio que se tarde en realizar el proceso de validación para mejorar la seguridad de la cadena.

3.2.5. Transparencia

La transparencia es uno de los pilares de la crítica cuando se habla de criptomonedas y Blockchain y esto se debe a los distintos tipos de estas de los cuales hablaremos después. En las Blockchain de carácter público la transparencia es total, cualquier persona puede acceder en cualquier momento al historial de transacciones u operaciones, pero los usuarios que las realizan son de carácter anónimo, por el contrario, en las privadas o mixtas el acceso suele ser limitado y el grado de anonimato puede ser desde nulo, y poder identificarse a todos los usuarios hasta completamente anónimo y de transparencia nula. En el último caso es en el que suelen llevar a cabo las actuaciones no legitimas, pero suelen ser minoría.

3.2.6. Descentralización

Si se desea tener una base de datos no centralizada, en la que no solo un solo servidor contenga toda la información el Blockchain es la mejor opción ya que la cadena la van a mantener estable los nodos participantes en ella, dependiendo de su carácter público o privado, estos nodos tendrán acceso limitado a ciertos datos de la cadena y a diferentes roles (en las privadas suele haber administradores).

Como decía en la parte de seguridad, tener copias de seguridad de la cadena en varios servidores, sin depender de un servidor central permite tener la certeza de que, si alguna copia se llegase a corromper, las demás copias permitirían su restauración, si solo hubiese un servidor seria muchísimo más difícil reparar los daños.

Además, otra virtud de esta descentralización, la cual es objeto de crítica, es que, al no haber intermediarios, o más bien no ser necesarios, no se requiere intervención alguna a la hora de realizar cualquier operación permitiendo que se agilicen todos los procesos de transacciones entre usuarios de la cadena. Esto anterior solo pasa en las redes públicas ya que las privadas o mixtas si pueden establecer controles intermedios, motivo por el cual surgen cosas como los Smart Contracts de los que se hablará más adelante.

3.3. ¿Cómo funciona?

El proceso de transacción o intercambio de datos a través del Blockchain sigue un conjunto de pasos. Antes de realizar nada debes, lógicamente, formar parte del sistema por lo que debes convertirte en un nodo, para ello hay varias formas, la general suele ser a través de una aplicación asociada a la cadena en cuestión de la que se quiera formar parte, y la otra, consiste en realizar la conexión a través de una web asociada a la cadena, aunque en este caso generalmente el usuario estará limitado a las opciones que la web le permita siendo un usuario subordinado a la cadena que los bloques promedio generan.

Una vez te conviertes en nodo puedes transmitir o enviar datos a los servidores a los que estás conectado, los cuales serán los primeros en validar la información y verificar que sea segura y valida, no cometa actividades fraudulentas y una vez lo hayan verificado lo añadirán a su *pool*, o coloquialmente hablando, su lista de transacciones pendientes de enviar al resto de la cadena. Para evitar que estén enviando la misma información de forma perpetua tienen unos sistemas de detección que ignoran las operaciones que ya tienen en su pool, o ya han almacenado, permitiendo así un flujo eficiente de información.

El resto del proceso es sencillo, a medida que el *pool* se va llenando se van enviando los datos al resto de servidores en rondas de envíos a servidores de forma aleatoria, el protocolo de consenso ya mencionado, por lo que no siguen un orden establecido, lo que garantiza el anonimato y la nula dependencia.

Una vez se recibe la información esta se almacena en un nuevo bloque de la cadena de cada servidor, el cual será verificado e identificados con un *hash* (digito de control del bloque).

Cuando la información es validada y se le atribuye a su nuevo bloque un *hash* todos los servidores de la cadena actualizan su copia de esta para añadir el nuevo bloque de información que contiene las últimas operaciones validadas.

De esta forma y con este proceso se realiza el proceso de almacenaje y transferencia de información a través del Blockchain.

Ilustración 9 Funcionamiento del Blockchain

Fuente: MrHouston, 2021

3.4. Tipos de Blockchain

Hay tres tipos básicos de Blockchain de los cuales surgen otros modelos u opciones, los principales son: Blockchain públicas, privadas e hibridas.

3.4.1. Publicas

Las Blockchain públicas son todas aquellas a las que puede acceder cualquier persona, se suele acceder mediante su aplicación concreta y todos los nodos asociados a la cadena tienen el mismo nivel jerárquico por lo que tiene acceso a la información, así como la opción de minar si lo desea. Son redes que funcionan de forma consensuada y anónima por lo general, es decir, las transacciones y operaciones de datos realizadas en estas redes pueden rastrearse, pero no son identificables.

3.4.2. Privadas

Las Blockchain privadas son aquellas en las que el acceso a los datos no tiene un alcance público y solo los usuarios con autorización y claves pueden consultar las operaciones realizadas en ellas. Suelen ser distribuidas por uno o varios nodos con un mayor nivel jerárquico los cuales otorgan acceso a los nodos que deseen y limitan el acceso o incluso el número de nodos participantes en la red. Al ser redes privadas los dueños de estas pueden decidir el nivel de anonimato de estas pudiéndose identificar las operaciones

si así se desea o haciéndolas completamente anónimas. En este tipo se pierde la descentralización.

3.4.3. Híbridas

Este tipo de redes también suele llamarse Blockchain federadas ya que su ámbito de uso suele darse por gobiernos y empresas y son administradas por ellas. El acceso a estas redes suele tener un alcance público y privado ya que se puede acceder a ellos como usuario promedio a través de interfaces web puestas a disposición por los dueños de la red, pero el acceso a los datos está limitado por parte de los administradores de la cadena. Al no formar parte de los nodos de la cadena, sino ser meros observadores, los usuarios promedios se ven limitados en funciones, en estas redes la recompensa de minado no se produce ya que son las propias administraciones las que se encargan de mantener los servidores y los bloques de información validados.

En las redes públicas el minado de bloques es esencial para mantener ese carácter público, pero en este tipo, al ser de administración privada no tiene cabida en este sistema.

Dentro de este grupo hay un mercado creciente del que surgen otros modelos como es el *Blockchain as a service*, modelo por el cual se ofrece almacenamiento de datos de tu Blockchain en la nube. Este tipo de negocio lo están llevando a cabo grandes empresas como pueden ser Microsoft con R3, IBM colaborando con Hyperledger Fabric, Amazon junto con Digital Currency Group, entre otras empresas de renombre. Este servicio suele garantizar una seguridad mayor a cambio de un precio determinado, esto les permite no requerir tanto de hardware además de tener un canal Blockchain simplificado que no requiera de conocimientos de programación avanzados.

3.5. Aplicaciones del Blockchain

El Blockchain es una de las tecnologías con más potencial que han surgido en los tiempos modernos y es casi certero decir que acabará revolucionando, a largo plazo, los modelos de negocio actuales. Es una tecnología que permite y puede lograr aumentar la eficiencia en muchos sectores, financieros, mercados de valores, almacenamiento de datos, contratos, etc. A continuación, hablaremos de los sectores y las aplicaciones con mayor impacto y que mayor potencial a futuro tienen, dejaremos la parte de sistemas financieros para el final para permitirlo usar de puente con el punto siguiente del trabajo.

3.5.1. Almacenamiento en la nube

Como ya hemos mencionado anteriormente hay grandes empresas ofreciendo la posibilidad de almacenar Blockchain en sus sistemas, pero, también hay Blockchain que permiten a las empresas la posibilidad de tener un almacenamiento de datos y archivos en ellas para no depender de un servidor central.

Los datos se almacenan en el Blockchain encriptados y se distribuyen entre los nodos de la cadena integrando la información en nuevos bloques, permitiendo que se realicen tantas copias de seguridad como nodos haya en la cadena garantizando una seguridad mayor ante posibles pérdidas de datos, hackeos o incluso cualquier problema que en caso de haber un único servidor paralizasen el acceso a la información, por ejemplo, una caída de la corriente en la zona donde se encuentra el único servidor no afectaría a la entidad si sus datos estuviesen almacenados en la nube a través de una cadena.

Una empresa con gran peso en este sector, del que fue pionera es Storj, su modelo de negocio consiste en ofrecer el alquiler de espacio en sus cadenas de datos a empresas o usuarios, lo cual, según un informe realizado por la empresa en 2018 esto permite un abaratamiento de costes a las empresas de hasta el 80% en comparación al sistema tradicional de servidor privado y único.

Otras alternativas a Storj pueden ser Microsoft con su plataforma Azure o Backblace, empresa que se dedica a gestionar copias de seguridad de servidores con información de empresas de cualquier tamaño. Tambien otras de gran volumen de negocio que surgieron gracias al código abierto de Storj como pueden ser Cockroach Labs o Pindrop Security.

Ilustración 10 Microsoft Azure

Fuente: Microsoft

La desventaja que tiene este servicio es simple, estamos utilizando servidores ajenos para guardar nuestra información por lo que depositamos nuestra confianza en ellos, dándoles información de mucho valor, delicada.

3.5.2. Registros de datos

En una Blockchain pueden almacenarse cualquier tipo de datos, ya sean registros médicos, registros de propiedad física o intelectual (patentes, diseños, etc.) y cualquier tipo de dato imaginable desde cualquier sector tradicional. Puede haber un registro de

propiedad almacenado en una Blockchain y poder consultar quien es el propietario, cuáles han sido las transacciones que se han realizado por dicho inmueble, o tener una patente registrada y poder consultar la autoría, la fecha de creación o registro, etc., las posibilidades son infinitas.

Hay empresas ofreciendo sus servicios en cada uno de estos sectores, en el caso de la protección y almacenamiento de propiedad intelectual empresas como Proof of existence ofrecen sus servicios, también Tierion, posiblemente la más grande en este ámbito de aplicación del Blockchain la cual bajo el eslogan “Simplifique su confianza” ofrece a las empresas la posibilidad de almacenar sus datos a un coste económico.

Haciendo uso del Blockchain un artista podría crear una obra y probar ser el creador sin necesidad de registrarlo, simplemente vinculando esa obra al hash de una transacción vinculada a esa obra, de esta forma surgen entre otras cosas las mediáticas NFTs (Tokens no fungibles vinculados a una obra).

3.5.3. Sistema de votaciones electrónicas

Una forma de votar cada vez que hay elecciones es a través de internet, sin embargo, este sistema tiene varias contras, la primera es el alto coste que este sistema supone tanto digitalmente como físicamente (papeletas, montar colegios, conteos, personal, etc.), y la segunda contra es la vulnerabilidad a sufrir ataques informáticos en el voto digital, y que los conteos se vean alterados.

El Blockchain puede ser una vía que permita realizar este sistema de voto con un coste reducido, de acceso público, con un anonimato garantizado e infalsificable. Al convertir los votos en transacciones se puede crear una cadena de bloques que contenga un registro de todos ellos, además al ser vía Blockchain la alteración de la cadena no sería posible y ningún voto deberia removerse por ser ilegitimo o erróneo. Además, serian públicos y cualquiera podría tener acceso al conteo final, evitando así cualquier duda o polémica asociada a la votación.

En Julio de 2018 se realizaron en Suiza, concretamente en la ciudad de Zug, votaciones online vía Blockchain y fue todo un éxito. (Bit2Me Academy, 2019)

3.5.4. Smart Contracts

Uno de los elementos más importantes de los Blockchain, del cual me han hablado en asignaturas como Contratos mercantiles, ha sido los Smart Contracts, o contratos inteligentes.

Este novedoso tipo de acuerdos consiste en contratos en los que se estipulan un conjunto de cláusulas, como pueden ser los controles que debe seguir la mercancía, el tipo de pago, etc., como cualquier otro contrato de transacciones, pero empleando la tecnología Blockchain. Estos contratos se codifican y almacenan en cadenas Blockchain donde son supervisados por los nodos de la cadena, por lo que una vez formalizados si se quisiera realizar alguna modificación deberia hacerse un nuevo contrato que sustituya al anterior dado que son inmodificables de otro modo.

Este tipo de contratos tiene una seria de ventajas, algunas de ellas son:

- La autonomía de estos, ya que no hay intermediarios, es el propio usuario el que accede al acuerdo.
- La fiabilidad, al estar almacenados en la cadena no pueden ser modificados ni extraviados.
- La rapidez de gestión ya que no son necesarios papeleos, manuales, etc.

Este nuevo tipo de contratos aún no está implementado de forma habitual en el sistema comercial actual, aún es un formato que debe madurar y el mundo comercial con él para que esté listo para ser implementado de forma habitual. La gente aún desconfía de la tecnología Blockchain y de las mejoras que esta podría ofrecer, pero lo cierto es que de usarse mal podrían tornarse en contratos de sometimiento más que de contratos que busquen una mejora en las condiciones contractuales en forma y fin. Para ello, para que actualmente los Smart Contracts sean aceptados es recomendable la supervisión previa por expertos reguladores, en materia de prevención de datos, de requisitos mínimos de contratación, de sujeción a normas, etc., y con el tiempo, a medida que la gente y el formato maduren podrán llegar a establecerse como un formato de uso habitual que de muchas ventajas respecto los tradicionales.

Ilustración 11 Funcionamiento de un Smart Contract

Fuente: Blockgeeks

3.5.5. Sistemas financieros y monedas digitales

La razón por la que surgió el Blockchain fue para descentralizar la confianza puesta en el sistema financiero actual. Actualmente el sistema financiero se sostiene bajo numerosos proveedores de capital, lo que conlleva un gran problema de operatividad, el sistema más conocido es el sistema SWIFT, Society for Worldwide Interbank Financial Telecommunication (muy oído actualmente tras el bloqueo de capital a Rusia a través de este sistema). A través del sistema Swift los bancos se transfieren dinero, el problema es que esa transmisión conlleva un plazo de demora de varios días, el Blockchain surgió con la idea en mente de evitar eso, permitiendo realizar transferencias de capital en tiempo real independientemente del volumen, de forma segura, además según el tipo de cadena, de una forma más o menos anónima.

Todas estas ideas del Blockchain y las criptomonedas se vieron claramente influenciadas a raíz de la crisis financiera de 2008 cuando el sector bancario quedó en evidencia para gran parte de la sociedad, y donde mucha gente perdió la confianza en el actual sistema financiero. De hecho, los propios bancos se subieron al barco del cambio invirtiendo capital en investigar la tecnología Blockchain. Actualmente prácticamente todos los bancos del mundo están invirtiendo en esta nueva tecnología, ya que saben que a largo plazo será un pilar del sistema financiero. (Forbes, 2021)

Además, a raíz de la crisis financiera de 2008, de estas inversiones, de la desconfianza y del surgimiento del Blockchain surgieron apoyados en esta, los medios de pago de los que hablaremos después, las criptomonedas.

3.5.6. Cadenas de suministros

Actualmente muchas empresas poseen una red de proveedores comúnmente llamada cadena de proveedores, la cual puede ser complicada de gestionar, para ello múltiples empresas del ámbito Blockchain ofrecen sus servicios para realizar el seguimiento de suministros, así como su procedencia a través de esta tecnología.

Una de las principales precursoras de este sistema, la empresa Skuchian está desarrollando desde 2019 un sistema de gestión de la cadena de suministros junto a la multinacional canadiense CGI Inc. y el Banco Nacional de Canadá (el sexto más grande del país), dicho sistema se sustenta en Smart Contracts y el Blockchain asociado a ellos. (Criptomonedas e ICOs, 2018)

3.5.7. Industria 4.0 e Internet de las cosas

Una de las grandes metas del comercio y la industria actual es lograr alcanzar el estadio que promete la cuarta revolución industrial, la llamada Industria 4.0 la cual promete una evolución que combine cambios en los procesos de producción, de gestión, de contabilidad y una postventa mucho más eficiente que afecte positivamente a la percepción de los clientes. Crear factorías inteligentes que combinaran a tiempo real datos con fabricación de una forma automatizada, donde todos los intermediarios tengan información a tiempo real, los procesos sean auto configurables, etc.

Esa soñada industria 4.0 puede lograrse de una forma mucho más sencilla a través del Blockchain, que ofrezca un registro de cualquier tipo de actividad, dato o transacción, de forma descentralizada, con gran seguridad de forma que sea prácticamente imposible modificar los procesos sin autorización previa de los usuarios de mayor rango jerárquico. Una de las grandes ventajas del Blockchain para lograr esta industria es el poder ofrecer una comunicación directa, segura y descentralizada entre todos los sistemas de la organización, facilitando el M2M (sistema de transmisión de información entre maquinas).

Los Smart Contracts ya mencionados son otra de las ventajas que ofrece el Blockchain para lograr implantar una industria 4.0 en las organizaciones.

Otro factor es la fusión del Blockchain con el llamado internet de las cosas, IoT, el cual permite que distintos dispositivos conectados a internet se transmitan datos de una forma eficaz. A través de redes Blockchain privadas podrían transmitirse de forma que no

puedan ser vulnerados o alterados por terceros, pudiendo así sistematizar procesos de cualquier ámbito, y aumentar su seguridad y eficiencia.

Un estudio de Fortune Bussiness Insights centrado en el Internet de las cosas y el mercado a través de internet, calcula que sobre 2028 las cifras alcanzadas gracias a este sistema superarán o rondarán los 2 billones de dólares en volumen de operaciones. (Fortune Bussiness Insights, 2021)

4. Criptomonedas

Una vez desarrollado de una forma breve lo que es el Blockchain, lo que ofrece, sus ventajas y mencionadas algunas de sus criticas sociales más comunes toca tratar el tema principal de este trabajo, los nuevos medios de pago que están surgiendo, las criptomonedas. En este punto plenamente dedicado a ellas, empezaremos hablando de como surgieron, del porqué de estas nuevas monedas, de sus tipos, las más importantes, sus usos, su valoración por la sociedad y, finalmente de sus aspectos contables, los cuales suelen acarrear dudas o criticas fuertes a estos nuevos medios de pago.

4.1. Orígenes

Como punto de origen para hablar de criptomonedas debemos fijar nuestra fecha en 2008, la crisis financiera surgida en EEUU por la quiebra del cuarto banco más importante del país, Lehman Brothers supuso el inicio de una larga década de crisis mundial. Entre las grandes consecuencias de esta crisis que supuso un desastre mundial para muchísimos países, con bancos solicitando rescates comunitarios en la UE sin ir más lejos, se encontraba la gran devaluación del dólar (sin ir más lejos en datos gráficos, en el año 2000 la relación €/$ suponía 1€/0,8$, en abril de 2008, llego al máximo de 1€/1,6$, actualmente ronda la relación 1€/0,9$) la cual tuvo que frenarse a través de la flexibilización cuantitativa por parte de todo el primer mundo, es decir, a través de la inyección de dinero en las reservas nacionales para lograr estabilizar su valor.

Gráfico 3 Evolución tasa de cambio €/$. 1999-2012

Fuente: ELBLOGSALMON

Durante la crisis la confianza de la gente en el sistema bancario actual se vio quebrada, las monedas se devaluaron, los bancos debieron rescatarse, se empleó dinero de los contribuyentes para subsanar y evitar quiebras, mucha gente perdió su dinero, y todo esto junto torno la opinión pública en contra del sistema actual, al cual deben aferrarse debido a que no había otras opciones viables donde depositar su confianza.

Y, en ese momento, como cualquier otra iniciativa de negocio, surgió una figura de carácter anónimo llamado Satoshi Nakamoto, creador, y desarrollador de la criptomoneda más famosa y conocida popularmente, el Bitcoin. La identidad de Nakamoto es desconocida, nadie sabe si es una o varias personas, si es una organización o no, lo cual, ya hablaremos más adelante, pero suscita a dudas y críticas a nivel social. En 2008, pasados dos meses del inicio de la crisis, publicó el artículo “Bitcoin: A Peer-to-Peer Electronic Cash System” en el que hablaba de su invento, el bitcoin, de su forma de ver el sistema actual y las mejoras que su invento podría producir, en el artículo.

En ese artículo también explicaba como funcionaria su nuevo sistema, a través del peer to peer, es decir, traspaso de información entre iguales, con un sistema open source, disponible para todo el mundo, descentralizado y sin intermediarios. El objetivo también es buscar la nula regulación por parte de agentes financieros como bancos y gobiernos, o al menos que ellos no lo controlen. Este sistema busca complementar y tratar de sustituir a largo plazo al sistema fiduciario por lo que más adelante hablaremos de la viabilidad a futuro de este objetivo.

Lo cierto es que los inicios no fueron fáciles, de hecho, anteriormente muchos otros habían intentado ofrecer un sistema similar, pero fracasaron por no tener a su disposición una tecnología como el Blockchain que haga posible de verdad lo que Satoshi se propuso. Y al igual que no fue el primero tampoco fue el último ya que, desde que las criptomonedas empezaron a hacerse eco más allá de foros, y el interés por la gente crecía, empezaron a surgir muchas más criptomonedas, actualmente hay más de 18.000 criptomonedas a fecha de 2022, aunque no todas tienen un peso o importancia como para ser relevantes a nivel global, muchas pueden estar asociadas a foros, grupos, membresías de apoyo a algún influencer, recompensas por estas, etc. (Investopedia, 2022)

Como hemos dicho antes, el bitcoin no fue el primer intento de establecer este sistema, antes lo intentaron otros, entre los que principalmente destacan David Chaum y Wei Dai, quienes, a parte de Satoshi, podrían ser considerados los padres de las criptomonedas. En 1983 David Chaum, criptógrafo estadounidense, desarrolló el sistema eCash, un sistema criptográfico confeccionado con la idea de ser un dinero electrónico de carácter anónimo. Este sistema funcionaba de forma que los bancos asociados a él

almacenasen en el sistema el dinero y el usuario de este pueda realizar transacciones con él, este sistema funcionó en un banco estadounidense, Mark Twain Bank de St. Louis, desde 1995 hasta 1998 bajo el nombre de DigiCash, una versión actualizada que mantenía confidenciales los datos de los efectores de las transacciones. Esta fue la "primera criptomoneda" y la precursora del movimiento *ciberpunk* (movimiento activista de la privacidad criptográfica).

En 1998, el ingeniero y criptógrafo Wei Dai publicó un ensayo que iba más allá de la propuesta de Chaum y acercaba el concepto de las criptomonedas más a lo que es hoy. En el ensayo Dei definió el sistema con unas características que deben estar presentes como por ejemplo el hecho de afirmar que debía realizarse un registro contable colectivo de todas las transacciones realizadas, para mejorar su seguridad, y que ese esfuerzo colectivo debía recompensarse para incitar a colaborar. Además, afirmaba que debían implementarse claves públicas para autentificar las transacciones. Wei no llegó a lanzar un sistema con las características que el describía en su ensayo *"b-money"* pero fue de gran inspiración para los siguientes sistemas, tanto que como homenaje la unidad fragmentada más pequeña de Ethereum, la secunda criptomoneda con más peso, por detrás del Bitcoin, se denomina "wei".

4.2. Criptografía

4.2.1. Tipos de criptografía

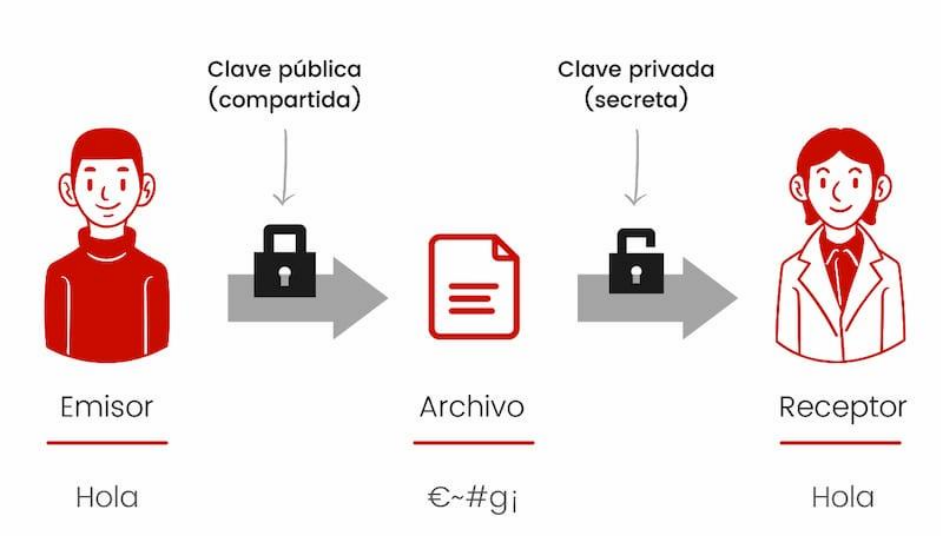
Para poder comprender como funcionan las criptomonedas es necesario conocer los distintos tipos de criptografía que existen actualmente, los principales son dos: simétrica y asimétrica.

La criptografía simétrica es la que solo emplea un tipo de clave para enviar mensajes cifrados y poder descifrarlos, en este caso la clave la deben conocer tanto el emisor como el receptor para poder llegar a comprender el mensaje cifrado. Este tipo tiene un problema muy importante, y es que quien tenga la clave puede acceder al mensaje, de forma que si la clave se filtra cualquier persona podría descifrarlo.

Un ejemplo de criptografía simétrica sería Enigma, los alemanes tenían un sistema en clave, y para poder entenderse ambos, emisor y receptor, sabían las claves. Una vez que los británicos obtuvieron las claves pudieron acceder al mensaje, provocando la perdida de información y en su caso la derrota de los alemanes. Aplicado al caso de que una criptomoneda funcionase con este tipo de criptografía haría que cualquier persona con la clave pudiese acceder a nuestro monedero y robarnos.

Para evitar el problema de seguridad surge la simetría asimétrica la cual cambia completamente su funcionamiento, en este caso hay dos claves, una pública y otra privada de forma que a la hora de enviar un mensaje la persona lo cifra con su clave publica, y el receptor emplea su clave privada para descifrarlo, siendo solo conocida por las dos partes la clave pública.

Ilustración 12 Emisión y recepción de un mensaje con criptografía asimétrica



Fuente: Atico34

Para comprender esto es conveniente entender cómo funciona la generación de claves, es posible descifrar con una clave privada un mensaje emitido con una clave pública debido a que la pública es generada matemáticamente a partir de la privada, la cual es personal, y en caso de perderse o que sea conocida por alguien más volveríamos a estar en un problema de filtrado de información. A partir de una clave privada se pueden generar tantas claves públicas como se deseen y es la que nos permite plasmar la autenticidad de una transmisión de datos o transmisión de capital. A partir de la clave privada se pueden generar públicas, pero no al revés.

Este tipo de criptología tiene una seguridad mucho más alta que la simétrica al necesitar una clave de mayor rango para poder acceder a la información, la cual, solo con la clave común no puede conocerse.

4.3. Características de las criptomonedas

Antes hablar de los tipos de criptomonedas más importantes, y sus características propias hay que conocer las características comunes que las permiten tener la utilidad y el

valor que verdaderamente tienen. Tambien comentar las ventajas y desventajas frente a sistemas tradicionales.

4.3.1. Características generales

Criptografía

Como hemos mencionado previamente los usuarios de criptomonedas emplean técnicas de cifrado para realizar las transferencias de capital de unos a otros, haciendo uso de sus claves públicas y privadas.

Descentralización

No necesitan el control de ninguna organización o institución para funcionar lo cual les otorga una operatividad muy superior a los sistemas tradicionales los cuales, funcionan a través de autorización de una institución justo antes de realizar una transacción, lo cual, en caso de requerir alguna autorización inmediata deberíamos esperar a que esta institución esté operativa para llevar a cabo los tramites.

Transparencia

Todas las transacciones realizadas quedan registradas automáticamente en la cadena de bloques, que funciona como un libro contable el cual es compartido y guardado en copias de seguridad por todos los usuarios de la red, siendo prácticamente imposible de manipular.

Seudoanonimato

Una de las mayores críticas, sino la mayor, a las criptomonedas es que la gente ha difundido y/o se han visto atraídos por un concepto de moneda virtual, descentralizada, segura, privada y anónima, lo cual lleva a mal pensar y creer que las criptomonedas se van a emplear para llevar a cabo actividades ilícitas. Y sí, es cierto que parte del tráfico de criptomonedas tiene uno de los problemas que Satoshi buscaba evitar cuando creo el bitcoin, el tráfico de dinero negro, pero lo hace con una diferencia respecto al sistema original y es el hecho de que las transacciones llevadas a cabo con criptomonedas NO son anónimas, son suedoanonimas.

Cuando se realiza una transacción con criptomonedas no puedes identificar quien la ha realizado, pero si puedes rastrear la transacción, y ver el origen y el destino de las criptomonedas de esta operación, y, solo en caso de hacerse públicas también podrás rastrear las cuentas que participan en ella. No, no se puede saber, por norma general, quien ha efectuado la operación, pero se puede rastrear, al igual que no se puede saber

de quién es el correo electrónico de una persona hasta que esa misma persona te diga que le pertenece a él, pero puede rastrearse la IP.

Inmediatez

Acompañando a la descentralización mencionada anteriormente se encuentra la inmediatez que esta permite, al no depender de ningún intermediario para realizar el pago.

Whitepaper

Esto más que una característica es un manual que tienen todas las criptomonedas, es el plan estratégico de desarrollo del equipo que lleva a cabo la gestión y la creación de la criptomoneda y su utilidad caduca en el momento que se lanza una oferta inicial, ya que es el documento que trata de atraer a los usuarios a la criptomoneda en cuestión.

4.3.2. Ventajas frente a sistemas tradicionales

Las principales ventajas frente a los medios de pago tradicionales son las siguientes:

- **Menores costes de transacción**, dada la nula participación de intermediarios.
- **Seguridad**, cada dueño tiene su propio monedero (explicado en el punto siguiente), y cada monedero dos claves, la pública y la privada. La seguridad anti-hackeos está prácticamente garantizada, la seguridad antirrobo también, siempre que no se comparta la clave privada, en ese caso cualquier persona que la tenga podrá acceder al monedero vinculado a ella.
- **Inmediatez y operatividad** superior.

4.3.3. Desventajas frente a sistemas tradicionales

Poe otro lado, las desventajas generales son:

- Altísima, aunque previsible, **volatilidad de sus precios.** Actualmente las criptomonedas son más un activo financiero que un medio de pago en sí, aunque es su principal función y se pueden realizar pagos con ellas, y como activo su valor en el mercado de valores es altamente volátil y la mayoría de criptomonedas han sufrido grandes crecimientos y decrecimientos de valor muy grandes, sin ir más lejos el bitcoin ha llegado a sufrir, hasta que se ha estabilizado, crecimientos del 800% de su valor para posteriormente sufrir caídas del 80% del máximo alcanzado en la subida.

- Falta de aceptación social y por parte de empresas y algunos mercados. Están en proceso de maduración tanto las criptomonedas como el conocimiento general hacia ellas.
- Nula regulación, al no estar regulados, y no haber intermediarios, si, se gana operatividad, pero como hemos mencionado antes también permite que bajo el paraguas del seudoanonimato se realicen actividades ilegales con ellas. Esta desventaja hace que la gente desconfié de ellas y las vea como un peligro más que como una opción a tener en cuenta para gestionar sus pagos y su capital.

4.4. Monederos

Un monedero, o Wallet, de criptomoneda es y tiene la misma función que un monedero tradicional, es el lugar donde almacenas tu dinero, en este caso tus criptomonedas. Además, como en los wallets virtuales convencionales en los que registras tus tarjetas (Google Pay, Apple Pay, etc.), sirven como medio para realizar transacciones, recibir y enviar capital.

Un monedero es un archivo encriptado que posee unas claves y unas direcciones a través de la cuales se realizan transacciones, siendo la protección de la clave privada responsabilidad del usuario ya que en caso de pérdida cualquiera podría acceder al monedero y operar con él, y al no haber regulación, perder definitivamente esos fondos.

Las direcciones son cadenas de caracteres identificativos del usuario en la red de la moneda con la que se esté operando, cumplen en la práctica la misma función que los números identificativos de las cuentas bancarias tradicionales, si alguien los tiene puede enviarte dinero. A diferencia de una cuenta bancaria en un monedero puedes crear tantas direcciones como el usuario crea conveniente, incluso uno distinto por cada transacción.

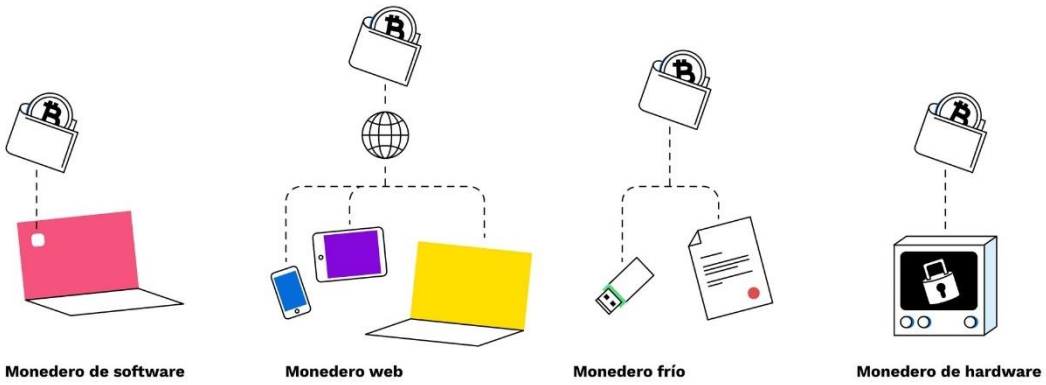
El funcionamiento de los wallets es relativamente sencillo, tienen claves públicas que se usan para que otros envíen dinero al monedero, y está compuesta por un conjunto de dígitos, números y letras. Y por otro lado la clave privada la cual permite al propietario movilizar sus fondos a voluntad.

La seguridad de los monederos depende del tipo de monedero que se utilice para almacenar los fondos, hay dos grandes categorías:

- Cold Wallets, o monederos fríos, los cuales son monederos físicos, a través del propio hardware, los cuales funcionan sin conexión a internet, por lo que su seguridad es completa.

- Hot Wallets, o monederos calientes, los cuales funcionan con conexión online permanente, a través de aplicaciones instalables o extensiones del propio navegador que use el usuario.

Ilustración 13 Tipos de monederos de criptomonedas



Fuente: Bitpanda Academy

Dentro de los Cold Wallets cabe la posibilidad de distinguir dos tipos de wallets físicos:

- Los wallets de hardware propiamente dichos, las cuales cuentan con un código PIN que añade más seguridad al monedero, además de poseer una clave llamada "seed" la cual sirve para recuperar tus activos en caso de pérdida o problemas del dispositivo por lo que es el sistema más seguro de todos. Algunos ejemplos de este tipo de monederos son Trezor y Ledger.

Ilustración 14 Monedero Ledger

Fuente: Ledger

- Y los Paper Wallets los cuales funcionan como un papel moneda tradicional además de como almacén de activos, consiste en un documento físico con las claves públicas y privadas reflejadas en él, además de las direcciones asociadas. Son como una caja fuerte ya que generalmente se usan cuando no se piensa usar los activos en un determinado plazo, cuentan con QR escaneable que se verifica vía Blockchain y permite cargar los fondos en un software.

Y, por otra parte, dentro de la categoría de monederos fríos también podemos diferenciar dos tipos:

- Exchange Wallets, los cuales no son un tipo de monedero en si ya que tus criptoactivos se almacenan en el Exchange (lugar donde se intercambian criptomonedas a cambio de dinero Fiat, como por ejemplo el dólar) en el que los has adquirido, el más conocido es Bit2Me. El problema de este "monedero" es que es la propia plataforma la que almacena tus monedas y en caso de ser hackeada, ya que la plataforma en si no forma parte de una red Blockchain, los activos podrían ser vulnerables.
- Monederos en línea, este tipo de monederos funcionan conectados a internet a través de un software digital que te almacena tus monedas y te permite operar con ellas. Dentro de este tipo hay algunos que bloquean el rastreo de la IP para darte más seguridad (y como siempre, a más privacidad, más posibilidad de conductas ilícitas). Son independientes del Exchange a través del cual adquieres tus criptomonedas y en muchos casos no necesitan que tengas una cuenta en sus plataformas para funcionar. El más famoso es Coinbase Wallet de la plataforma Coinbase.

4.5. Bitcoin

Ya explicado el origen de las criptomonedas, sus características generales, y los monederos y cómo funcionan toca hablar de posiblemente uno de los ítem más buscados en Google de los últimos años: el Bitcoin.

Ilustración 15 Búsqueda de "Bitcoin" en Google, desde su origen

Fuente: Google Trends

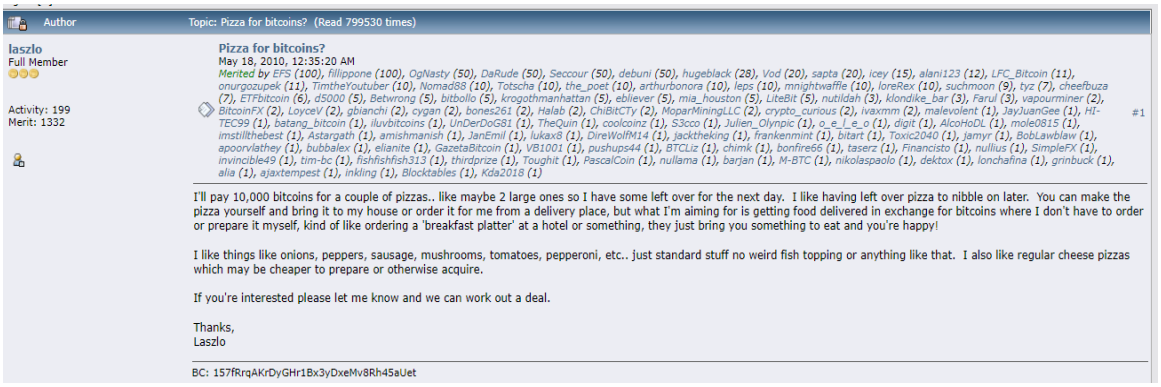
En enero de 2009 la versión 0.1 del Bitcoin fue publicada, y el primer bloque de la cadena fue minado por su fundador, “Satoshi Nakamoto”, a este bloque se le conoce como el Bloque Genesis el cual contenía un total de 50 Bitcoins, los primeros, y los que marcarían y marcarán la cantidad de bitcoins que contendrán los bloques desde ese día hasta que el ultimo bloque sea minado. Esto es posible gracias a dos factores que mencionaremos más adelante, el *halving* y el carácter finito del bitcoin.

Ilustración 16 Logo del Bitcoin

Desde el mineo del primer bloque el bitcoin continúo siendo minado por parte de distintos usuarios, la mayoría usuarios de foros con la esperanza de que algún día esa minería se convertirse en activos de gran valor, lo cual continuo hasta 2010.

El 22 de mayo de 2010 ocurrió algo que marcaría el origen del bitcoin como medio de pago con un determinado valor, de la misma forma que se narra la anécdota de Newton y la manzana el día 22 de mayo se narra la historia de Laszlo, la pizza y el bitcoin. El programador Laszlo Hanyecz publicó en un foro el siguiente mensaje: “Pagaré 10000 BTC por dos pizzas”.

Ilustración 17 Mensaje original de Laszlo Hanyecz



Author | Topic: Pizza for bitcoins? (Read 799530 times)

laszlo
Full Member
Activity: 199
Merit: 1332

Pizza for bitcoins?
May 18, 2010, 12:35:20 AM
Merited by EFS (100), filippone (100), OgNasty (50), DaRude (50), Seccour (50), debuni (50), hugeblack (28), Vod (20), sapta (20), icey (15), alani123 (12), LFC_Bitcoin (11), onurgozupek (11), TimtheYoutuber (10), Nomad88 (10), Totscha (10), the_poet (10), arthurbonora (10), leps (10), mnightwaffle (10), loreRex (10), suchmoon (9), tyz (7), cheefbuza (7), ETFbitcoin (6), d5000 (5), Betwrong (5), bitbollo (5), krogothmanhattan (5), ebliever (5), mia_houston (5), LiteBit (5), nutildah (3), klondike_bar (3), Farul (3), vapourminer (2), BitcoinFX (2), LoyceV (2), gbianchi (2), cygan (2), bones261 (2), Halab (2), ChiBitCTy (2), MoparMiningLLC (2), crypto_curious (2), ivaxmm (2), malevolent (1), JayJuanGee (1), HI-TEC99 (1), batang_bitcoin (1), iluvbitcoins (1), UnDerDoG81 (1), TheQuin (1), coolcoinz (1), SScco (1), Julien_Olynpic (1), o_e_l_e_o (1), digit (1), AlcoHoDL (1), mole0815 (1), imstillthebest (1), Astargath (1), amishmanish (1), JanEmil (1), lukax8 (1), DireWolfM14 (1), jacktheking (1), frankenmint (1), bitart (1), Toxic2040 (1), jamyr (1), BobLawblaw (1), apoorvlathey (1), bubbalex (1), elianite (1), GazetaBitcoin (1), VB1001 (1), pushups44 (1), BTCLiz (1), chimk (1), bonfire66 (1), taserz (1), Financisto (1), nullius (1), SimpleFX (1), invincible49 (1), tim-bc (1), fishfishfish313 (1), thirdprize (1), Toughit (1), PascalCoin (1), nullama (1), barjan (1), M-BTC (1), nikolaspaolo (1), dektox (1), lonchafina (1), grinbuck (1), alia (1), ajaxtempest (1), inkling (1), Blocktables (1), Kda2018 (1)

I'll pay 10,000 bitcoins for a couple of pizzas.. like maybe 2 large ones so I have some left over for the next day. I like having left over pizza to nibble on later. You can make the pizza yourself and bring it to my house or order it for me from a delivery place, but what I'm aiming for is getting food delivered in exchange for bitcoins where I don't have to order or prepare it myself, kind of like ordering a 'breakfast platter' at a hotel or something, they just bring you something to eat and you're happy!

I like things like onions, peppers, sausage, mushrooms, tomatoes, pepperoni, etc.. just standard stuff no weird fish topping or anything like that. I also like regular cheese pizzas which may be cheaper to prepare or otherwise acquire.

If you're interested please let me know and we can work out a deal.

Thanks,
Laszlo

BC: 157fRrqAKrDyGHr1Bx3yDxeMv8Rh45aUet

Fuente: Foro Bitcointalk

Las pizzas, por un valor de 24$ le fueron entregadas y el hizo su parte del trato entregando los 10000 BTC a la persona que se las envió esa fue la primera vez que se realizaba una venta con bitcoins y ese día recibieron su primera asignación de valor, 10000

BTC equivaliendo a 24$, es decir, 1BTC/0,0024$ (a día 4 de junio de 2022 esos 10000 BTC rondan los 278 millones de $, y cada unidad aproximadamente 29 mil dólares).

Desde entonces el bitcoin ganó fama en los mercados online, y también en el mercado negro moviendo el más grande de ellos casi 10 millones de BTC hasta que se desarticuló, esto hizo que muchos países decidieran poner barreras al bitcoin, de hecho, el Banco Popular Chino prohibió el uso de esta moneda a las instituciones financiera en 2013, en su totalidad en 2017 y en 2021 empezó a perseguir a los mineros.

Como mencionamos antes, los bitcoin tienen un carácter finito, cada 10 minutos se genera un bloque de la cadena con una cantidad de bitcoins determinada por la edad de estos. Esto se debe a que cada 4 años se produce un fenómeno denominado *halving,* siendo el primero que ocurrió en 2012 cuando los bloques pasaron de 50 bitcoins a 25, eso es el *halving*, el fenómeno en el que la cantidad de bitcoins por bloque se reducen con el objetivo de que llegue un día en el que todos los bitcoins programados se hayan minado, esa fecha está fijada en 2140, pero se espera que ya en 2036 se haya minado aproximadamente el 99% de las bitcoins según su programación de *halving* y el ritmo de generación de bloques. Además, al igual que las monedas convencionales un BTC puede subdividirse en unidades más pequeñas.

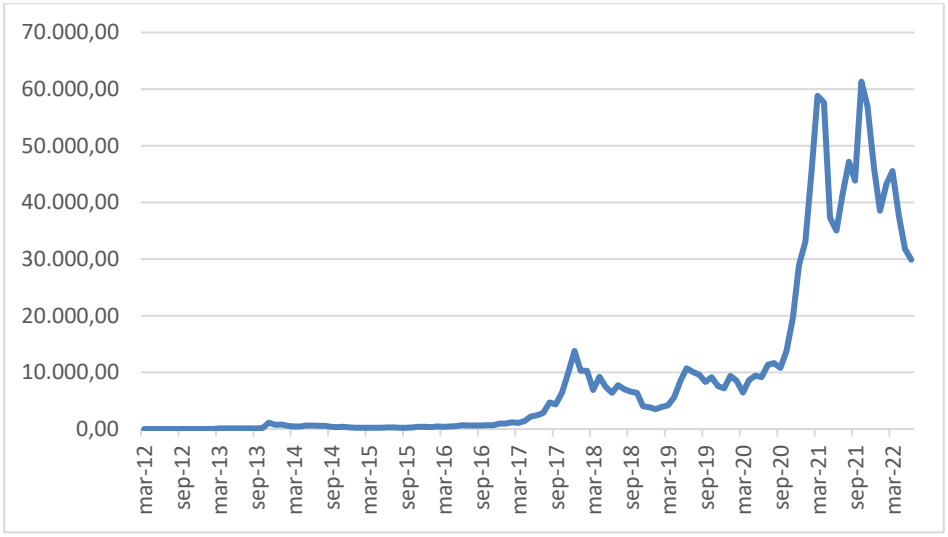
Este hecho hace que la recompensa por minar sea menor, y que los que hayan apoyado desde el inicio hayan tenido unos beneficios mucho mayores, independientemente de esto la vida del bitcoin ha estado llena de fluctuaciones, pero dentro de estas se puede realizar un ciclo de cuatro fases que se repite de forma continuada desde su aparición:

- Fase 1. Acumulación: esta fase se da cuando el valor del BTC ha caído (en el caso de la primera vez, cuando surgió) y la tristeza y la ansiedad se apodera de los usuarios, por lo que acaban vendiendo a perdidas, mientras que los que lo ven como una oportunidad compran grandes cantidades al ver el precio por los suelos.
- Fase 2. Tendencia Alcista: en esta fase los precios superan el máximo anterior y continúa subiendo, significando un gran alivio para los usuarios. Todas las fases alcistas del BTC han acabado con subidas del 500-600% sobre su valor máximo anterior.
- Fase 3. Crecimiento Parabólico: son los momentos en los que se produce una entrada descontrolada de usuarios y el precio empieza a dispararse debido a la avaricia y la especulación, la demanda supera a la oferta y el descontrol, es el momento de vender ya que se aproxima la fase 4.

- Fase 4. Caída: Se trata de la fase de mayor desesperación, la burbuja explota y empiezan a haber caídas del 50% del valor máximo alcanzado, del 70% incluso y los más inexpertos venden huyendo del desastre, con pérdidas muy altas.

Una vez acaba esta fase 4 el ciclo pasados unos días vuelve a ocurrir, volviendo a la fase 1, ha habido varias épocas muy marcadas en las que este ciclo ha supuesto un cambio muy significativo del valor del BTC. A continuación, recogemos en un gráfico de elaboración propia la relación histórica del dólar y el Bitcoin:

Gráfico 4 Evolución histórica de la tasa de cambio del BTC respecto al $.



Fuente: Elaboración propia
(datos recogidos de: https://es.investing.com/crypto/bitcoin/btc-usd-historical-data)

Actualmente, concretamente desde diciembre de 2021 estamos en una etapa de caída, donde el BTC ha pasado de los 56000$/BTC de noviembre a los 29000$/BTC de mayo de 2022.

Para muchos el bitcoin es más un activo financiero que una moneda (Cheah&Fry, 2015) y que su valor y estabilidad es nula, lo cual, actualmente es cierto, se pueden realizar compras con ellas como un método de pago, pero necesita aún mucha más madurez para llegar a establecerse socialmente, aún así ya hay países que realizan o aceptan compras usando Bitcoins, mismamente Rusia estaría dispuesta a aceptarla a cambio de Gas y Petróleo según dijo el Presidente del Comité de energía del estado, Pavel Zavalny en marzo de 2022. Lo que si es cierto es que cada vez más empresas importantes empiezan a aceptar el BTC como medio de pago, por nombrar un par de ejemplos, la empresa de

viajes española Destinia, páginas de claves de videojuegos (G2A, Instantgaming, etc.), la cadena de tiendas GearBest, CeX, Microsoft, Reddit, ONGs como Save the children o Green Peace, y muchas más organizaciones, cada día más lo aceptan y poco a poco se va estableciendo como otra alternativa más.

Ilustración 18 Bitcoin aceptado por Microsoft

Fuente: Microsoft

4.6. Ethereum

Ilustración 19 Logo de Ethereum

Fuente: Ethereum.org

Bitcoin fue la criptomoneda que empezó todo, la más famosa, la más criticada y la más descentralizada, pero no es la única criptomoneda relevante, de hecho, cuando hablamos de opciones y usos tal vez la más importante sea otra, el Ether, y su red Ethereum.

El Ether no fue confeccionado inicialmente con el objetivo de ser un medio de pago, su objetivo, recogido por su creador, el canadiense Vitalik Buterin, en su Whitepaper, en 2013, es ser “combustible para un ordenador mundial”, energía.

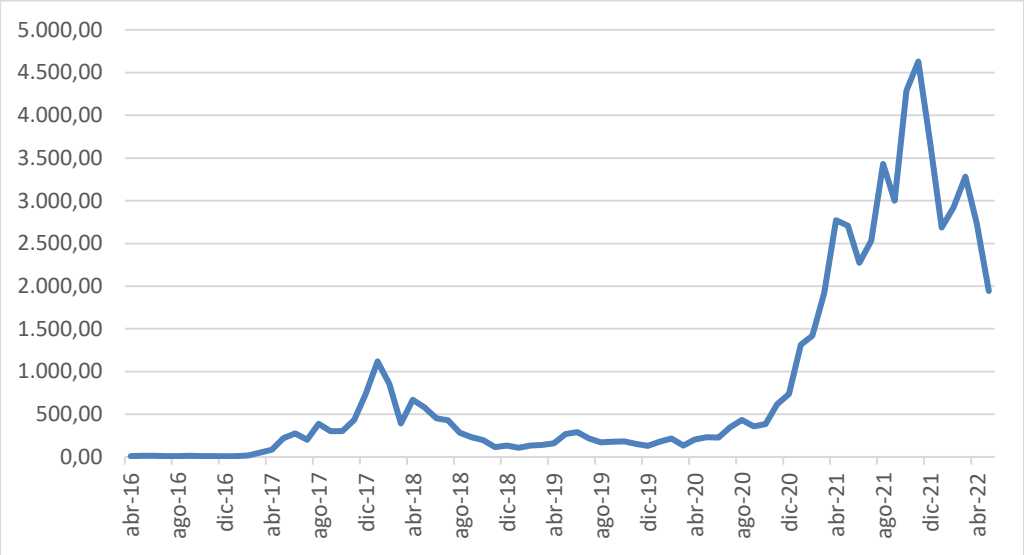
Cuando hablamos del Blockchain en este trabajo hicimos un apartado exclusivo a los Smart Contracts, lo que eran y lo que podían llegar a ser, pues bien, esos contratos funcionan a través de la red Ethereum, red la cual, funciona como una computadora global que administra y ejecuta en base de sus condiciones los Smart Contracts recogidos en ella.

El Ether existe como moneda ya que es el medio para sostener la red Ethereum, es la recompensa que se da a los nodos de la red por sustentarla, del mismo modo que el bitcoin la red Ethereum premia a sus usuarios con un cantidad determinada de Ether, 5 ETH, cuando minan un bloque, esto sucede aproximadamente cada 15 segundos.

La oferta inicial (ICO) de Ethereum fue de 60 millones de Ether creados, entre ellos 12 millones fueron para la fundación y sus desabolladores, porque a diferencia del Bitcoin la red Ethereum si está gestionada por unos desarolladores conocidos no anónimos, y cada vez que se valida un bloque se reciben otros 5 ETH de los 60 millones creados. A diferencia

del Bitcoin cada año se generan 18 millones nuevos de Ether, por lo que no es una red finita, la emisión es fija, lo que permite controlar su inflación.

Gráfico 5 Evolución histórica de la tasa de cambio del ETH respecto al $.



Fuente: Elaboración propia

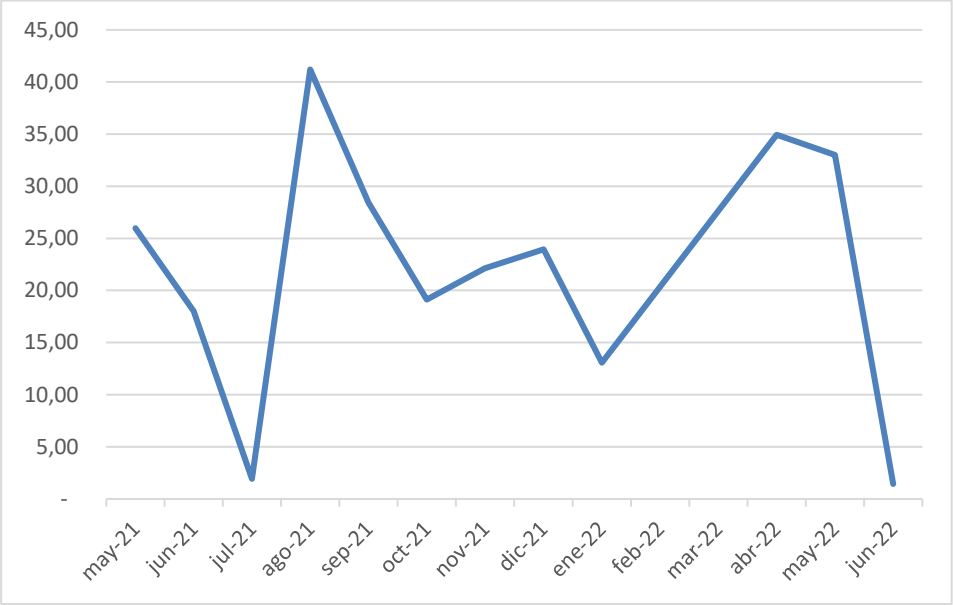
(datos recogidos de: https://es.investing.com/crypto/ethereum/historical-data)

Una de las mayores críticas hacia la red Ethereum es el elevado coste energético y daño ambiental que provoca, pare evitar esto los desarrolladores están trabajando en pasar la red a una versión 2.0 más concienciada con el medio ambiente, al reducir su consumo energético necesario para mantenerla, subdividiendo la cadena en otras más pequeñas e independientes encargadas de validar las transacciones y los Smart Contracts almacenados en ellas.

Además de servir como medio de gestión de los Smart Contracts nos gustaría destacar otro uso a mayores del Ether, los tokens. Y es que dentro de la red Ethereum se ha habilitado de generar tokens no fungibles, los conocidos NFTs, que sirven para efectuar compras de obras de arte digitales, pero también para validar cualquier propiedad, incluidas las físicas, por ejemplo, si una empresa inmobiliaria construyese almacenando sus registros en la red Blockchain a través de un NFT podría demostrarse la propiedad de la vivienda accediendo a la red. Otro uso que se le está dando es en el mundo del entretenimiento sirviendo como los antiguos álbumes de cromos, o incluso en el metaverso actual, el cual reside en los videojuegos, para gestionar la propiedad de los bienes digitales. Cabe destacar que en mayo de 2022 este mercado de los NFTs ha sufrido una caída tras

la eliminación de aproximadamente el 90% de los productos, quedando solo los más relevantes.

Gráfico 6 Volumen de negocio de los NFTS en millones de dólares



Fuente: Elaboración propia
(datos recogidos de: https://es.investing.com/equities/nft-investments-historical-data)

4.7. Otras criptomonedas importantes

4.7.1. Tether y las stablecoins

La primera criptomoneda que me gustaría comentar es Tether, la cual forma parte del grupo de las stablecoins, las cuales son criptomonedas respaldadas, al igual que las monedas fiduciarias, por una entidad.

Ilustración 20 Logo de Tether

Tether es una criptodivisas muy aceptada por las plataformas de compraventa de activos, y lo que la hace especial es que su precio es estable, 1$ equivale a 1 Tether (USDT) ya que están vinculadas.

Las stablecoins buscan ser un puente entre las modelas tradicionales y las criptomonedas ofreciendo estabilidad y transparencia plena.

4.7.2. Ripple, Litecoin y Cardano

Ripple (XRP) es llamado “el sucesor del Bitcoin” ya que fue desarrollada por supuestos desarolladores del Bitcoin con el objetivo de mejorarlo y servir de puente entre bancos y proveedores de pago con las criptomonedas, haciendo que sean medios de pago más aceptados. Es la tercera criptomoneda más usada del mundo y está respaldada por entidades como el Banco Santander o el Royal Bank de Canadá. A diferencia de otras criptomonedas el Ripple no tiene minería involucrada, funciona más como una moneda tradicional que como una red Blockchain.

Litecoin, también es un intento de mejorar el Bitcoin, es una criptomoneda muy joven y muy poco extendida, pero tiene un funcionamiento similar al bitcoin, con un algoritmo más simple y una mayor rapidez.

Cardano (ADA), es el representante de la 3º generación del Blockchain, y si Litecoin trata de mejorar a Bitcoin, Cardano tiene como objetivo ser un “Ethereum killer” como su fundador, Charles Hoskinson, antiguo desarrollador de Ethereum, lo describe.

4.8. Fiscalización de las criptomonedas

Que no exista una regulación específica hacia las criptomonedas no quiere decir que estén libres de las obligaciones fiscales. Estas obligaciones difieren dependiendo del uso que se les dé a las criptomonedas en cuestión.

4.8.1. Criptomonedas como medio de pago

En referencia a las criptomonedas como medios de pago surgen varias dudas ¿están sujetas al IVA? ¿Y al impuesto de transmisiones patrimoniales?

Lo cierto es que la Dirección General de Tributos señala lo siguiente: “las bitcoins, criptomonedas y demás monedas digitales son divisas porque los servicios financieros vinculados con las mismas están exentos de IVA”, es decir, las criptomonedas al usarse como medio de pago están sujetos pero exentos del Impuesto de Valor Añadido (artículo 20.1.18 Ley del IVA). Y también están exentas del impuesto de transmisiones patrimoniales ya que las entregas de dinero para pagar bienes y servicios están exentas.

4.8.2. Criptomonedas como inversión

Dentro del campo de las inversiones la cosa cambia ya que invertir activos en criptomonedas puede dar lugar a ganancias o pérdidas patrimoniales las cuales están

sujetas al IRPF (Art. 33 Ley del IRPF) por lo que los inversores en criptomonedas deberán tributarlas con el IRPF según sea la base imponible aplicable a sus ganancias generadas. En caso de ser una sociedad serán sujetos al Impuesto de sociedades.

La pérdida de las criptomonedas por robo, al haber dado la clave privada a alguien o que nos la hayan robado será considerado como pérdidas patrimoniales.

Además, las criptomonedas que una persona posea forman parte de su patrimonio por lo que estarán sujetas al Impuesto sobre el patrimonio y se sumarán en el cálculo de la base imponible aplicable de este.

La adquisición de criptomonedas a través de una donación o herencia estará sujeta al Impuesto de Sucesiones y Donaciones, que se aplique según la CCAA.

Solo estarán sujetas y no exentas al IVA las comisiones cobradas por el exchanger a través del cual se realicen los cambios de moneda.

4.8.3. Criptomonedas como actividad económica, minería.

Y por último esta la minería la cual es una actividad económica a través de la cual se generan unos beneficios que deberán declararse y estarán sujetos al Impuesto de actividades económicas, además según sea una persona física p una sociedad la beneficiaria de la minería deberán tributar las ganancias obtenidas a través de la actividad en sus impuestos correspondientes, IRPF o IS.

4.8.4. Fiscalidad de los NFT

La adquisición de un NFT debe ser declarada por las personas físicas en su declaración de la renta, ya que lo más cercano al concepto es un bien patrimonial y como tal estaría sujeto a tributos.

Además, como actividad económica dentro de un ámbito empresarial estaría sujeto al IRPF o al Impuesto de Sociedades en caso de ser una sociedad.

Tambien, al poder considerarse parte del patrimonio de una persona o entidad los NFTs están sujetos al Impuesto de Patrimonio, y en caso de heredarlos o recibirlos por donaciones estarían sujetos al Impuesto de Sucesiones y Donaciones.

4.9. Contabilidad de las criptomonedas

Lo primero que hay que tener en cuenta es el hecho de que las criptomonedas son “medios de pago al portador” ya que al no estar reguladas y no tener una entidad que las respalde

por norma general, no pueden ser consideradas dinero electrónico de curso legal, aún. Pero, independientemente de eso cualquier entidad que opere con ellas debe saber que esa actividad puede estar sujeta a la ley de Prevención de Blanqueo de Capitales y en la Ley de Protección de Datos de carácter personal.

En marzo de 2014 el Instituto de Contabilidad y Auditoría de Cuentas de España clasificó las criptomonedas como medios intangibles (como si fuesen programas informáticos, cosa que no acompaña del todo al concepto de criptomonedas) y como Existencias, concretamente mercaderías (pero de nuevo, tampoco tiene mucho sentido ya que las criptomonedas se comercian por su cualidad de medios de pago, no como software comerciable). Por si parte las Normas internacionales de Contabilidad los consideran activos financieros y como tales están sujetos a esta.

Para contabilizar de una manera correcta las criptomonedas cabe destacar dos hechos contables diferentes:

- Cuando el hecho contable suponga la compraventa de criptomonedas con entrega de dinero Fiat, pasarán a ser activos corrientes si permanecerán menos de un año en nuestras reservas, o no corriente si lo excede, por lo que figuraran en la partida de deudores comerciales y otras cuentas a cobrar.
- Por otro lado, se contabilizará como una Permuta Comercial cuando se realice la compraventa de productos y servicios y la contrapartida recibida (en caso de ser una venta) o entregada (en caso de ser una compra) sean criptomonedas.

Las criptomonedas no son consideradas tesorería debido a que no están respaldadas por ningún banco o entidad financiera, por norma general, y tampoco están aceptadas de forma generalizada como medio de pago. Además, hay que diferenciar según como se hayan adquirido, si por vía primaria (minando) o secundaria (plataforma de trading).

La falta de regulación da lugar a una incertidumbre total, que sumado al carácter de seudoanonimato de las criptomonedas puede dar la ocasión de que se realicen actividades ilícitas con ellas. Y también es importante destacar que si se pierde la clave se sufre una pérdida total de las criptomonedas del monedero contenido en ellas.

Además, no es que haya una falta mundial de regulación, sino que las pocas propuestas que van surgiendo en cada país chocan con las de los demás dificultando mucho más el lograr una regulación común y completa que facilite y aclare todas las dudas que hay respecto a la contabilización de estos activos inmateriales.

5. Conclusiones

Para empezar estas conclusiones destacar, sin que parezca que lo decimos de forma grandilocuente, como la tecnología está cambiando a pasos agigantados el mundo, y las criptomonedas han llegado para quedarse, la educación sobre este tema es necesaria, porque tal vez no sustituyan al dinero tradicional como medio de pago estandarizado, ya que su volatilidad y su propio carácter de privacidad total hacen que esto sea complicado, por no decir imposible, pero si se van a quedar como una alternativa más. Desde que han aparecido, las criptomonedas no han dejado de sufrir burbujas, las cuales hasta cuando parece que se estabilizan estallan.

En este trabajo hemos tratado de determinar si las criptomonedas son medios de pago, y lo cierto es que actualmente según a quien preguntes te podrá responder una cosa u otra, pero se acercan más a un activo especulativo que un medio de pago aceptado socialmente. Tambien cabe decir que, debido a su carácter tan opaco, a todas sus polémicas, a todas sus críticas y a su desconocimiento nos encontramos hablando de un activo con un futuro completamente imprevisible, puede que en el futuro pierdan ese carácter especulativo, puede que sean más aceptadas más que vistas como un peligro. Lo cierto es, que las criptomonedas han abierto un mercado completamente nuevo del cual solo nos queda esperar y ver como acabará.

Asimismo, no todas las criptomonedas son monedas porque buscan ser medios de pago, el bitcoin sí, pero por ejemplo Ethereum busca otros objetivos, y la moneda en si solo es una recompensa para todos aquellos que ayudan a sus fundadores a lograrlos.

Por otro lado, está el Blockchain tecnología la cual, sí que me permite el lujo de considerarla, sin parecer grandilocuente, una de las grandes invenciones tecnológicas con más potencial de los últimos tiempos, o al menos de la última década. Las inversiones que están realizando múltiples entidades, gobiernos y empresas en el campo del Blockchain confirma que existe un gran interés en madurar, aprender, y adaptarse a esta nueva invención. El ámbito financiero no es el único sector donde esta tecnología puede mejorar nuestras vidas, también el sanitario, el energético, el informático blindándole más seguridad, o incluso el alimenticio reduciendo los tiempo de suministro, muchas son las opciones para las cuales puede ser muy útil.

Es necesaria una normativa que regule mas todo lo referente a las criptomonedas y el Blockchain, la protección al usuario, la contabilidad y tributación, que se dé más información, lograr blanquear más aun las actividades que se realicen con ellas, frenando el mercado negro, y sobretodo que socialmente se aprenda más sobre ellas, que se pierda

el miedo a lo desconocido, porque no sabemos qué pasará con ellas, pero tienen mucho potencial y si no las conocemos no seremos capaz de explotarlo.

6. Bibliografía

PÁGINAS WEB

- Asesoria Afiris (Junio 2022). Fiscalidad y Contabilidad de las criptomonedas. Obtenido de https://www.afiris.es/la-fiscalidad-nft/ y https://www.afiris.es/fiscalidad-de-las-criptomonedas/
- Bankinter (Mayo 2022). Microsoft acepta Bitcoin. Obtenido de https://www.bankinter.com/blog/lo-ultimo/microsoft-ya-acepta-bitcoin-para-la-compra-de-aplicaciones-y-juegos
- Bit2Me Academy (Abril 2022). Seudoanonimato del Bitcoin. Obtenido de https://academy.bit2me.com/bitcoin-no-es-anonimo/
- Contaone (Junio 2022). Contabilidad de las criptomonedas. Obtenido de https://www.contaone.com/como-contabilizar-el-dinero-digital-criptomonedas-o-monedas-virtuales/, gracias a Eulogio Alonso.
- Criptomonedas e ICO (Marzo 2022). Skuchian, empresa de Smart contrats. Obtenido de https://criptomonedaseico.com/noticias/skuchain-la-plataforma-blockchain-ofrece-contratos-inteligentes-para-financiar-el-comercio-en-canada/
- Criptonoticias (Enero 2022). ¿Cómo elegir un monedero de bitcoin, otras criptomonedas y criptoactivos?. Obtenido de https://www.criptonoticias.com/
- Criptonoticias (Enero 2022). Blockchain y criptomonedas: fundamentos y características. Obtenido de https://www.criptonoticias.com/
- Economía3 (Abril 2022). Monederos de criptomonedas. Obtenido de https://economia3.com/wallet-monedero-criptomoneda-que-es/
- Economist (Noviembre 2021). El fin del efectivo. Obtenido de (https://www.economist.com/leaders/2007/02/15/the-end-of-the-cash-era
- El Blog Salmon (Abril 2022). Devaluación del dólar, crisis 2008. Obtenido de https://www.elblogsalmon.com/economia/la-devaluacion-del-dolar-y-la-nueva-guerra-de-divisas
- ELPAIS (Diciembre 2021). Dinero negro en el mundo. Obtenido de https://elpais.com/economia/2019/09/21/actualidad/1569062038_189861.html
- ELPAIS (Diciembre 2021). Primera plataforma de criptomonedas reconocida por el Banco de España. Obtenido de https://elpais.com/economia/2022-02-17/bit2me-se-

convierte-en-la-primera-plataforma-de-criptomonedas-reconocida-por-el-banco-de-espana.html

- FMI (Abril 2022). Informe volumen de negocio del mercado negro. Obtenido en (https://www.imf.org/external/pubs/ft/fandd/2019/09/pdf/fd0919.pdf)
- Finect (Abril 2022). Tipos de monederos. Obtenido de https://www.finect.com/usuario/vanesamatesanz/articulos/wallet-criptomonedas-que-es-tipos-como-elegir
- FORBES (Enero 2022). Los bancos están adoptando el Blockchain. Obtenido de https://www.forbes.com/sites/forbesbusinesscouncil/2021/06/23/trends-in-blockchain-why-big-banks-are-adopting-this-technology/?sh=496c3d8151e2
- Foro Bitcointalk (Abril 2022). Mensaje de Laszlo, primera transacción de Bitcoin. Obtenido de https://bitcointalk.org/index.php?topic=137.msg1141#msg1141
- Grupo Atico34 (Abril 2022). Tipos de criptografia. Obtenido de https://protecciondatos-lopd.com/empresas/criptografia-asimetrica/
- Hablemos de Empresas (Marzo 2022). Blockchain y la industria 4.0. Obtenido de La tecnología Blockchain en la industria 4.0: casos y aplicaciones (hablemosdeempresas.com)
- IMF F&D (Noviembre 2021). HIDDEN CORNERS OF THE GLOBAL ECONOMY. Obtenido de Hidden Corners of the Global Economy – IMF F&D | September 2019
- INTRUM (Abril 2022). Informe de previsiones sobre el uso de efectivo, en España. Obtenido en https://www.intrum.es/soluciones-empresariales/sala-de-prensa/noticias/3-de-cada-4-empresas-espanolas
- Investing (Abril 2022). Datos de valores respecto al dólar. Obtenido de https://es.investing.com/
- Investopedia (Abril 2022). Otras criptomonedas importantes. Obtenido de https://www.investopedia.com/tech/most-important-cryptocurrencies-other-than-bitcoin/
- Medium (Marzo 2022). La historia de ecash. Obtenido de https://medium.com/blockchain-academy-mexico/la-historia-de-ecash-y-cómo-el-sueño-de-david-chaum-originó-el-movimiento-cypherpunk-19fa003b1a3c
- MyChouseToPay (Noviembre 2022). Formas de pago online. Obtenido de ¿Cuáles son las principales formas de pago online? | MyChoice2Pay

- Stadista (Mayo 2022) Datos de compras online por dispositivos. Obtenido de https://es-statista-com.ponton.uva.es/estadisticas/496546/distribucion-de-dispositivos-utilizados-para-compras-en-linea-en-espana/
- Xakata (Noviembre 2021). Nueva legislación de criptomonedas en España. Obtenido de https://www.xataka.com/legislacion-y-derechos/entra-vigor-nueva-regulacion-para-criptomonedas-espana-como-afecta-que-obligaciones-se-anaden
- Xakata (Diciembre 2021) Planes del Gobierno respeto al efectivo, España. Obtenido de Cómo es el plan del Gobierno para acabar con el dinero en efectivo en España y qué límites marca la Unión Europea (xataka.com)

LIBROS Y ARTICULOS

- Bitcoin lo cambia todo: Implicaciones sociales y económicas de la invención más importante del siglo XXI - Gael Sánchez Smith
- Bitcoin, un sistema de dinero en efectivo electrónico peer-to-peer (Artículo) - Satoshi Nakamoto
- Bitcoins. Revolución o Historia - Jaime Sánchez de Diego Martínez-Cabrera
- Blockchain y sus aplicaciones - Benjamin Yahari Navarro
- Blockchain. Cómo desarrollar confianza en entornos complejos para generar valor de impacto social - Marcos Allende López
- Contabilidad y auditoría de criptomonedas: España, NIIF y USGAAP - Belén Toro Universidad Pontificia de Comillas y Manuel Rejón Universidad de Granada, gracias a Eulogio Alonso.
- Criptomonedas : qué son, cómo utilizarlas y por qué van a cambiar el mundo: todo lo que necesitas saber para invertir en criptomonedas con éxito - José Manuel Torres
- El mercado de las criptomonedas. Análisis de rentabilidad y riesgo. - Leandra Caro Padrón